Omega Core Audit ™
For MS SQL Server

August, 2025

DATAPLUS

Access control, audit monitoring and protection in real time

Omega Core Audit
For MS SQL Server

User's Guide

1.0.0

www.dataplus-al.com

TABLE OF CONTENTS

1 CHAPTER 1: Omega Core Audit Overview

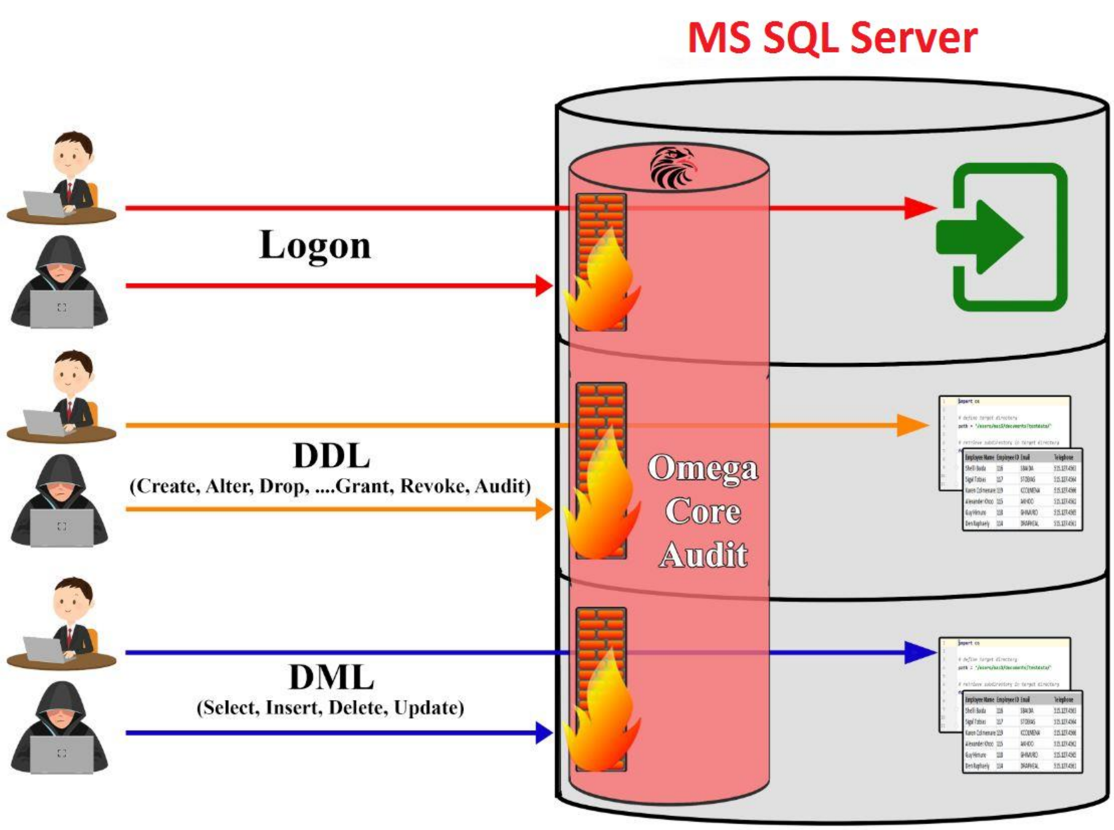
1.1 Introducing Omega Core Audit

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 MS SQL Server 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 MS SQL Server 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 server - 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.



Omega Core Audit diagram

1.2 Key Benefits

- Real-Time Access Control, mandatory authorization of the server logon process.
- Continuous Audit Monitoring, highly detailed, up to the full SQL
- Real-Time Protection for structural (DDL commands) changes.
- Enforcement on privileged accounts and SYSADMINs.
- Common Security Events Trail for all modules.
- Separation of Duty and out-of-box Roles for system's main components.
- Secured Protected Areas.
- Change Control.
- Policy-based evaluation.
- Multi-factorial User & environment context authorization in real time.
- Automatic management of audit trail records.
- 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.
- SIEM Integration.

1.3 Omega Core Audit Architecture

The Omega Core Audit solution has three main components:

- **Omega Core Audit Engine**: a MS SQL T-SQL software package containing core audit and protection logic, Back-End installed into the repository and server running under SYSADMIN privilege.
- **Omega Core Audit Repository**: a MS SQL Server database containing all system configurations and audit events, Back-End installed into the target MS SQL Server.
- **Omega Core Audit Application**: Windows-based client desktop Application, connecting to the target server and interacting with the Engine and Repository.

Omega Core Audit Engine

The Omega Core Auditing Engine is a MS SQL T-SQL software package installed in the server under SYSADMIN privileges. The Engine contains the core logic of the access control, auditing and protection.

Engine's core objects are:

P_SS_% procedures	T-SQL procedural objects containing core logic
OMEGACA_ACC	Server Trigger on After Logon event
OMEGACA_RTP_DDL	Server Trigger on Before DDL event
OMEGACA_TRANS	Server scheduler job for audit trails collection

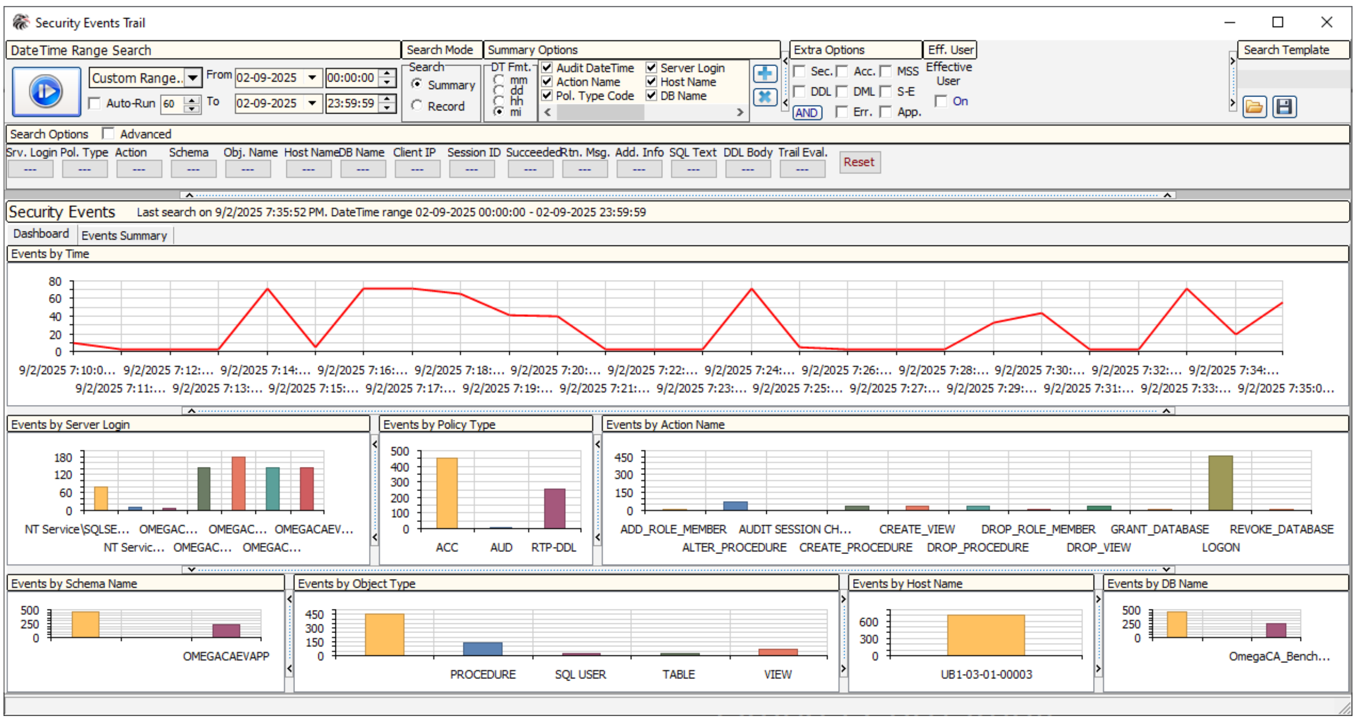
Omega Core Audit Repository

The Omega Core Auditing Repository is a MS SQL Server database named OmegaCoreAudit, containing all objects for Security Events data and all configuration options needed by the Engine.

OMEGACA a schema inside the database containing repository data and configurations

Omega Core Audit Application

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



Omega Core Audit SIEM integration option

Omega Core Audit's open structure allows and enables automatic retrieval of audited events to SIEMs and Log Management Systems that support:

- "Pull" by running a MS SQL query - supported by its open structure and as specifically by each SIEM

Note

Omega Core Audit is fully autonomous. SIEM built-in integration is an option for clients owning a SIEM system.

1.4 Compatibility, Requirements and Limitations

MS SQL Server support

Omega Core Audit supports on MS SQL Server versions 2019, 2022 and 2025.

All editions of the MS SQL Server are supported!

Omega Core Audit Application requirements

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

- All x86/x64 versions of Windows from XP and above supported by MDAC 2.8.
- MDAC 2.8 for MS SQL client connectivity.

Omega Core Audit limitations

Omega Core Audit has currently the following limitations:

1. Only databases opened in Read-Write mode are supported.

Visit our website for news on current developments.

www.dataplus-al.com

1.5 Release notes for version 1.0.0

New in 1.0.0:

This is the first release of Omega Core Audit for MS SQL Server.

Fixes in 1.0.0:

This is the first release of Omega Core Audit for MS SQL Server.

Note:

Full development is presented in Annex B. Development History

2 CHAPTER 2: System Wide Functionalities, Utilities and Guidelines

2.1 Common Application functionalities

2.1.1 Connecting to the target database

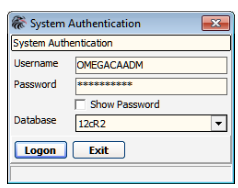
With the Omega Core Audit application you can connect one-at-a-time to all MS SQL Servers in which you have previously installed the Omega Core Audit Engine and Repository, and that you have configured in its initialization file.

Connecting to the target database

After you have opened the Omega Core Audit Application, to connect to (one of) the monitored target MS SQL Servers, 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.

This will invoke the target database System Authentication form. The Database combo box loads the target database section entries configured in the initialization file OmegaCA.ini (refer to the Omega Core Audit Deployment Guide, topic Omega Core Audit Application Deployment for more details on connectivity).

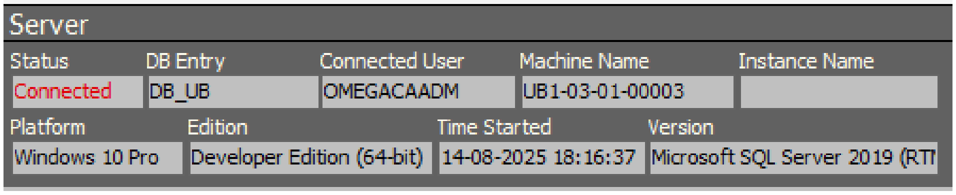
Enter the username and password of your Omega Core Audit account on the selected target database.



Press the Logon button to connect to the target database. After a correct authentication, the application's main Menu will display other menus, according to the Omega Core Audit Role grants of the current user.

Target database information

After logging on to the target server, the edit boxes of the Server panel, bottom-left of the application's main form, will be filled with information related to the target server.



The Server panel fields are:

Status	Connection Status of the target server
DB Entry	Target database connection entry as loaded from the initialization file
Connected User	The Omega Core Audit user account connected to the target server
Machine Name	Name of the server's host
Instance Name	Name of the instance (when applies)
Platform	Target server's platform
Edition	Target server's edition
Time Started	Time last started of the target server
Version	MS SQL Server

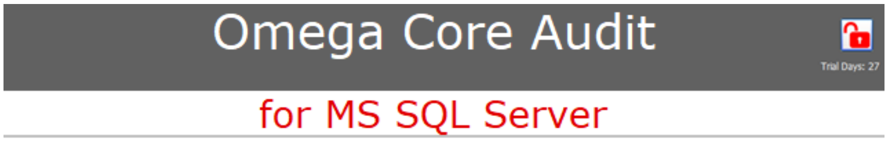
Disconnecting from the target server

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

This will clear all the fields of the Server panel, except for the Status!

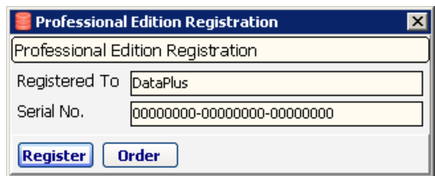
2.1.2 Software License Activation

Initially the Omega Core Audit will with full features for a Trial evaluation.



The Trial period is 30 days. After the trial period expires the application's main features will disable.

The software can be registered during the Trial period or after its expiration by clicking on the red-lock button on the right of the program's name – on form's bottom



The "Registered To" and the Serial number are both assigned to the client by DATAPLUS (the Order button!). Complete both and press button Register to register the software. You will receive a confirmation on the right combination of Registered To/Serial.

2.1.3 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 the 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.

Performance Note:

Remember that Omega Core Audit is a typical Windows Desktop data-aware application. The whole set of records queried on the server is returned as a record-set and there is no "Next 50 Records" concept. As the Omega Core Audit Engine and Repository are integrated inside the monitored server, queried is the "live production" machine!

Large amounts of records, most probable when searching in Records Search Mode (!), are normally limited only by your server and network capacity, and also the amount of your local workstation's RAM. Queries like:

1. FTSs - full table scans on the (large table) Security Events Trail.
2. Large amount of data returned from Security Events Trail.

Not only can cause burden on the database server and then on the network, but in the later case the application will throw an error because of the incapacity of your local workstation's RAM to handle the big amount of information. To protect from such eventual failures, the Omega Core Audit sets limits in the queries performed in the Security Events Trail, for queries of both Search modes Summary and Records (discussed in respective topics); and raises Warnings when these limits are met. These limits are implemented via the two initialization parameters "Unified Trail Max. Rows" and "Unified Monitor Max. Rows", both default set to 100,000, which you can increase in the form "System Settings".

Hint

Search Summary first, and next on raw records!

2.1.4 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.

2.1.5 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 (usually) 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.

2.1.6 DateTime Field Format

The Omega Core Audit application always uses the DD-MM-YYYY and optionally HH24:MI:SS 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 Audit Specification and can be individual user statements or database object to be audited, depending on the 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 database Name, 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.

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, and Real-Time Protection DDL 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 MS SQL syntax is supported.
- Factor validation by Minimum Trust Level - required match with different predefined factor identities assigned with trust levels.

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 should 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.

The cache mechanism is implemented separately for each policy module, the respective form are available under the main menu Audit Policies, bottom to every module's button that opens the policies forms.

Reminder:

Cache is applied at Access Control and Real-Time Protection DDL modules only!

Important Note:

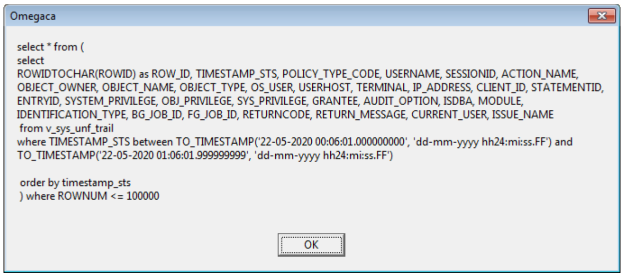
Under normal circumstances all policies where cache applies should be cache-enabled!

2.4 Debug and Diagnostics

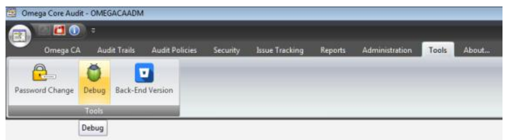
Omega Core Audit comes with a set of functionalities for debugging and diagnostics.

2.4.1 Client-Side Debug

Client-Side 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 application code points. It is helpful for performing debug and diagnosis of application's possible issues or behavior understanding.

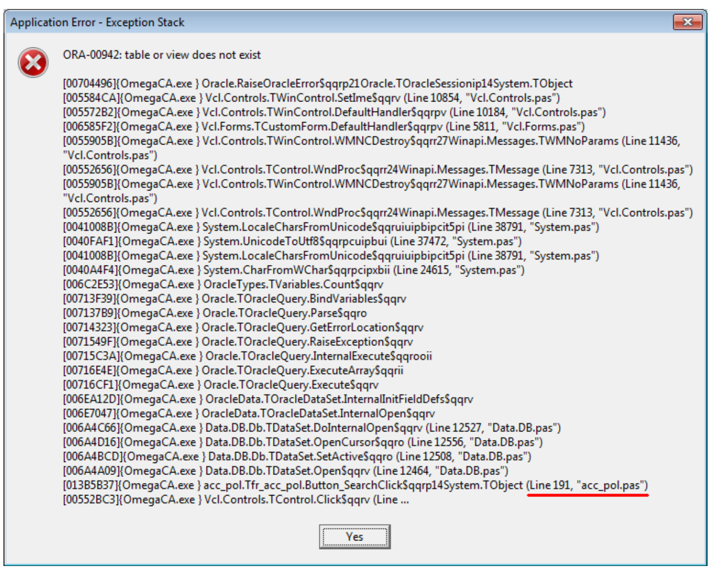


To enable the functionality, in the Application's main menu, tab Tools, click on the button Debug (button's image will change to indicate an active debug). To disable click again button Debug. You will receive a message in both cases.

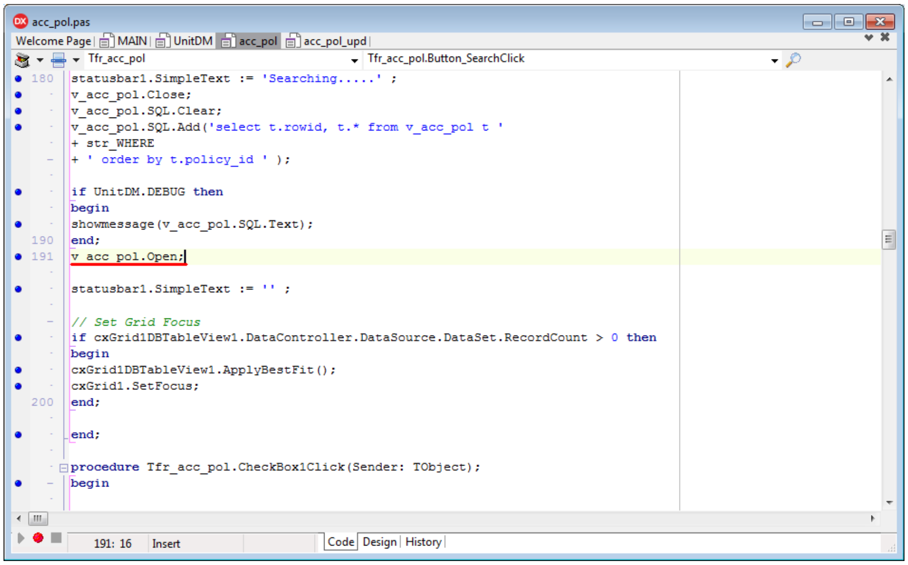


Full Error Stack

The Full Error Stack produces extra debug information on eventual program errors. The Full Error Stack is controlled by the Application's Debug status! The detailed error stack part will be added to the normal error message.



Detailed up to the line number of the failing application code-unit, it facilitates program's debug and diagnostics and enables support to immediately locate the faulting code unit and line.



According to specific operations, the full error stack is produced as one or more of:

- Program Error Message Dialogs
- Clipboard text (later topic)
- Report Scan Message field content

Full Error Stack in Clipboard

The Full Error Stack feature is also available at operating system's Clipboard – and as such Paste-able on any text editor, ex. Notepad/WordPad – under the following circumstances:

On each unattended Error Message Dialog
On all Report Class single-Items form execution Error Message Dialog *

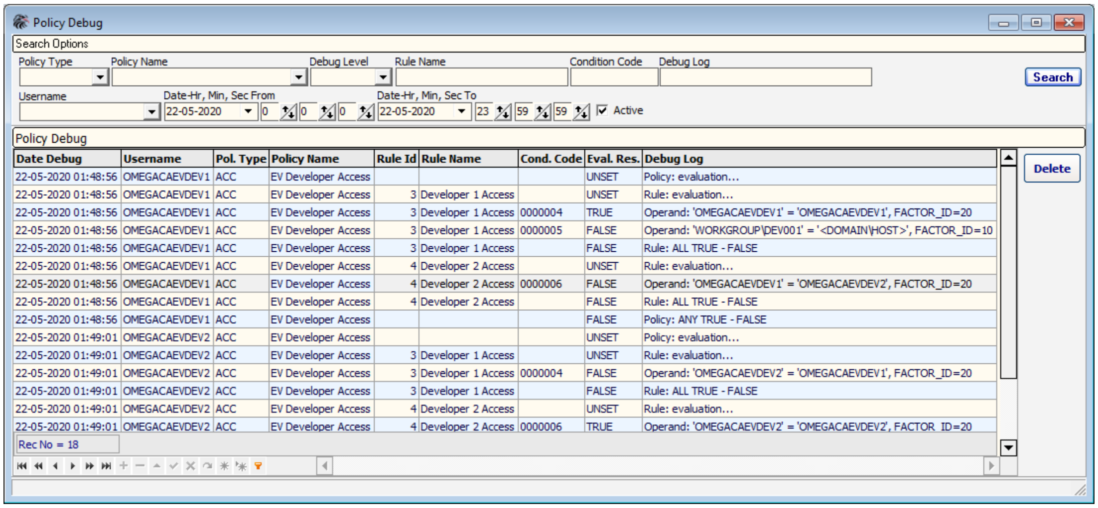
```
ORA-00942: table or view does not exist

[00704496]{OmegaCA.exe } Oracle.RaiseOracleError$qqrp21Oracle.TOracleSessionip14System.TObject
[005584CA]{OmegaCA.exe } Vcl.Controls.TWinControl.SetIme$qqrv (Line 10854, "Vcl.Controls.pas")
[005572B2]{OmegaCA.exe } Vcl.Controls.TWinControl.DefaultHandler$qqrpv (Line 10184, "Vcl.Controls.pas")
[006585F2]{OmegaCA.exe } Vcl.Forms.TCustomForm.DefaultHandler$qqrpv (Line 5811, "Vcl.Forms.pas")
[0055905B]{OmegaCA.exe } Vcl.Controls.TWinControl.WMNCDestroy$qqrr27Winapi.Messages.TWMNoParams (Line 11436, "Vcl.Controls.pas")
[00552656]{OmegaCA.exe } Vcl.Controls.TControl.WndProc$qqrr24Winapi.Messages.TMessage (Line 7313, "Vcl.Controls.pas")
[0055905B]{OmegaCA.exe } Vcl.Controls.TWinControl.WMNCDestroy$qqrr27Winapi.Messages.TWMNoParams (Line 11436, "Vcl.Controls.pas")
[00552656]{OmegaCA.exe } Vcl.Controls.TControl.WndProc$qqrr24Winapi.Messages.TMessage (Line 7313, "Vcl.Controls.pas")
[0041008B]{OmegaCA.exe } System.LocaleCharsFromUnicode$qqruiuipbipcit5pi (Line 38791, "System.pas")
[0040FAF1]{OmegaCA.exe } System.UnicodeToUtf8$qqrpcuipbui (Line 37472, "System.pas")
[0041008B]{OmegaCA.exe } System.LocaleCharsFromUnicode$qqruiuipbipcit5pi (Line 38791, "System.pas")
[0040A4F4]{OmegaCA.exe } System.CharFromWChar$qqrpcipxbii (Line 24615, "System.pas")
[006C2E53]{OmegaCA.exe } OracleTypes.TVariables.Count$qqrv
[00713F39]{OmegaCA.exe } Oracle.TOracleQuery.BindVariables$qqrv
[007137B9]{OmegaCA.exe } Oracle.TOracleQuery.Parse$qqro
[00714323]{OmegaCA.exe } Oracle.TOracleQuery.GetErrorLocation$qqrv
[0071549F]{OmegaCA.exe } Oracle.TOracleQuery.RaiseException$qqrv
[00715C3A]{OmegaCA.exe } Oracle.TOracleQuery.InternalExecute$qqrooii
[00716E4E]{OmegaCA.exe } Oracle.TOracleQuery.ExecuteArray$qqrii
[00716CF1]{OmegaCA.exe } Oracle.TOracleQuery.Execute$qqrv
[006EA12D]{OmegaCA.exe } OracleData.TOracleDataSet.InternalInitFieldDefs$qqrv
[006E7047]{OmegaCA.exe } OracleData.TOracleDataSet.InternalOpen$qqrv
[006A4C66]{OmegaCA.exe } Data.DB.Db.TDataSet.DoInternalOpen$qqrv (Line 12527, "Data.DB.pas")
[006A4D16]{OmegaCA.exe } Data.DB.Db.TDataSet.OpenCursor$qqro (Line 12556, "Data.DB.pas")
[006A4BCD]{OmegaCA.exe } Data.DB.Db.TDataSet.SetActive$qqro (Line 12508, "Data.DB.pas")
[006A4A09]{OmegaCA.exe } Data.DB.Db.TDataSet.Open$qqrv (Line 12464, "Data.DB.pas")
[013B5B37]{OmegaCA.exe } acc_pol.Tfr_acc_pol.Button_SearchClick$qqrp14System.TObject (Line 191, "acc_pol.pas")
[00552BC3]{OmegaCA.exe } Vcl.Controls.TControl.Click$qqrv (Line 7429, "Vcl.Controls.pas")
[00C7007C]{OmegaCA.exe } JvXPCore.TJvXPCustomControl.Click$qqrv
[00C71944]{OmegaCA.exe } JvXPButtons.TJvXPCustomButton.Click$qqrv
```

* On both cases use Ctrl-V just before clicking the OK button of the Error Message Dialog

2.4.2 Server-Side individual Policy Debug

You can set the Debug option for each policy on any module, 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 of the debug-activated policy. It is helpful for performing debug and diagnosis of eventual issues or behavior understanding.

The Policy Debug Log form is common to policies of all modules. It is accessible in the main menu Audit Policies.



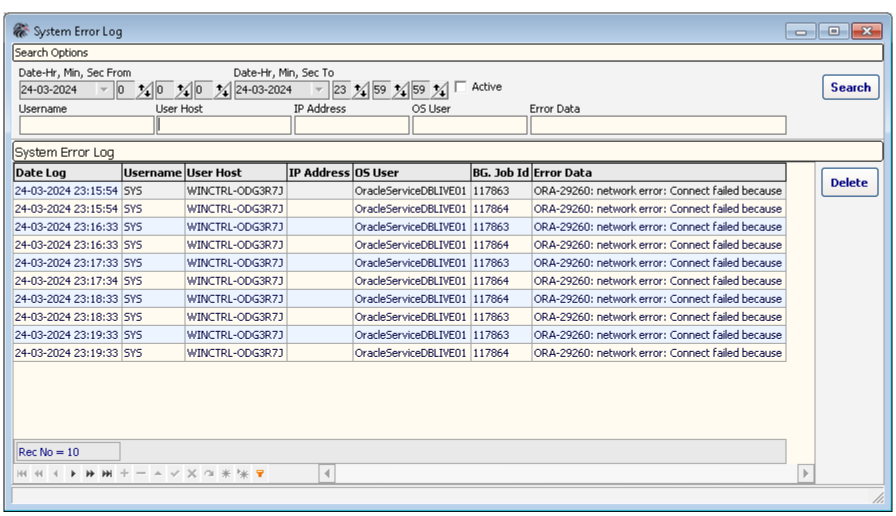
Important Notes:

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!

Cache is applied at Access Control and Real-Time Protection DDL modules only!

2.4.3 System Error Log

Any potential execution error of the Omega Core Audit's is silently stored in a central system error log, without any interruption of the activities. To view any such 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. 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. 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 Collect Job, unknown values in columns. This might be the case for new codes provided by MS SQL Server, 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 Security Events 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.

3 CHAPTER 3: Security Events Trail

Omega Core Audit Repository features a Security Event Trail of audit and protection events from the following source modules:

- Access Control
- Audit
- Real-Time Protection DDL

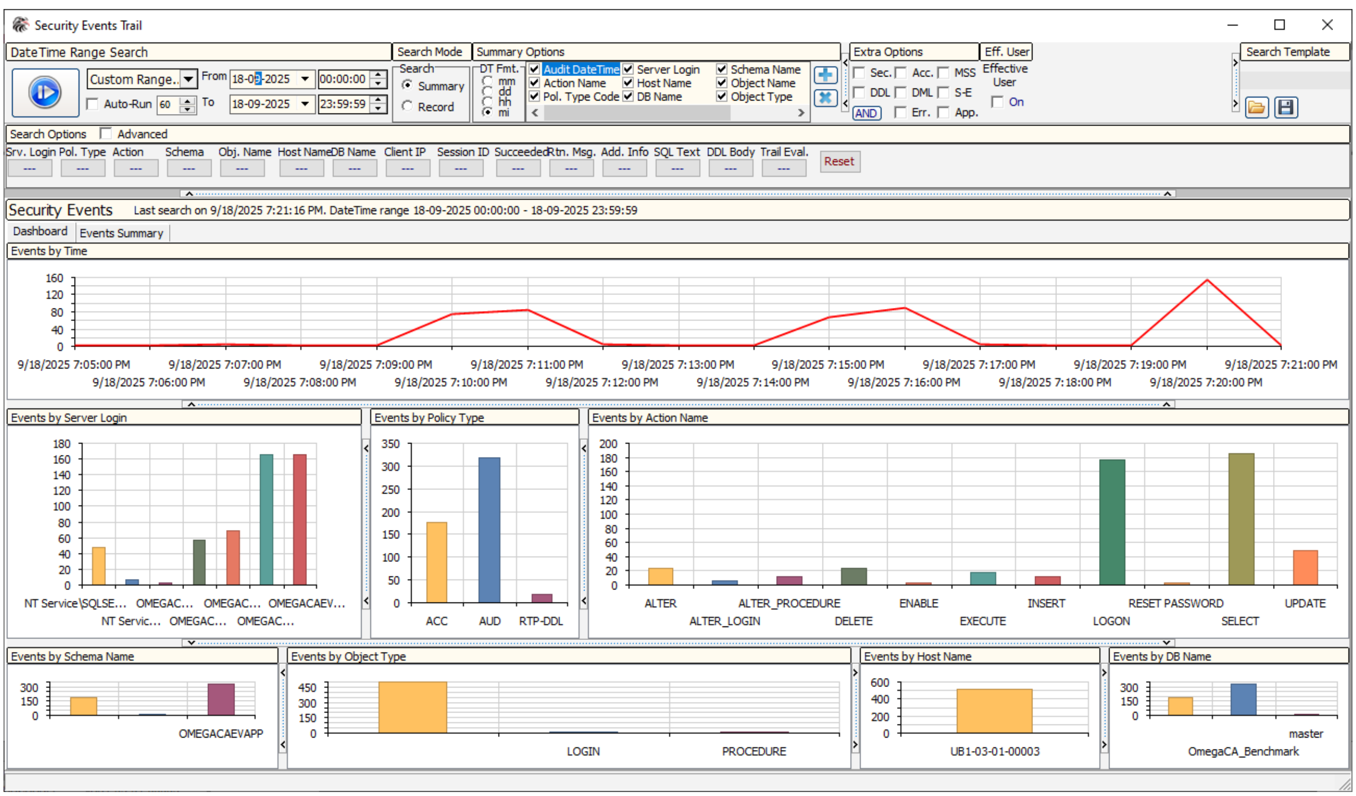
The unification of security events from different sources (functional modules) into a single trail offers benefits in visualization, management and provides a better look into the monitored database activity.

3.1 The Security Events Trail form

The Security Events Trail form is of most importance and is used to view the audited database activity. To open it, in the Main Menu, Tab Security Events, group Security Events Trail click the button Security Event Trail.

3.1.1 Security Events Trail form - Overview

In this form the Security Event records are searched and presented in both Summary and Records general views, as determined by the Search Mode.

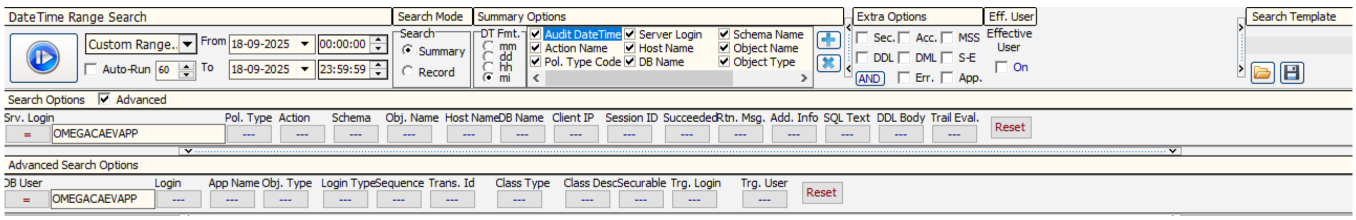


In the Summary mode, the several dashboards in the first tab Dashboard, and summary dataset in the second tab Events Summary, display overall visual and summary information on the audited security events.

In the Records mode, the Security Events are presented in whole as a dataset in the first tab Security Events, and individually in the second tab Event Details, for each previously selected in the first.

3.1.2 Searching the security events

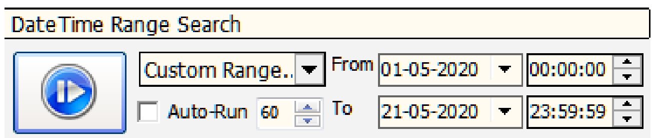
On top of the form features a flexible search on the Security Events, with security-related built-in templates and custom conditions on over 30 search-enabled fields of top importance.



Search components of the Security Events Trail form are described below:

Date Time Range Search

In this panel you define the obligatory DateTime range conditions for searching the Security Events.



Several predefined DateTime Range intervals are available in the combo box. Or choose any interval by "Custom Range…".

They will auto-complete when you click the Search (blue arrow) button, with the date-time referenced from the database server! If the Custom Range interval is chosen, it will unlock for editing and auto-complete the Date Time editors with the range of the current date.

To search the Security Events, press the Search (blue arrow) button and wait until search completes. The Auto-Run checkbox, available in Summary mode only, will enable auto-searching of audited security events.

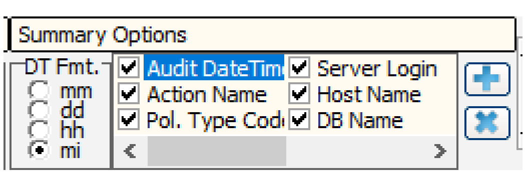
Search Mode

Here you define the mode in which search will be performed.

Summary	Security Events are presented in summary mode, by grouping fields of choice in the Summary Options fields. Database audited activity is displayed visually and as a summary dataset. Default option.
Records	Security Events are presented at record-level, with almost 30 fields of top importance, and also at individual record-level.

Summary Options

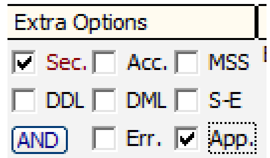
In this panel, activated for Search Mode Summary only, the following summary search options are defined:



Date Format	The format of DateTime fields when present in summary mode: Month, Date, Hour or Minute.
Summary Fields	Fields selected for summary grouping. Press the "Plus" button to invoke form Event Columns and add other available fields by double-clicking on the grid. Press the "Minus" button to remove a field from group display.

Extra Options

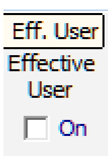
In this panel built-in security templates can be activated with a single click to implement specific conditions on the search of security events, according to specific built-in aspects of database security.



Security	Grant and revoke actions on system, roles and objects privileges Audis and No-Audit actions on user statements and object privileges Actions on Users and Roles Actions on important MS SQL Server security related objects Actions on any object of Omega Core Audit repository schema
Access	System access activity, logons and logoffs
MSS	Actions on MS SQL-owned objects (Dictionary included)
DDL	DDLs - Data Definition commands
DML	DMLs - Data Manipulation commands (SELECT not included)
S-E	Actions of kind SELECT and EXECUTE
Errors	All non-successful security events, Return Code not 1, either from MS SQL or Omega Core Audit
Application	Actions performed on user-made databases

Effective User

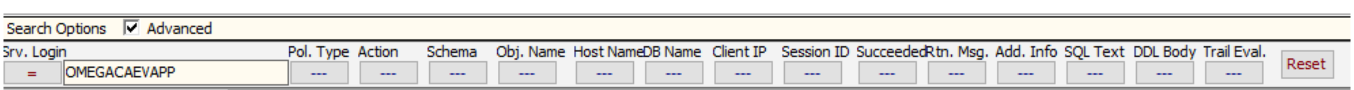
A Top-SQL action is an action explicitly launched by the user. A non-top SQL is an action called implicitly by the user, ex. via a trigger or from the body of a procedure called by the user.



Checking the Effective User On checkbox will activate searching of Top-SQL security events only!

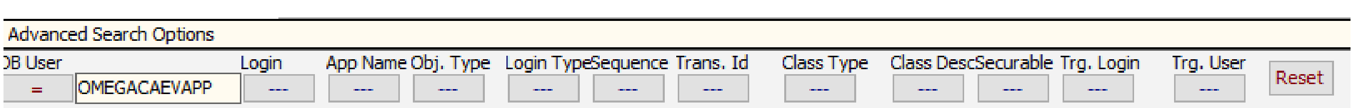
Search Options

In this panel search conditions on the most important fields of the Security Event record are defined.



The field search groups start with the Srv. Login and Policy Type and end with the Trail Eval.. By default all field search groups contained are inactive. 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. Use the Reset button to clear all search conditions in this panel.

Advanced Search Options



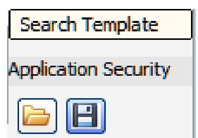
In this panel search conditions for other important fields of the Security Event record are defined. It operates the same as the Search Options panel. Not visible by default, is activated by checking the checkbox Advanced on the main Search Options panel. The fields search groups start with the IP Address and Terminal and end with the Target (DB) User. By default all field searches are inactive. Use the Reset button to clear all search conditions in this panel.

Notes

1. It is at this form that mostly the topic "Important Performance Note" of the paragraph "Client-Side information retrieval" mostly applies. Try to narrow the DateTime Range Search interval, especially in Records Search Mode, when searching the Security Events. Although the "Audit DateTime" field is the sole indexed (by default) in the Repository's table, extend your search with other field conditions for large DateTime intervals.
2. Search on SQL Text, DDL Body, Return Message and Trail Evaluation is case-insensitive.
3. The separator for operands in case of IN/NOT IN operators is the semicolon (;).

Search Template

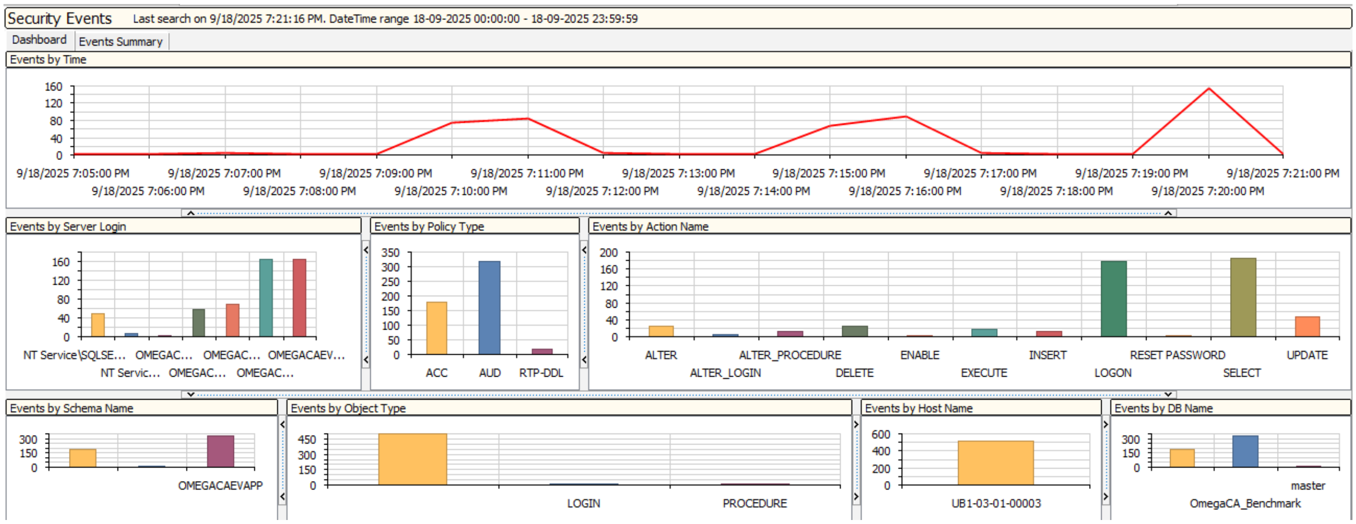
On form's top left, the Search Template allows for persisting and reloading all search configurations above except for the values of Date and Time fields "from and to" values when "Custom Range …" is chosen.



Load press button to load saved-search from disk
Save press button to save saved-search from disk

3.1.3 Dashboard

When Security Events are searched in Summary mode, the first tab Dashboard contains several ones for the security events by fields of top importance.



The dashboards available are:

Events by Time, Server Login, Policy Type, Action Name, Schema Name, Object Type, (user) Host Name, and DB Name.

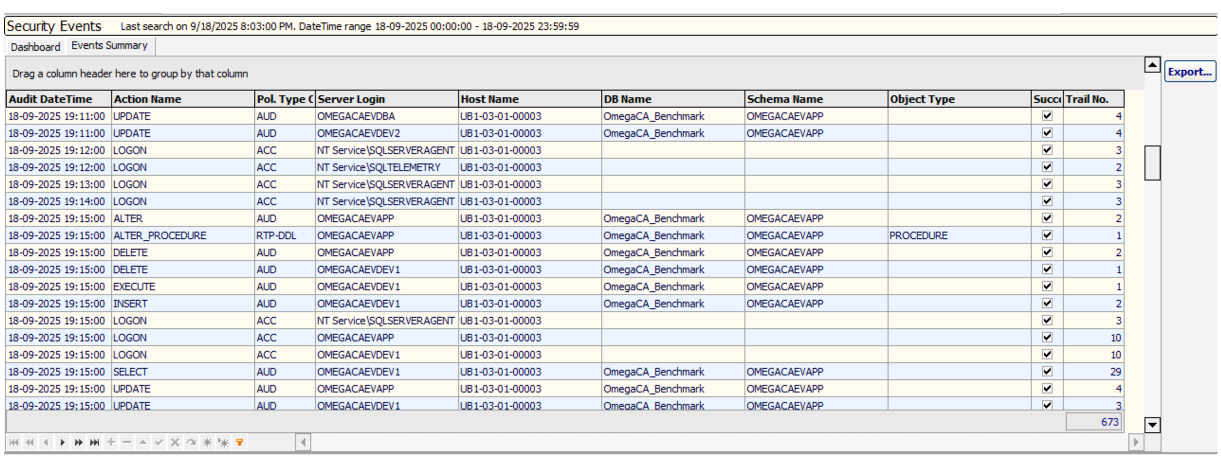
Right-click on each chart to save it as a Bmp file.

Hint:

Availability of each chart is related to the presence of the field in the summary search, as defined in the Summary Options panel fields.

3.1.4 Events Summary

The second tab Events Summary displays a summary of Security Events, same base data of the charts in the first tab Dashboard! The last field "Trail No." is an event count of the grouped fields!



Security Events Last search on 9/18/2025 8:03:00 PM. DateTime range 18-09-2025 00:00:00 - 18-09-2025 23:59:59

Dashboard Events Summary

Drag a column header here to group by that column

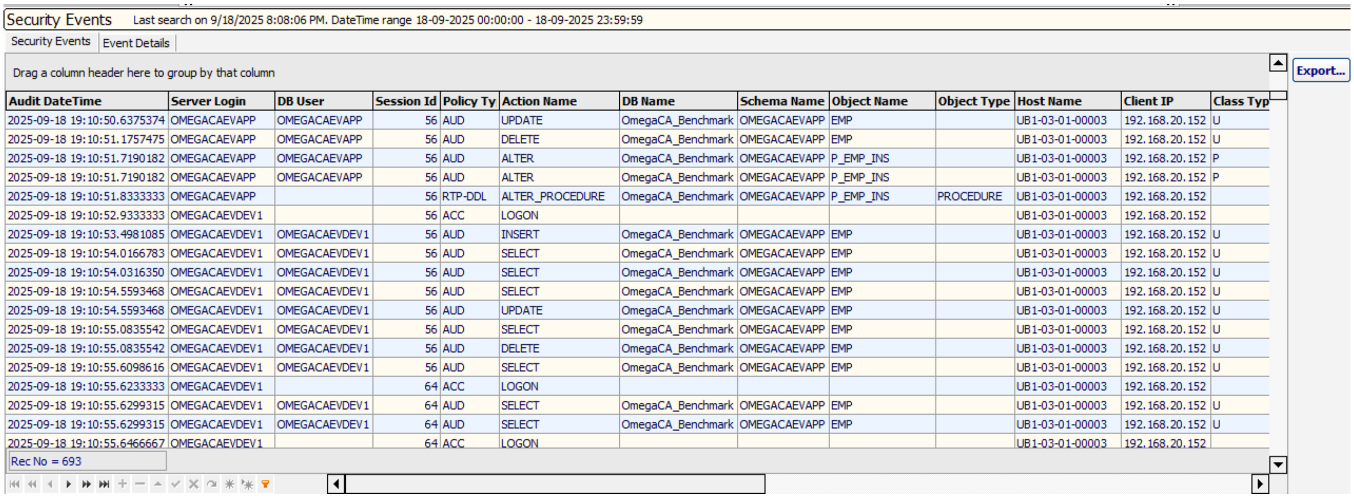
Export...

Audit DateTime	Action Name	Pol. Type (	Server Login	Host Name	DB Name	Schema Name	Object Type	Succ	Trail No.
18-09-2025 19:11:00	UPDATE	AUD	OMEGACAEVDBA	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	4
18-09-2025 19:11:00	UPDATE	AUD	OMEGACAEVDEV2	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	4
18-09-2025 19:12:00	LOGON	ACC	NT Service\SQLSERVERAGENT	UB1-03-01-00003				✓	3
18-09-2025 19:12:00	LOGON	ACC	NT Service\SQLTELEMETRY	UB1-03-01-00003				✓	2
18-09-2025 19:13:00	LOGON	ACC	NT Service\SQLSERVERAGENT	UB1-03-01-00003				✓	3
18-09-2025 19:14:00	LOGON	ACC	NT Service\SQLSERVERAGENT	UB1-03-01-00003				✓	3
18-09-2025 19:15:00	ALTER	AUD	OMEGACAEVAPP	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	2
18-09-2025 19:15:00	ALTER_PROCEDURE	RTP-DDL	OMEGACAEVAPP	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP	PROCEDURE	✓	1
18-09-2025 19:15:00	DELETE	AUD	OMEGACAEVAPP	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	2
18-09-2025 19:15:00	DELETE	AUD	OMEGACAEVDEV1	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	1
18-09-2025 19:15:00	EXECUTE	AUD	OMEGACAEVDEV1	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	1
18-09-2025 19:15:00	INSERT	AUD	OMEGACAEVDEV1	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	2
18-09-2025 19:15:00	LOGON	ACC	NT Service\SQLSERVERAGENT	UB1-03-01-00003				✓	3
18-09-2025 19:15:00	LOGON	ACC	OMEGACAEVAPP	UB1-03-01-00003				✓	10
18-09-2025 19:15:00	LOGON	ACC	OMEGACAEVDEV1	UB1-03-01-00003				✓	10
18-09-2025 19:15:00	SELECT	AUD	OMEGACAEVDEV1	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	29
18-09-2025 19:15:00	UPDATE	AUD	OMEGACAEVAPP	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	4
18-09-2025 19:15:00	UPDATE	AUD	OMEGACAEVDEV1	UB1-03-01-00003	OmegaCA_Benchmark	OMEGACAEVAPP		✓	3
									673

Use the Export… button to export the summary dataset in different file formats - txt, xls, html and xml.
Use the Mark button to invoke the form "Security Events - Mark" to perform retrieved records marking.

3.1.5 Security Events

When the Security Events are searched in Record mode, the first tab Security Events displays security events at record-level, with fields of top importance.



Security Events Last search on 9/18/2025 8:08:06 PM. DateTime range 18-09-2025 00:00:00 - 18-09-2025 23:59:59

Security Events | Event Details

Drag a column header here to group by that column

Audit DateTime	Server Login	DB User	Session Id	Policy Ty	Action Name	DB Name	Schema Name	Object Name	Object Type	Host Name	Client IP	Class Typ
2025-09-18 19:10:50.6375374	OMEGACAEVAPP	OMEGACAEVAPP	56	AUD	UPDATE	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:51.1757475	OMEGACAEVAPP	OMEGACAEVAPP	56	AUD	DELETE	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:51.7190182	OMEGACAEVAPP	OMEGACAEVAPP	56	AUD	ALTER	OmegaCA_Benchmark	OMEGACAEVAPP	P_EMP_INS		UB1-03-01-00003	192.168.20.152	P
2025-09-18 19:10:51.7190182	OMEGACAEVAPP	OMEGACAEVAPP	56	AUD	ALTER	OmegaCA_Benchmark	OMEGACAEVAPP	P_EMP_INS		UB1-03-01-00003	192.168.20.152	P
2025-09-18 19:10:51.8333333	OMEGACAEVAPP		56	RTP-DDL	ALTER_PROCEDURE	OmegaCA_Benchmark	OMEGACAEVAPP	P_EMP_INS	PROCEDURE	UB1-03-01-00003	192.168.20.152	
2025-09-18 19:10:52.9333333	OMEGACAEVDEV1		56	ACC	LOGON					UB1-03-01-00003	192.168.20.152	
2025-09-18 19:10:53.4981085	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	INSERT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:54.0166783	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:54.0316350	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:54.5593468	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:54.5593468	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	UPDATE	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:55.0835542	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:55.0835542	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	DELETE	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:55.6098616	OMEGACAEVDEV1	OMEGACAEVDEV1	56	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:55.6233333	OMEGACAEVDEV1		64	ACC	LOGON					UB1-03-01-00003	192.168.20.152	
2025-09-18 19:10:55.6299315	OMEGACAEVDEV1	OMEGACAEVDEV1	64	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:55.6299315	OMEGACAEVDEV1	OMEGACAEVDEV1	64	AUD	SELECT	OmegaCA_Benchmark	OMEGACAEVAPP	EMP		UB1-03-01-00003	192.168.20.152	U
2025-09-18 19:10:55.6466667	OMEGACAEVDEV1		64	ACC	LOGON					UB1-03-01-00003	192.168.20.152	

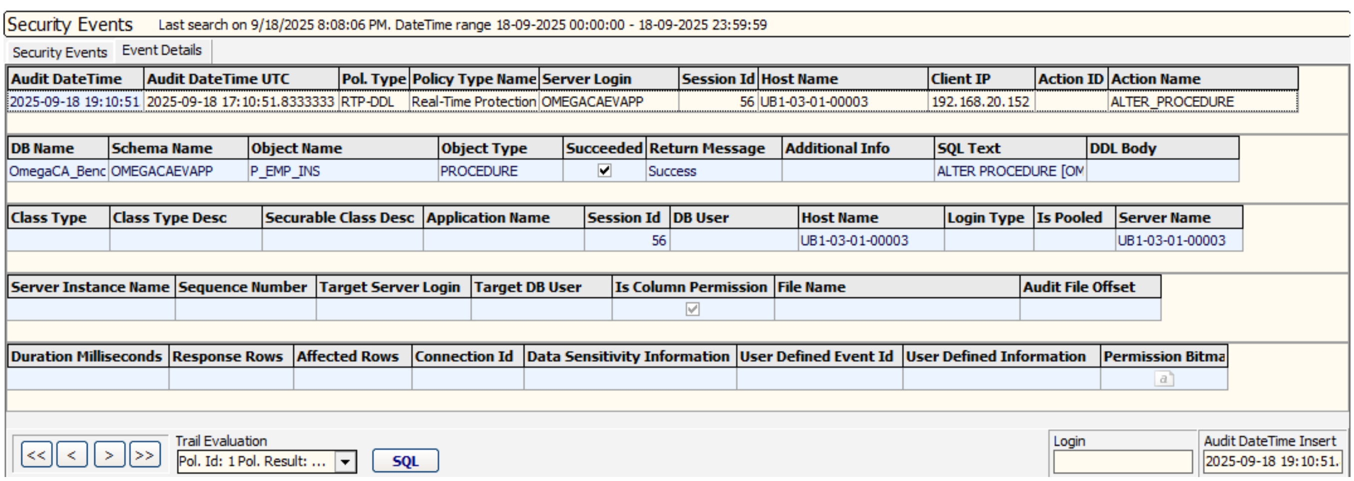
Rec No = 693

Export...

Use the Export… button to export the summary dataset in different file formats - txt, xls, html and xml.

3.1.6 Event Details

The second tab Event Details displays an individual full view of the record selected in the first tab Security Events.



Security Events Last search on 9/18/2025 8:08:06 PM. DateTime range 18-09-2025 00:00:00 - 18-09-2025 23:59:59

Security Events | Event Details

Audit DateTime	Audit DateTime UTC	Pol. Type	Policy Type Name	Server Login	Session Id	Host Name	Client IP	Action ID	Action Name
2025-09-18 19:10:51	2025-09-18 17:10:51.8333333	RTP-DDL	Real-Time Protection	OMEGACAEVAPP	56	UB1-03-01-00003	192.168.20.152		ALTER_PROCEDURE

DB Name	Schema Name	Object Name	Object Type	Succeeded	Return Message	Additional Info	SQL Text	DDL Body
OmegaCA_Benc	OMEGACAEVAPP	P_EMP_INS	PROCEDURE	☑	Success		ALTER PROCEDURE [OM	

Class Type	Class Type Desc	Securable Class Desc	Application Name	Session Id	DB User	Host Name	Login Type	Is Pooled	Server Name
				56		UB1-03-01-00003			UB1-03-01-00003

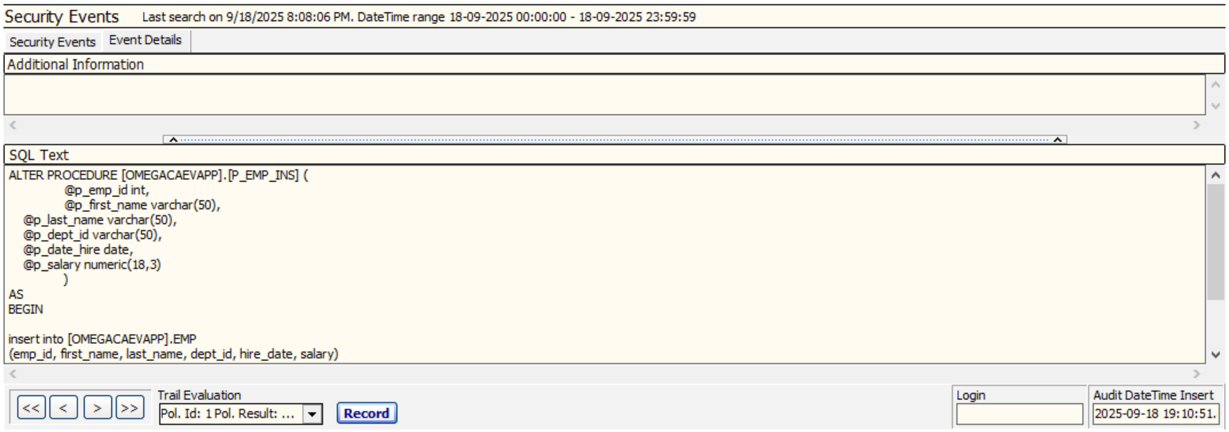
Server Instance Name	Sequence Number	Target Server Login	Target DB User	Is Column Permission	File Name	Audit File Offset
				☑		

Duration Milliseconds	Response Rows	Affected Rows	Connection Id	Data Sensitivity Information	User Defined Event Id	User Defined Information	Permission Bitma

<< < > >> Trail Evaluation Pol. Id: 1 Pol. Result: ... SQL Login Audit DateTime Insert 2025-09-18 19:10:51.

Use the navigation buttons bottom-left to navigate the records dataset opened in the first tab; and to display in full the currently selected in this one.

Press the SQL button to display in full Additional Information and SQL Text fields. Press it again (this time labeled Records) to switch back to full record Detail presentation.



3.2 Security Events Trail fields

The following are the most important fields of the Security Events trail in Omega Core Audit application:

Field Name	Field Description
Row ID	Unique ID of the record. Primary Key.
Audit DateTime	Timestamp of the audit event. This field is indexed
Audit UTC	Universal Time Coordinated of the Security Event.
Audit DateTime Ins	Timestamp of the record insert in the Security Events trail.
Sequence Number	Sequence of records
Action Id	Id of the audited action
Action Name	Name of the audited action
Succeeded	User's action status: 1 = success 0 = fail
Return Message	Details of the User's action status
Permission Bitmask	Permissions that were grant, denied, or revoked
Is Column Permission	Is a column level permission: 1 = true 0 = false
Session Id	ID of the session
Server Principal Id	ID of the login context
Database Principal Id	ID of the database user context
Target Server Principal Id	Server principal ID on which GRANT/DENY/REVOKE is performed
Target Database Principal Id	Database principal ID on which GRANT/DENY/REVOKE is performed
Object Id	Id of the object
Class Type	Audit type
Session Server Principal Name	Identity of the original login
Server Principal Name	Current login
Server Principal SID	Current login security identifier (SID)
Database Principal Name	Database current user
Target Server Principal Name	Target login of action
Target Server Principal SID	SID of target login.
Target Database Principal Name	Target database user of action
Server Instance Name	Name of the server instance
Database Name	Database context in which the action occurred
Schema Name	Schema context in which the action occurred
Object Name	Name of the object on which action occurred
SQL Text (Statement)	SQL text of the action
Additional Information	Additional information for the action
File Name	The path and name of the audit log file
Audit File Offset	Buffer offset in the audit file
User Defined Event Id	User defined event ID
User Defined Information	Extra information added by user writing audit log via sp_audit_write
Transaction Id	Id of the transaction
Client IP	IP of the client's machine
Application Name	Name of the client's application
Duration Milliseconds	Execution duration in milliseconds
Response Rows	Number of rows returned in the result

Affected Rows	Number of rows affected by the statement
Connection Id	ID of the connection in the server
Data Sensitivity Information	Information types and sensitivity labels of the classified columns
Host Name	Host Name of the client's machine
Policy Type Id	Id of the policy type
Policy Type Code	Code of the policy type
Policy Type Name	Name of the policy type
Server Name	Name of the server's machine
Login Type	Type of the server login
IS_POOLED	Instance number 0 – not pooled 1 – pooled
Trail Eval.	Policies related to this trail record
Object Type	Type of the object on which action is performed
Class Type Desc.	Type of the action's class
Securable Class Desc.	Type of the securable class
DDL Body	T-SQL body of the object after the DDL action

Note

A field receives value from one or more modules, but not (in every case) by all of them.

3.3 Automatic MS SQL Server Audit Trail Management

The Access Control and Real-Time Protection DDL Security Event records are written (in real-time) directly into the Omega Core Audit Repository, table Security Events (OMEGACA.SYS_UNF_TRAIL).

The Audit records are initially written (in real-time) into the MS SQL Server audit files as defined in the used Server Audit[s].

The retrieval of audit records from the MS SQL server audit files to Omega Core Audit Security Events Trail is done by the "DB Audit Trails Collect" job that runs periodically (every 60 seconds by default on install).
The OMEGACA_TRANS Scheduler job is installed by the installation script and is managed by the Omega Core Audit application, in the form System Components.

Obviously the OmegaCoreAudit database and its objects are subjects to common both routine and/or instant DBA and OS maintenance tasks, as any other application inside the MS SQL Server; including the purging of "old" records according to your needs when size grows.

Refer to Omega Core Audit Deployment Guide, topic "5.2 Engine and Repository Maintenance" for more details on the above.

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 MS SQL Server "on logon" trigger 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. In short: the Access Control Module features a Database Firewall, and is working from inside it - as the last resort.

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, and terminal names, IP addresses, program used, time and many more.

Access control security events provide details on user's logon activity into the system. An access control security event is generated depending on the settings of the evaluated policies and results of TRUE/FALSE. Evaluation of multiple policies by a login action generates a single access control security event.

A specific feature of the Access Control comparing to other modules is that an access control security event is always generated if no policy authorizes. You will always have an access control security event for a non-complying logging!

Protection

When the Access Control module has been set in non-Silent Mode, and no Access Control policy has been evaluated to TRUE, the end user's LOGON will fail will the message:

"Logon failed for login '<login_name>' due to trigger execution"

4.1.1 Access Control for MS SQL Connections

The "MS SQL Internals" policy is installed by default and establishes a secure logon channel for the following MS SQL internal logins:

- NT Service\MSSQLSERVER
- NT SERVICE\SQLSERVERAGENT
- NT SERVICE\SQLTELEMETRY
- NT SERVICE\SQLWriter
- sa

You must activate this policy before setting the Access Control module to non-Silent (protective) mode!

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 MS SQL 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.
- Use the Users Apply option of the policy's User Appliance and declare users to the respective list.
- Enable the Use Cache option for all policies.
- Disable the Debug Log option for all policies.
- Beware 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, independently to the result of policies evaluation.

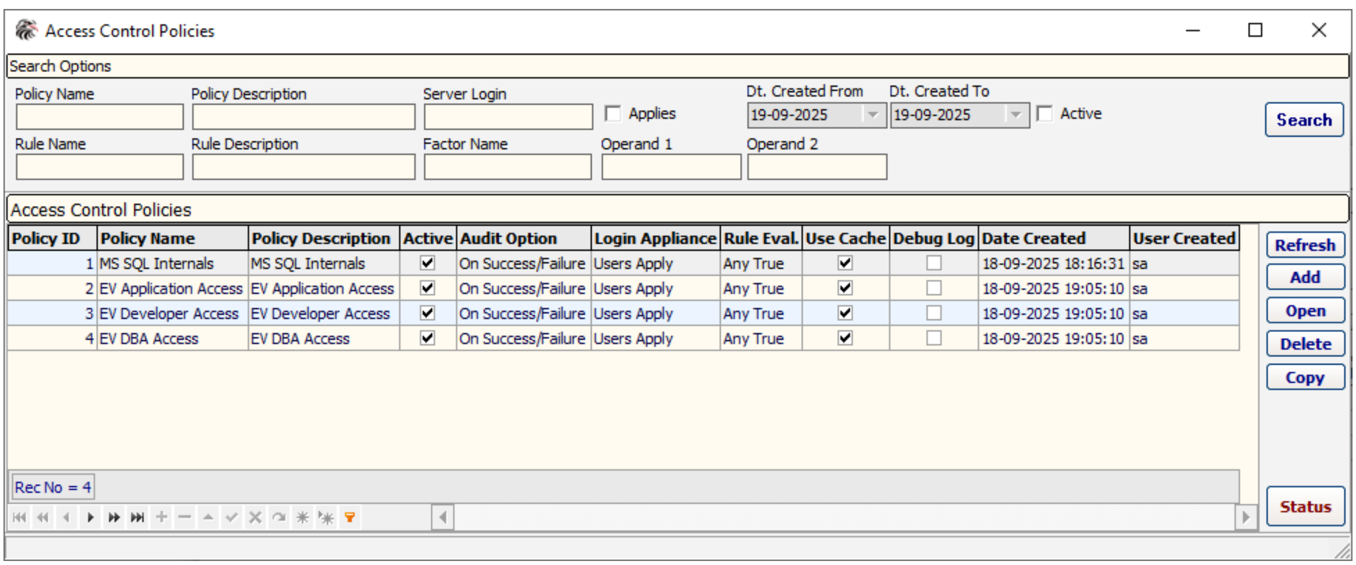
The Access Control Silent mode is enabled by default on Omega Core Audit install. Use the Silent mode for database access behavior discovery (retaining the audit capability), until you establish secured access paths for all logging accounts to the database through your policies. Mind the database internal actions, like those of MS SQL accounts, 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.

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.



Search Options

- All search options are available as case-free and (optional) partial value.
- When Checkbox Applies is checked, the search will return all policies that apply for the login. The later must be entered in full and is case-sensitive.
- Operand 1 will also search for the Operand's value in IN/NOT IN Condition's list.

The following are the properties of the Access Control policy:

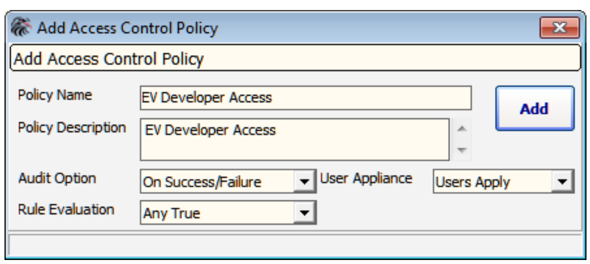
Field Name	Field Description
Policy ID	Unique identifier of the policy
Policy Name	Unique Name of the policy within the module.

Policy Description	Description of the policy.
Active	Policy status, Active or Inactive.
Audit Option	Security event generation. Available options: Disabled No Access Control security event is created. On Failure Access Control security event is created on a FALSE Policy. On Success and Failure Access Control security event is always created.
Login Appliance	Policy appliance regarding server logins. Available options: All Users Policy is applied to all logins. Users Apply Policy is applied only to logins in the Logins Apply List. Users Exclude Policy is not applied to logins in the Logins 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 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.

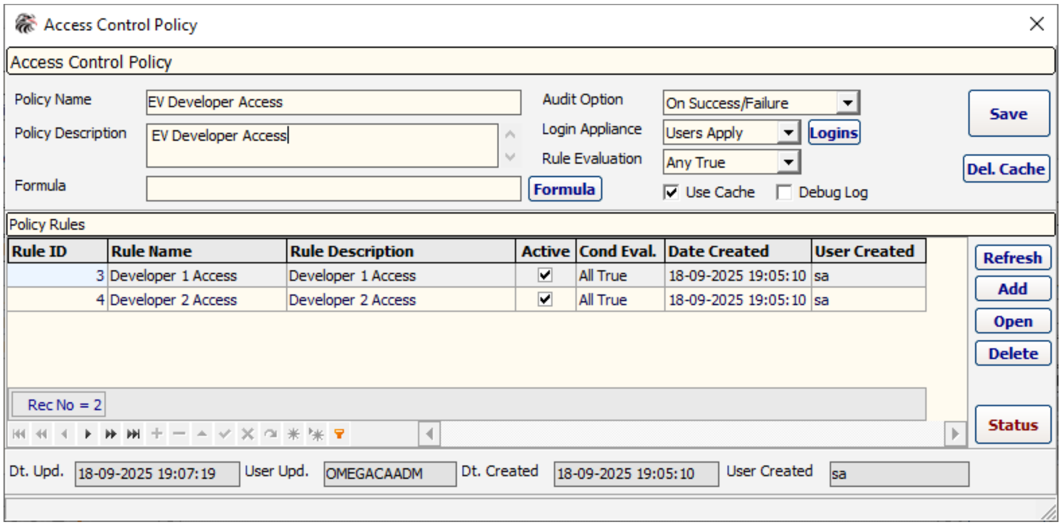


Set the required fields and press the button Add.

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.



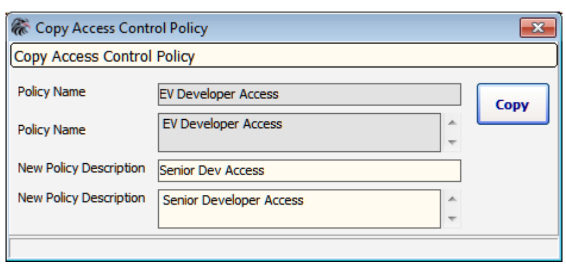
To update any policy changes press the button Save. You will receive a confirmation, or the error message when failure.
Press the button Del. Cache to manually clear the access control cache for this policy. Press the button Formula to open the policy's formula editor form. Press the button Users to 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.



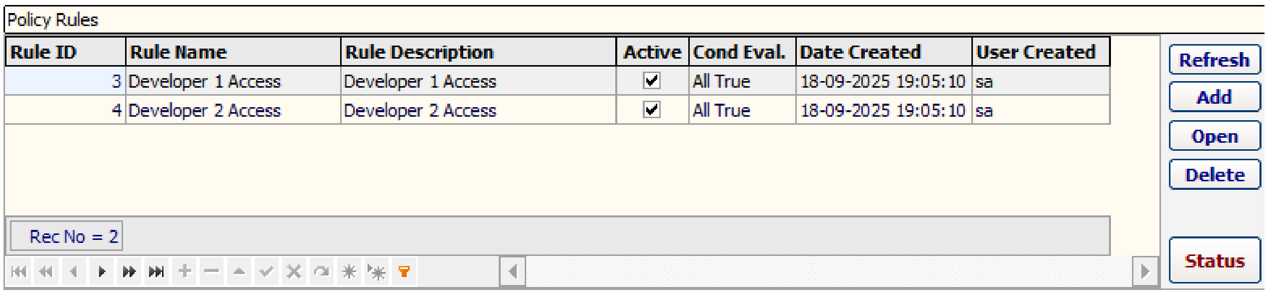
Set the required fields and press the button Copy. You will receive a confirmation, or the error message when failure. The new policy will be created with its rules, conditions, [not] IN lists as the original policy and with an Inactive status.

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.



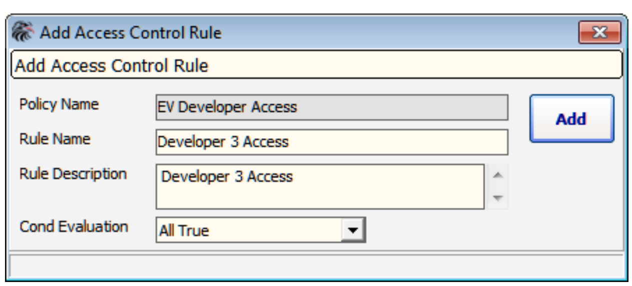
The following are the properties of the Access Control rule:

Field Name	Field Description
Rule Id	Unique identifier of the rule
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.

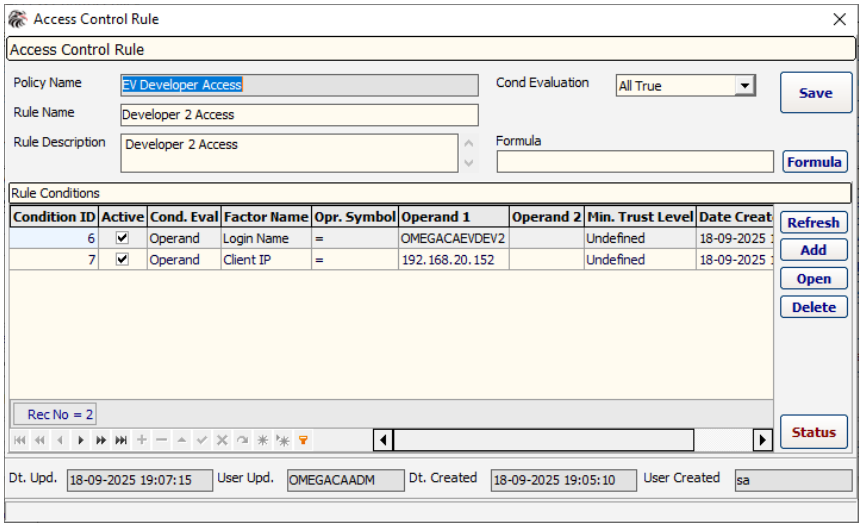


Set the required fields and press the button Add.

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.



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.

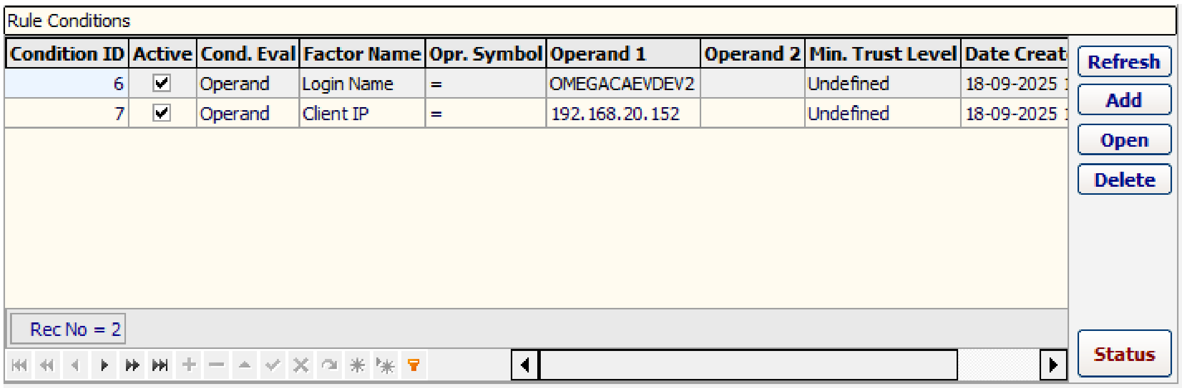
You will receive a confirmation, or the error message when failure.

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.



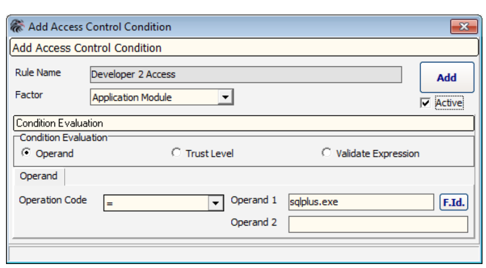
The following are the properties of the Access Control condition:

Field Name	Field Description
Condition ID	Unique identifier of the condition
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 a user-defined database function returning a Boolean result.
Factor	Factor being evaluated
Operation Symbol	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.

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.

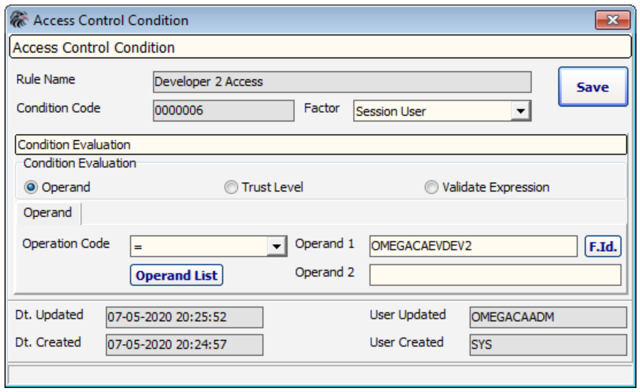


Set the required fields and press the button Add.

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: Audit

5.1 How it works

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

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 MS SQL native audit features, is easily configured and graphically enables a complex set of auditing commands via the interface. Auditing in MS SQL Server is done at two levels:

- Server level – auditing commands at server and databases
- Database level – auditing commands on individual databases

Automatic MS SQL audit trails management is effective. The DB Audit Trails Collect Job reads the audited events from the files stored into the dedicated OS directory and loads them to the Omega Core Audit Repository.

Note

Omega Core Audit supports only audit of type FL (FILE). In case of multiple Server Audits, they must write to the same OS directory, as the DB Audit Trails Collect Job looks into a single (configurable) OS directory only!

5.2 Audit Guidelines

Standard Auditing is relatively inexpensive, as demonstrated by audit benchmark tests performed by Microsoft and other third parties. However in order to minimize any possible performance impact and to keep the Security Events Trail from growing big too quickly, narrow the scope of the audit by referring sensitive objects in combination with the important permissions.

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 security information with your ability to store and process it.

Create audits for important statements [permissions] 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 MS SQL Audits

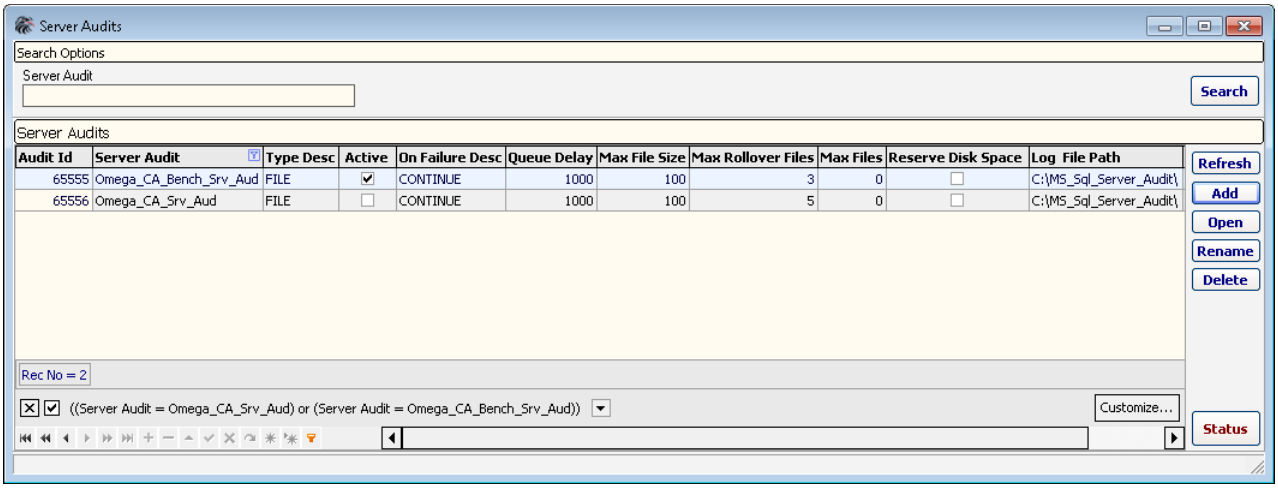
Existing (Standard) audit settings might be enabled in your database, prior to Omega Core Audit installation.

These audits are supported by Omega Core Audit as long as they:

- Are of type FILE
- Write into the same OS directory

5.4 Server Audits

The Server Audit determines the location of the audit events. To view the server audits, in the Application's main menu Audit Policies, tab Audit click the menu button Server Audits. This will open the Server Audits form.



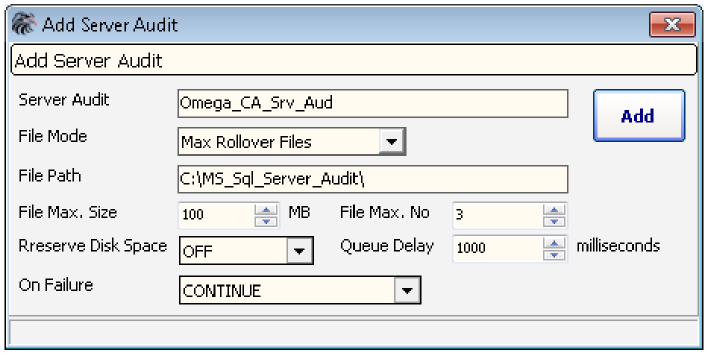
The following are the properties of an Audit Server

Field Name	Field Description
Audit Id	ID of the audit
Server Audit	Name of the audit
Type Description	Audit type description
Active	Server audit status, Active or Inactive.
On Failure Description	On Failure (audit event cannot be written) condition: CONTINUE – continues operation FAIL OPERATION – fail action SHUTDOWN – shutdowns the server instance
Queue Delay	Maximum time in milliseconds before writing to disk. On 0, an audit write will guarantee before the event can continue
Max. File Size	Maximum size, in megabytes, of the audit
Max. Rollover Files	Maximum number of files to use with the rollover option
Max. Files	Maximum number of files to use without the rollover option.
Reserve Disk Space	Amount of disk space to reserve per file. ON/OFF
Log File Path	Path to where audit is located.

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

5.4.1 Adding a new Server Audit

To create a new server audit, in the form Server Audits, Server Audits grid, press the button Add on the right. The form Add Server Audit will open.



The File Mode can be Max. Rollover Files (the suggested one) and Max Files.

Note:

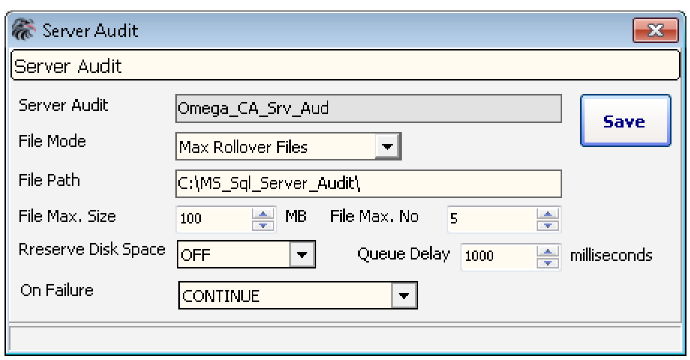
The SHUTDOWN server permission has been explicitly denied to role OMEGACA_ADMIN on install. To use the SHUTDOWN at On Failure this Deny must first be revoked!

Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new server audit will be created with an Inactive status.

5.4.2 Opening/modifying a Server Audit

To open a server audit in full details for viewing and modification, select a server audit record in the form Server Audits, Server Audits grid and press the button Open on the right. The form Server Audit will open.



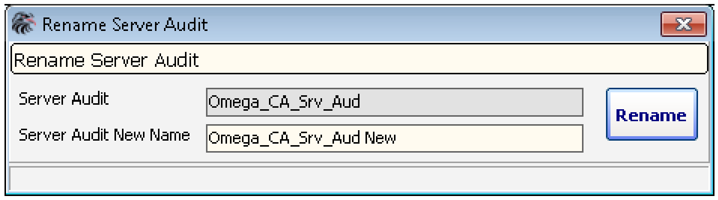
To update any server audit changes press the button Save.
You will receive a confirmation, or the error message when failure.

5.4.3 Deleting a Server Audit

To delete a server audit, select a server audit record in the form Server Audits, Server Audits grid and press button Delete on the right.
You will receive a confirmation, or the error message when failure.

5.4.4 Renaming a Server Audit

To rename a server audit in full details for viewing and modification, select a server audit record in the form Server Audits, Server Audits grid and press the button Rename on the right. The form Rename Server Audit will open.



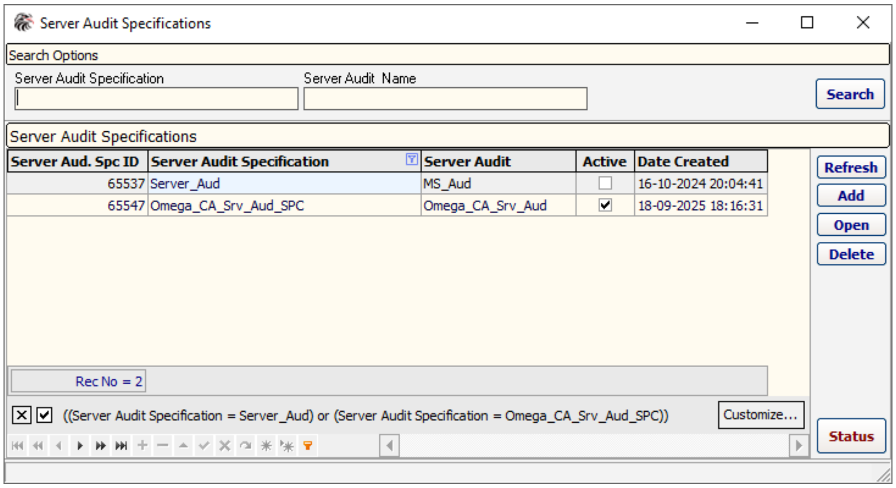
To rename the server audit enter the new name and press the button Save.
You will receive a confirmation, or the error message when failure.

5.4.5 Server Audit Status

To change a server audit status, select a server audit record in the form Server Audits, Server Audits grid and press the button Status below on the right. If the change status dialog box is confirmed the current server audit status will be reversed from its current setting.

5.5 Server Audit Specifications

Server Audit Specification is a collection of server-level audit options. To view the server audit specifications, in the Application's main menu Audit Policies, tab Audit, click the menu button Server Audit Specifications. This will open the Server Audit Specifications form.



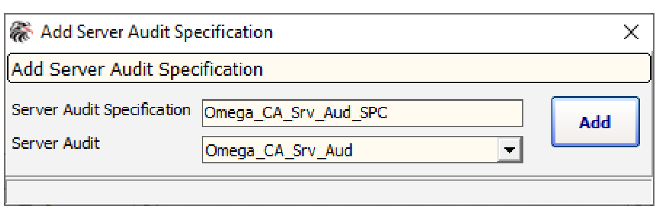
The following are the properties of the Server Audit Specification:

Field Name	Field Description
Server Audit Spc. ID	Unique identifier of the server audit specification
Server Audit Specification	Name of the server audit specification
Server Audit	Server Audit to which the Specification is bound
Active	Server audit specification status, Active or Inactive

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

5.5.1 Adding a new Server Audit Specification

To create a new server audit specification, in the form Server Audit Specifications, Server Audit Specifications grid, press the button Add on the right. The form Add Server Audit Specification will open.



Set the required fields and press the button Add.

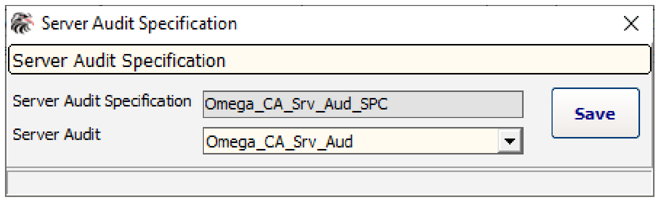
You will receive a confirmation, or the error message when failure. The new server audit specification will be created with an Inactive status.

Note:

You can create only one server audit specification bound to a server audit. If you need a new one, you must create a new server audit for it.

5.5.2 Opening/modifying a Server Audit Specification

To open a server audit specification in full details for viewing and modification, select a server audit specification record in the form Server Audit Specifications, Server Audit Specifications grid and press the button Open on the right. The form Server Audit Specification will open.



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

5.5.3 Deleting a Server Audit Specification

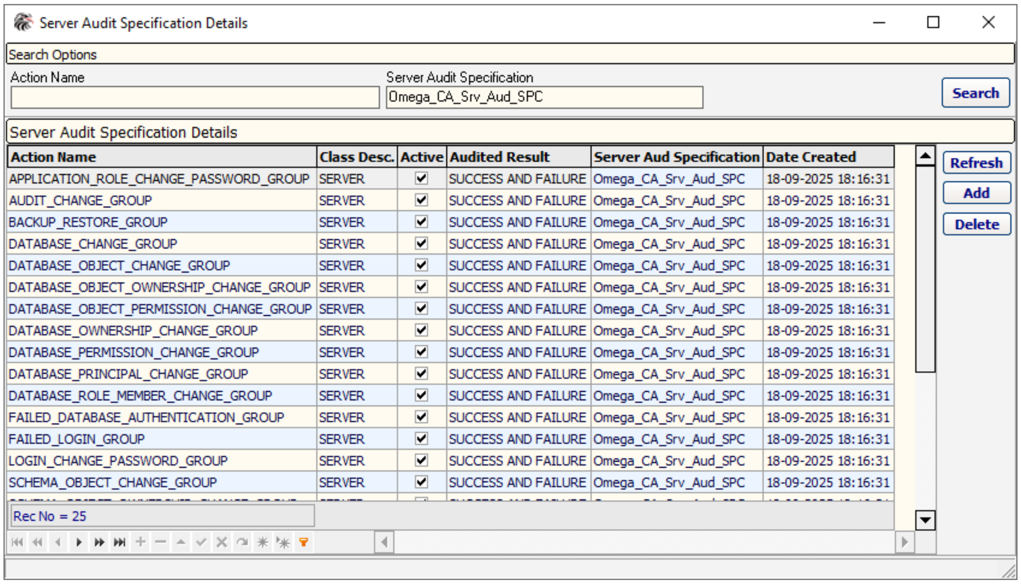
To delete a server audit specification, select a server audit specification record in the form Server Audit Specifications, Server Audit Specifications grid and press button Delete on the right. If the delete dialog box is confirmed, the selected server audit specification will be deleted.
You will receive a confirmation, or the error message when failure.

5.5.4 Server Audit Specification Status

To change a server audit specification status, select a server audit record in the form Server Audit Specifications, Server Audit Specifications grid and press the button Status below on the right. If the change status dialog box is confirmed the current server audit specification status will be reversed from its current setting.

5.6 Server Audit Specification Details

Server Audit Specification Details are the audit options set on server-level. To view the server audit specification details, in the Application's main menu Audit Policies, tab Audit, click the menu button Server Audit Spc. Details. This will open the Server Audit Specifications Details form.



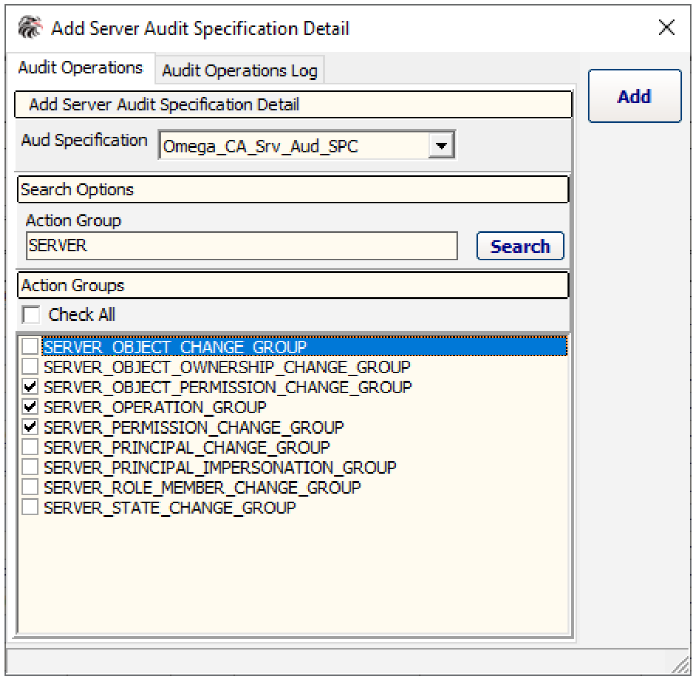
The following are the properties of the Server Audit Specification Detail:

Field Name	Field Description
Action Name	Name of group or name of audit action
Class Description	Description of action's class
Active	Server audit specification status, Active or Inactive
Audited Result	Audited result: SUCCESS AND FAILURE SUCCESS FAILURE
Server Aud. Specification	Name of the Server audit specification to which the detail is bound

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

5.6.1 Adding Server Audit Specification Details

To create a new server audit specification detail, in the form Server Audit Specification Detail, Server Audit Specification Details grid, press the button Add on the right. The form Add Server Audit Specification Detail will open.



Select the (Server) Audit Specification in the combo-box, search the Action Groups and check the desired options, and press the button Add.

The command confirmations, or the error message when failure, are displayed at tab Audit Operations Log.

Note:

You cannot add a detail to an enabled server audit specification. Disable the later first!

5.6.2 Deleting a Server Audit Specification Detail

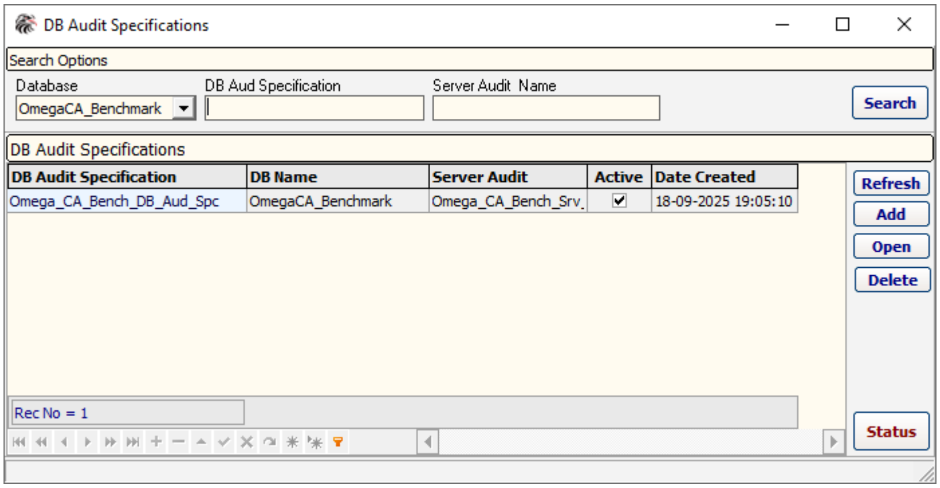
To delete a server audit specification detail, select a server audit specification detail record in the form Server Audit Specification Detail, Server Audit Specification Details grid and press button Delete on the right. If the delete dialog box is confirmed, the selected server audit specification detail will be deleted.
You will receive a confirmation, or the error message when failure.

Note:

You cannot delete the detail of an enabled server audit specification. Disable the later first!

5.7 Database Audit Specifications

Database Audit Specification is a collection of database-level audit options. To view the database audit specifications, in the Application's main menu Audit Policies, tab Audit, click the menu button DB Audit Specifications. This will open the DB Audit Specifications form.



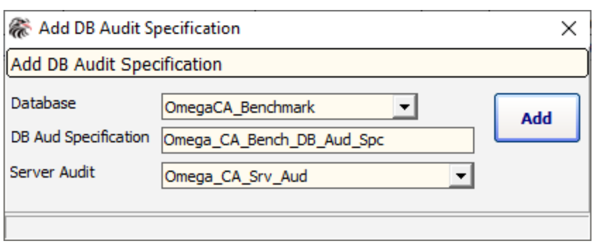
The following are the properties of the Database Audit Specification:

Field Name	Field Description
DB Audit Specification	Name of the database audit specification
DB Name	Name of the database
Server Audit	Server Audit to which the Specification is bound
Active	Database audit specification status, Active or Inactive

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

5.7.1 Adding a new Database Audit Specification

To create a new database audit specification, in the form DB Audit Specifications, DB Audit Specifications grid, press the button Add on the right. The form Add DB Audit Specification will open.



Set the required fields and press the button Add.

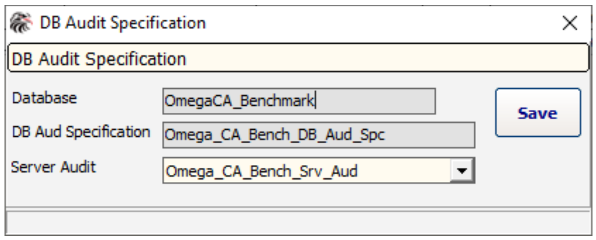
You will receive a confirmation, or the error message when failure. The new database audit specification will be created with an Inactive status.

Note:

You can create only one database audit specification bound to a server audit within the same database. If you need a new one, you must create a new server audit for it.

5.7.2 Opening/modifying a Database Audit Specification

To open a database audit specification in full details for viewing and modification, select a database audit specification record in the form DB Audit Specifications, DB Audit Specifications grid and press the button Open on the right. The form DB Audit Specification will open.



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

5.7.3 Deleting a Database Audit Specification

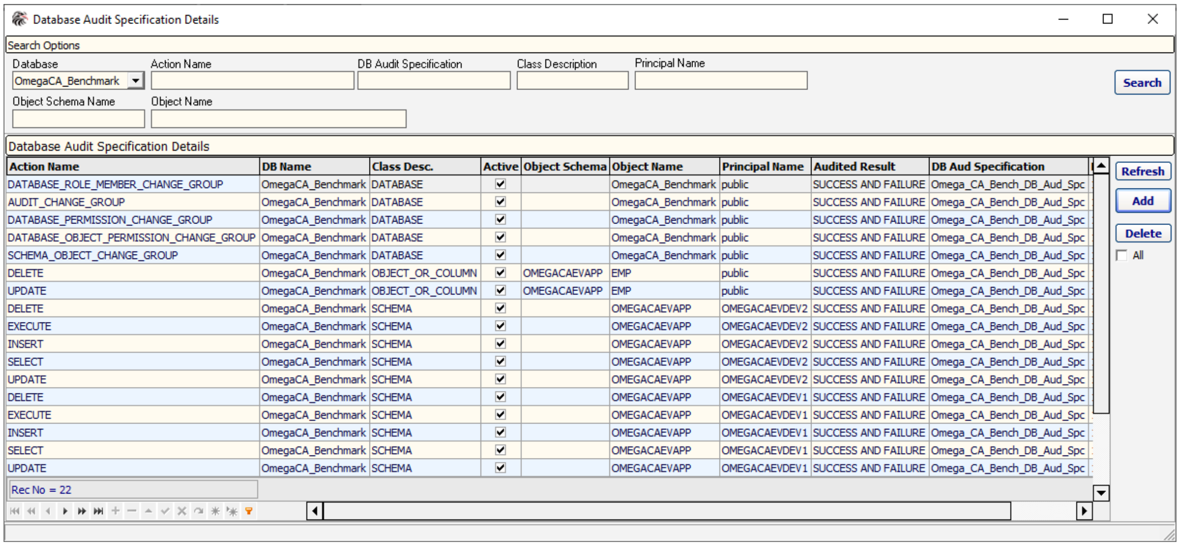
To delete a database audit specification, select a database audit specification record in the form DB Audit Specifications, DB Audit Specifications grid and press button Delete on the right. If the delete dialog box is confirmed, the selected database audit specification will be deleted.
You will receive a confirmation, or the error message when failure.

5.7.4 Database Audit Specification Status

To change a database audit specification status, select a database audit record in the form DB Audit Specifications, DB Audit Specifications grid and press the button Status below on the right. If the change status dialog box is confirmed the current database audit specification status will be reversed from its current setting.

5.8 Database Audit Specification Details

Database Audit Specification Details are the audit options set on database-level. To view the database audit specification details, in the Application's main menu Audit Policies, tab Audit, click the menu button DB Audit Spc. Details. This will open the Database Audit Specifications Details form.



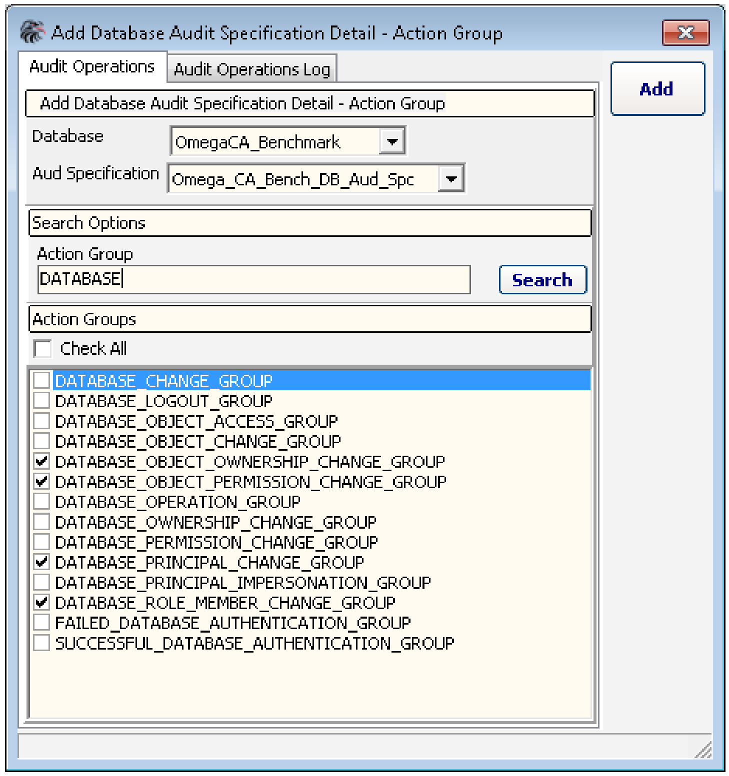
The following are the properties of the Database Audit Specification Detail:

Field Name	Field Description
Action Name	Name of group or name of audit action
DB Name	Name of the database
Class Description	Description of action's class
Active	Server audit specification status, Active or Inactive
Object Schema	Schema owner of the object
Object Name	Name of the object
Principal Name	Name of the database principal
Audited Result	Audited result: SUCCESS AND FAILURE SUCCESS FAILURE
DB Aud. Specification	Name of the database audit specification to which the detail is bound

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

5.8.1 Adding a new Database Audit Specification Detail – Action Group

To create a new database audit specification detail for action groups, in the form Database Audit Specification Details, Database Audit Specification Details grid, press the button Add on the right, and click on the Action Group menu. The form Add Database Audit Specification Detail – Action Group will open.



Set the Database Name and Database Audit Specification. Search the action groups and check the ones to audit. Press the button Add.

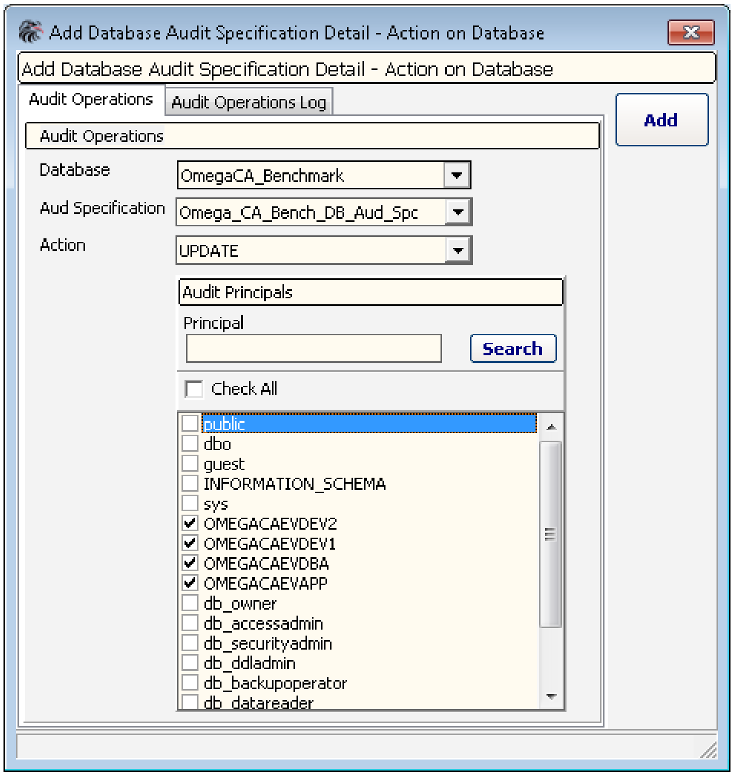
The command confirmations, or the error message when failure, are displayed at tab Audit Operations Log.

Note:

You cannot add a detail to an enabled database audit specification. Disable the later first!

5.8.2 Adding a new Database Audit Specification Detail – Action on Database

To create a new database audit specification detail for actions on databases, in the form Database Audit Specification Details, Database Audit Specification Details grid, press the button Add on the right, and click on the Actions on Database menu. The form Add Database Audit Specification Detail – Action on Database will open.



Set the Database Name, Database Audit Specification and the audited Action. Search the database principals and check the ones to audit. Press the button Add.

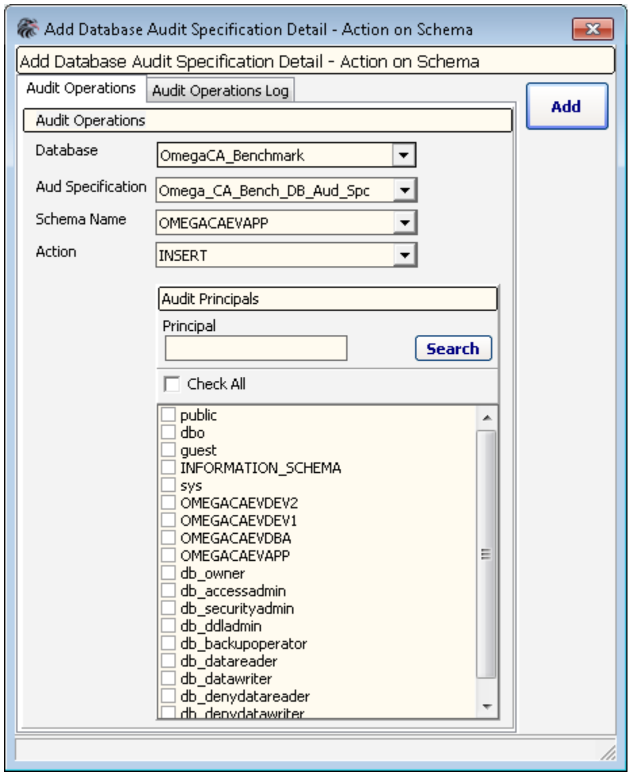
The command confirmations, or the error message when failure, are displayed at tab Audit Operations Log.

Note:

Auditing the public principal means auditing all principals!

5.8.3 Adding a new Database Audit Specification Detail – Action on Schema

To create a new database audit specification detail for actions on schemas, in the form Database Audit Specification Details, Database Audit Specification Details grid, press the button Add on the right, and click on the Actions on Schema menu. The form Add Database Audit Specification Detail – Action on Schema will open.

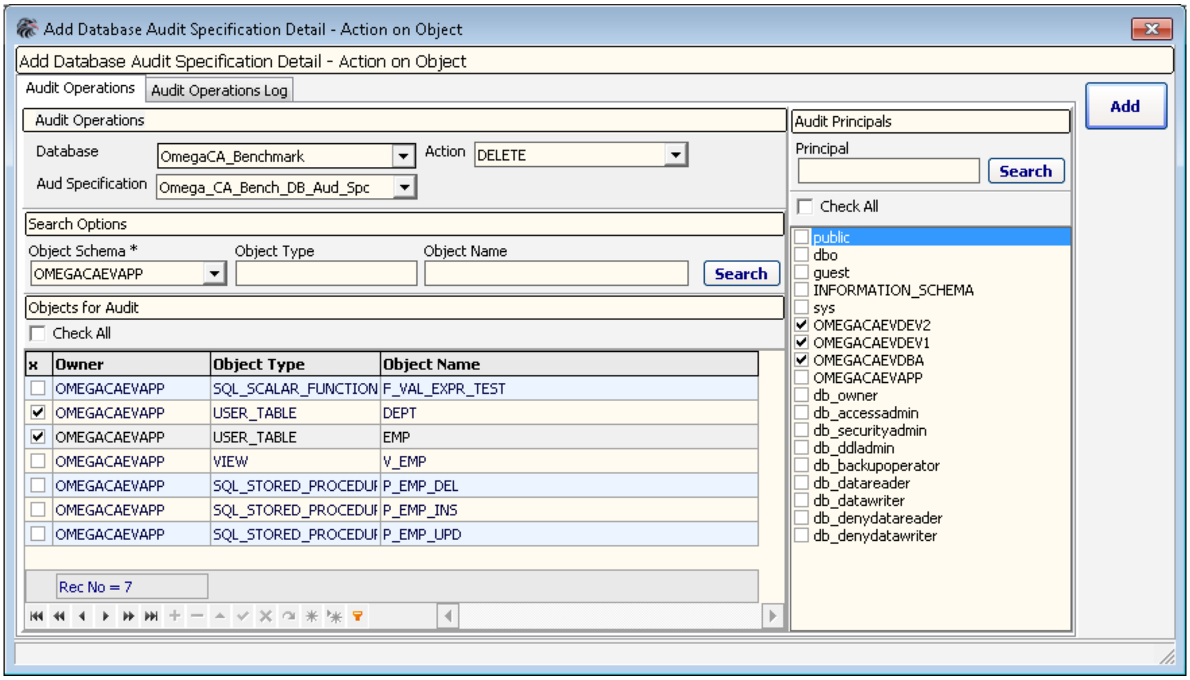


Set the Database Name, Database Audit Specification, Schema Name and the audited Action. Search the database principals and check the ones to audit. Press the button Add.

The command confirmations, or the error message when failure, are displayed at tab Audit Operations Log.

5.8.4 Adding a new Database Audit Specification Detail – Action on Object

To create a new database audit specification detail for actions on objects, in the form Database Audit Specification Details, Database Audit Specification Details grid, press the button Add on the right, and click on the Actions on Object menu. The form Add Database Audit Specification Detail – Action on Object will open.



Set the Database Name, Database Audit Specification, and the audited Action. Search the database objects and check the ones to audit. Search the database principals and check the ones to audit. Press the button Add.

The command confirmations, or the error message when failure, are displayed at tab Audit Operations Log.

5.8.5 Deleting a Database Audit Specification Detail

To delete a database audit specification detail, select a database audit specification detail record in the form Database Audit Specification Details, Database Audit Specification Details grid and press button Delete on the right. If the delete dialog box is confirmed, the selected database audit specification detail will be deleted.
You will receive a confirmation, or the error message when failure.

Note:

You cannot delete the detail of an enabled database audit specification. Disable the later first!

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 MS SQL server (change management). It operates on top of MS SQL Server DDL event trigger 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.

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 database name, schema, 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, and terminal names, IP addresses, client identifier, program used, time and many more.

Real-time protection DDL security events provide details on user's DDL activity into the system. A real-time protection DDL security event is generated depending on the settings of the evaluated policies and results of TRUE/FALSE. Evaluation of multiple policies by a DDL action generates one single real-time protection DDL security event.

Protection

When the Real-Time Protection DDL policy has been set in non-Silent Mode, and the policy has been evaluated to FALSE, the end user's DDL action will fail will the message:

"DDL Policy non-compliance!"

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 Security Events Trail.

Area Reminder:

If Area is not defined the policy will not be evaluated!

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, independently to the result of policies evaluation.

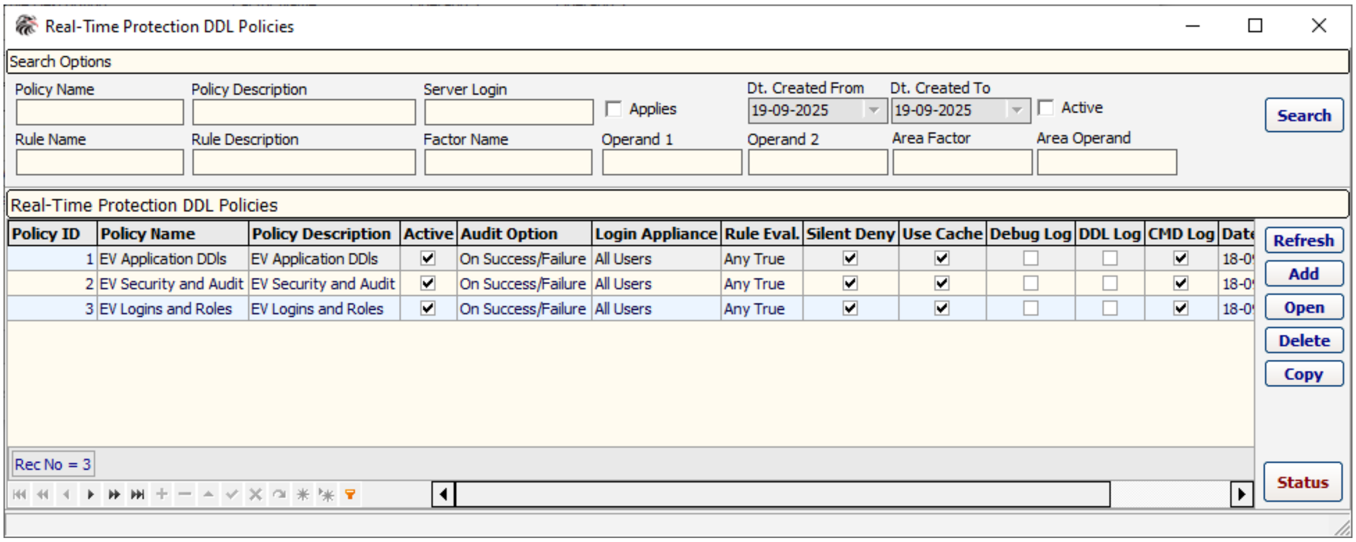
The RTP DDL Policy's Silent Deny mode is enabled by default on each new policy. Use the Silent Deny mode for database DDL behavior discovery (retaining the audit capability), until you establish secured access paths for DDLs affecting your defined Security Areas through your policies. Mind the MS SQL Server internal actions, 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.



Search Options

- All search options are available as case-free and (optional) partial value.
- When Checkbox Applies is checked, the search will return all policies that apply for the login. The later must be entered in full and is case-sensitive.
- Operand 1 will also search for the Operand's value in IN/NOT IN Condition's list.

The following are the properties of the RTP DDL policy:

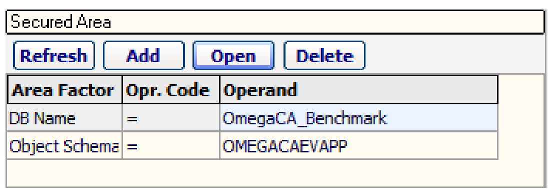
Field Name	Field Description
Policy ID	Unique identifier of the policy
Policy Name	Unique Name of the policy within the module.
Policy Description	Description of the policy.
Active	Policy Active or Inactive.
Audit Option	Security Events generation. Available options: Disabled — No RTP-DDL Security Event is created. On Failure — RTP-DDL Security Event is created on a FALSE Policy. On Success and Failure — RTP-DDL Security Event is always created.
Login Appliance	Policy appliance regarding server logins. Available options: All Users — Policy is applied to all logins. Users Apply — Policy is applied only to logins in the Logins Apply List. Users Exclude — Policy is not applied to logins in the Logins 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 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:

Database Name Secured area's database

Object Owner Secured area's object owner.

Object Type Secured area's object type. For example:
TABLE, FUNCTION, INDEX, PROCEDURE …

Object Name Secured area's object name.

Action (Event) Secured area's DDL action (event). One of the following:
CREATE_TABLE, CREATE_INDEX, CREATE_PROCEDURE, GRANT_DATABASE, DENY_DATABASE, REVOKE_DATABASE, LOGIN, ROLE ALTER_DATABASE_AUDIT_SPECIFICATION …

The Secured Area is managed after the creation of the policy.

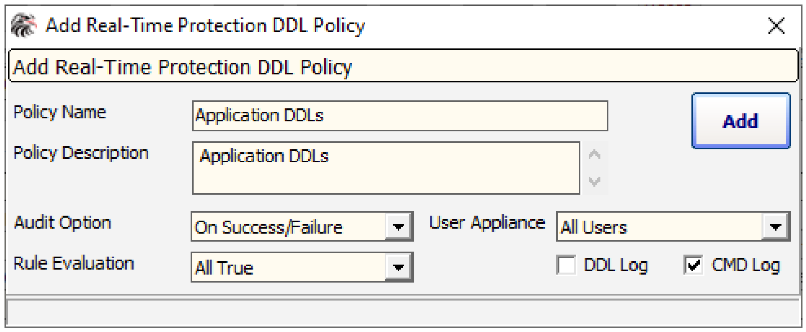
Note:

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, or as a closing mark. To satisfy possible long IN/NOT IN lists, operand's maximum length has been set to 2200 characters.

Manage them with the buttons on top of the factors grid

6.3.2 Adding a new Real-Time Protection DDL Policy

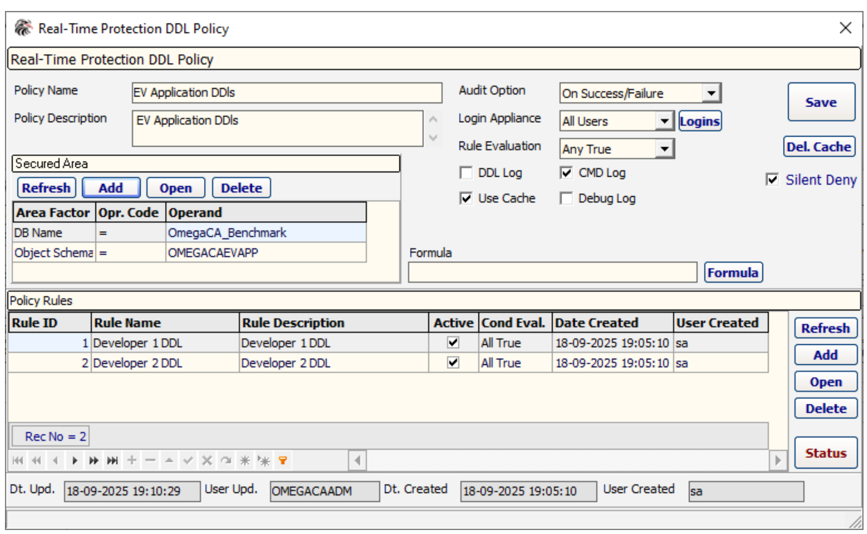
To create a new real-time protection DDL policy, in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid, press the button Add on the right. The form Add Real-Time Protection DDL Policy will open.



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.



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.

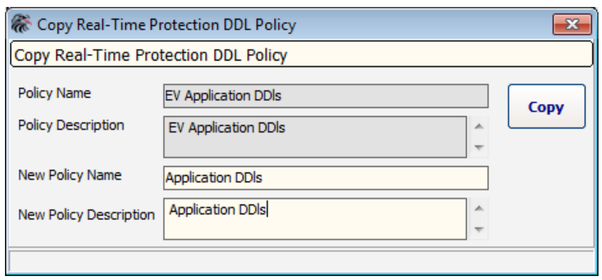
6.3.4 Deleting a Real-Time Protection DDL Policy

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.

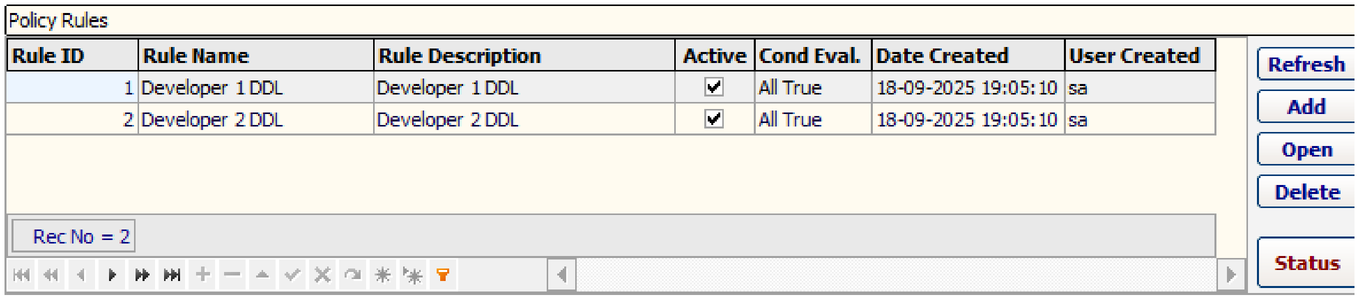
You will receive a confirmation, or the error message when failure. The new policy will be created with its rules, conditions, [not] IN lists as the original policy and with an Inactive status.

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 then 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.



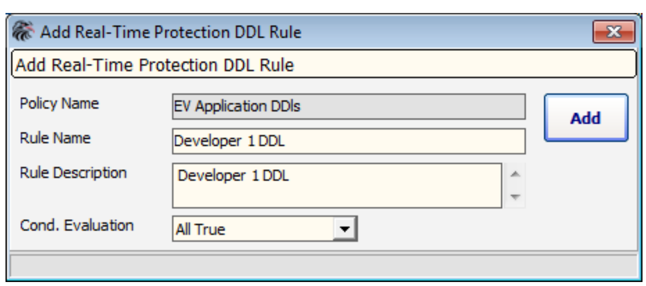
The following are the properties of the RTP DDL rule:

Field Name	Field Description
Rule ID	Unique identifier of the rule.
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. Form Add Real-Time Protection DDL Rule will open.

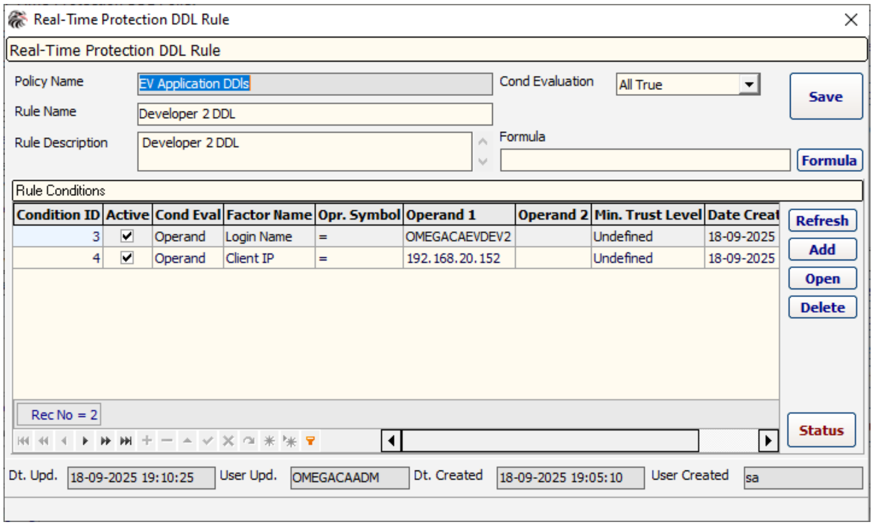


Set the required fields and press the button Add.

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.



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.

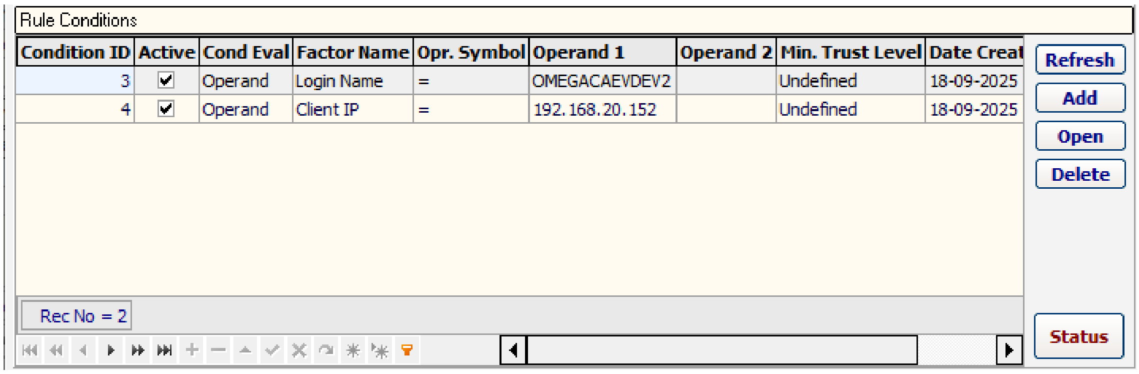
You will receive a confirmation, or the error message when failure.

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.



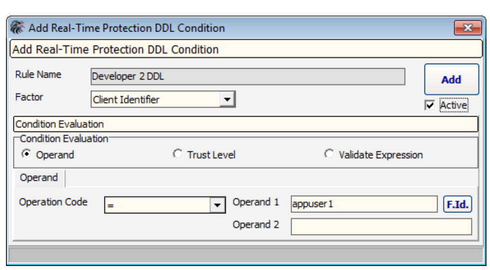
The following are the properties of the RTP DDL condition:

Field Name	Field Description
Condition ID	Unique identifier of the condition.
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 a user-defined database function returning a Boolean result.
Factor	Factor being evaluated.
Operation Symbol	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.

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.

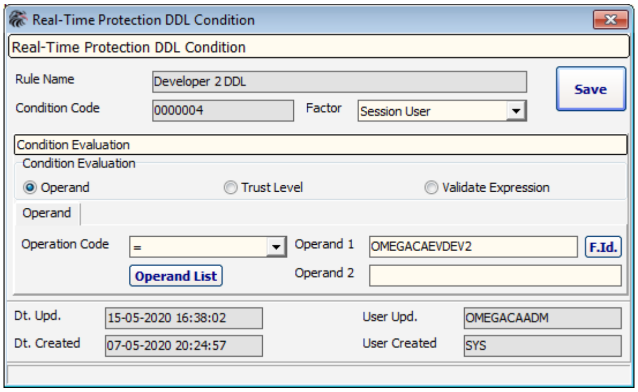


Set the required fields and press the button Add.

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.

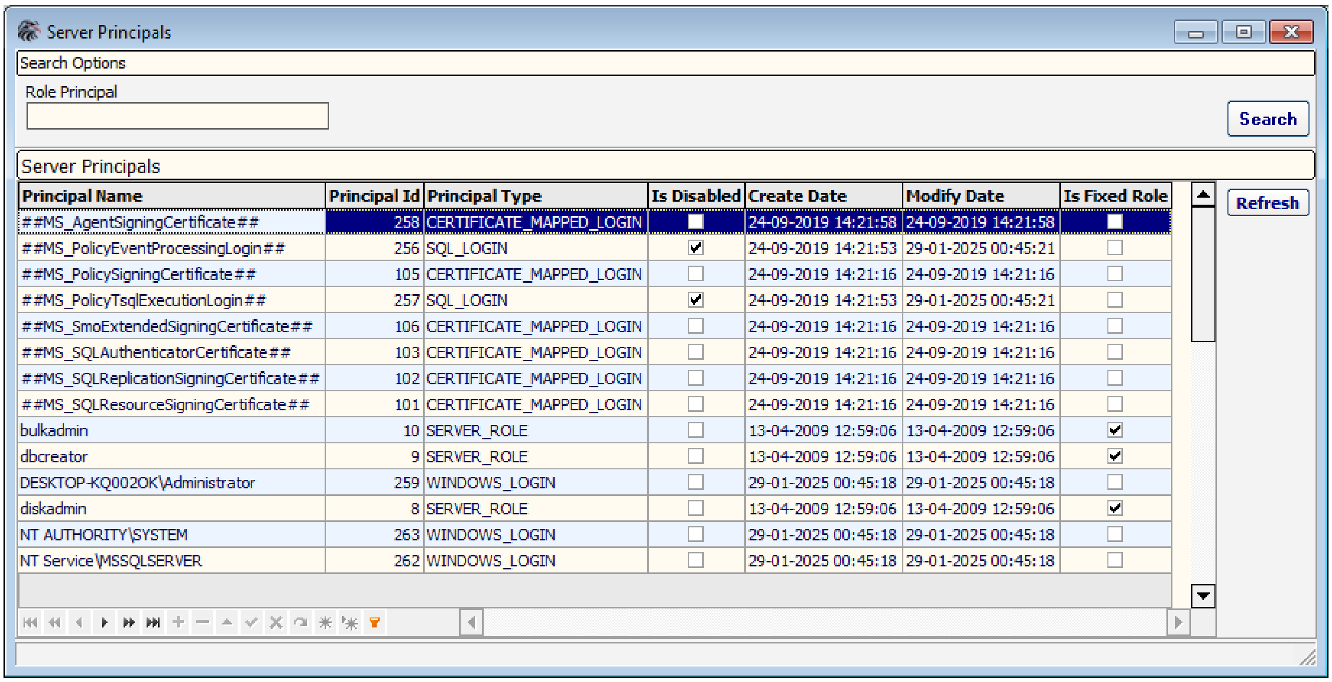
7 CHAPTER 7: Security Management

The Security module shows basic security on principals and permissions for server and databases.

7.1 Server Security

7.1.1 Server Principals

To view the server principals, in the Application's main menu Security, tab Server click the menu button Server Principals. This will open the Server Principals form.



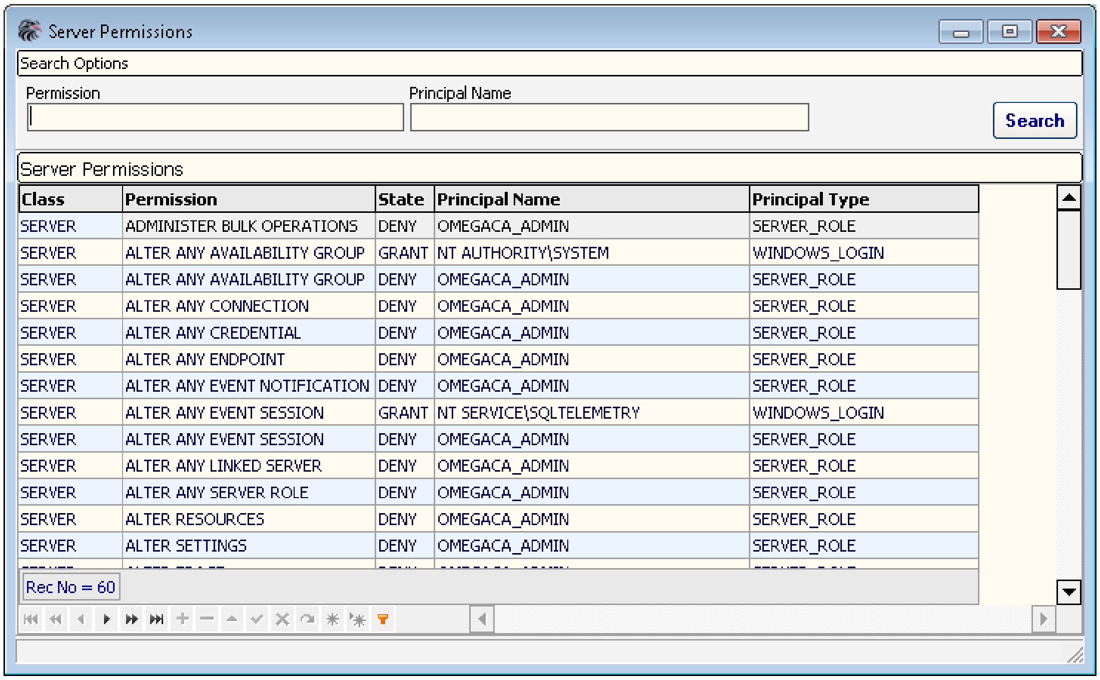
The following are the properties of the server principals:

Field Name	Field Description
Principal Name	Name of the principal
Principal Id	Numeric ID of the principal
Principal Type	Type of the principal
Is Disabled	Disabled status of the principal
Create Date	Date creation of the principal
Modify Date	Date last modify of the principal
Is Fixed Role	if the principal is a built-in server role with fixed permissions

Press the Refresh button to refresh them.

7.1.2 Server Permissions

To view the server permissions, in the Application's main menu Security, tab Server click the menu button Server Permissions. This will open the Server Permissions form.



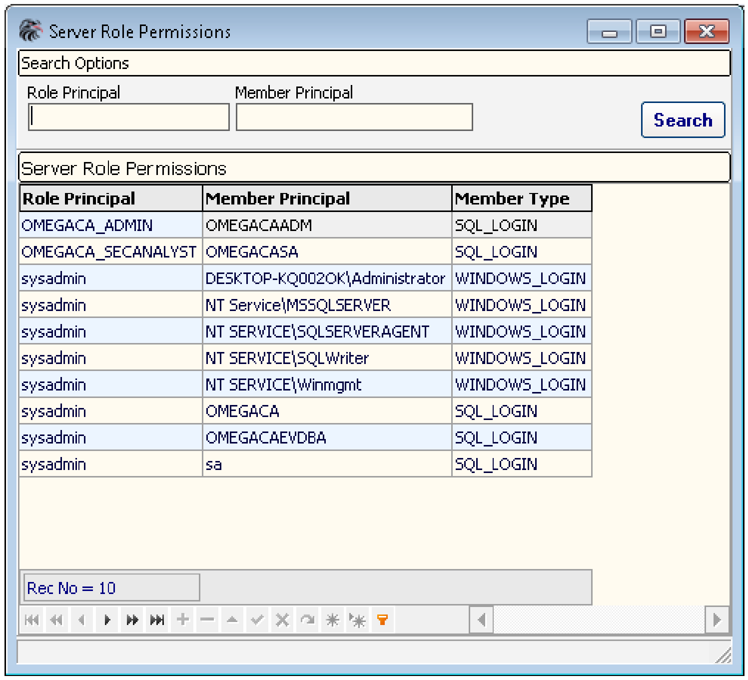
The following are the properties of the server permissions:

Field Name	Field Description
Class	Permission class
Permission	Permission name
State	Permission state. Options: DENY REVOKE GRANT GRANT_WITH_GRANT_OPTION
Principal Name	Principal grantee name
Principal Type	Principal grantee type

Press the Refresh button to refresh them.

7.1.3 Server Roles Permissions

To view the server role permissions, in the Application's main menu Security, tab Server click the menu button Server Role Permissions. This will open the Server Role Permissions form.



The following are the properties of the server role permissions:

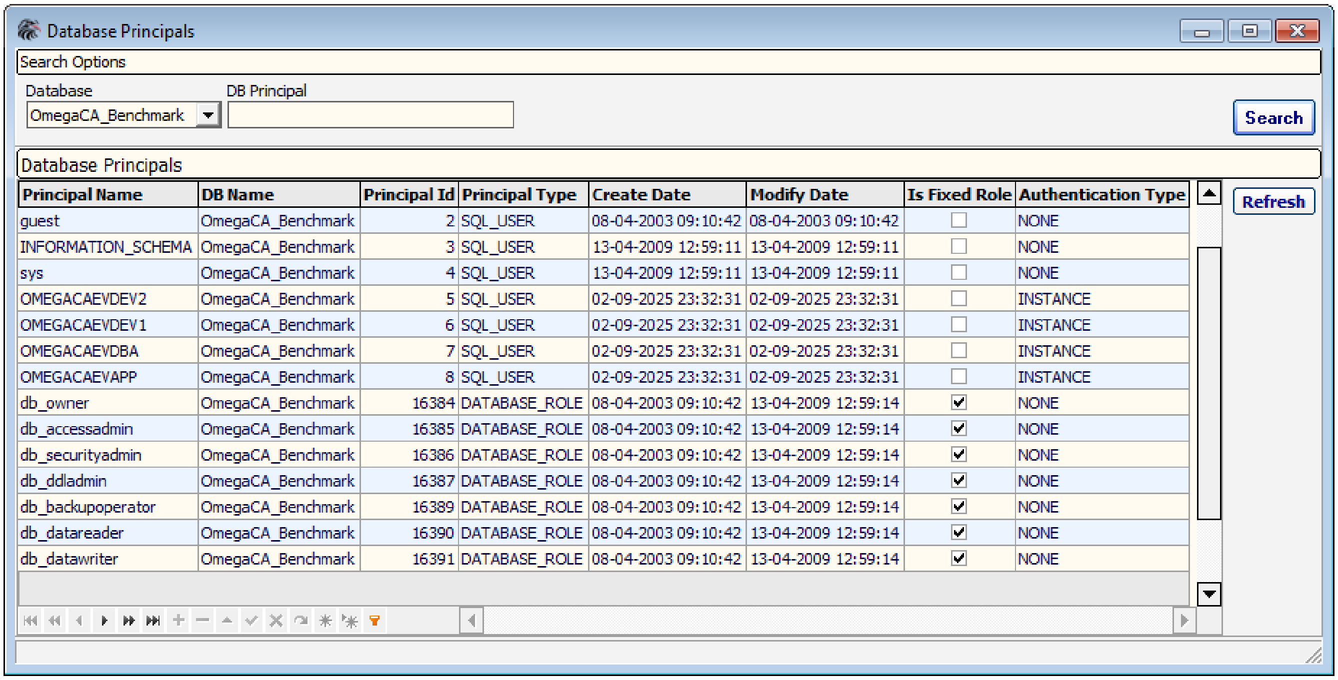
Field Name	Field Description
Role Principal	Role Principal granted
Member Principal	Principal grantee
Member Type	Principal grantee type

Press the Refresh button to refresh them.

7.2 Database Security

7.2.1 Database Principals

To view the database principals, in the Application's main menu Security, tab Database click the menu button Database Principals. This will open the Database Principals form.



Principal Name	DB Name	Principal Id	Principal Type	Create Date	Modify Date	Is Fixed Role	Authentication Type
guest	OmegaCA_Benchmark	2	SQL_USER	08-04-2003 09:10:42	08-04-2003 09:10:42	☐	NONE
INFORMATION_SCHEMA	OmegaCA_Benchmark	3	SQL_USER	13-04-2009 12:59:11	13-04-2009 12:59:11	☐	NONE
sys	OmegaCA_Benchmark	4	SQL_USER	13-04-2009 12:59:11	13-04-2009 12:59:11	☐	NONE
OMEGACAEVDEV2	OmegaCA_Benchmark	5	SQL_USER	02-09-2025 23:32:31	02-09-2025 23:32:31	☐	INSTANCE
OMEGACAEVDEV1	OmegaCA_Benchmark	6	SQL_USER	02-09-2025 23:32:31	02-09-2025 23:32:31	☐	INSTANCE
OMEGACAEVDBA	OmegaCA_Benchmark	7	SQL_USER	02-09-2025 23:32:31	02-09-2025 23:32:31	☐	INSTANCE
OMEGACAEVAPP	OmegaCA_Benchmark	8	SQL_USER	02-09-2025 23:32:31	02-09-2025 23:32:31	☐	INSTANCE
db_owner	OmegaCA_Benchmark	16384	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE
db_accessadmin	OmegaCA_Benchmark	16385	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE
db_securityadmin	OmegaCA_Benchmark	16386	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE
db_ddladmin	OmegaCA_Benchmark	16387	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE
db_backupoperator	OmegaCA_Benchmark	16389	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE
db_datareader	OmegaCA_Benchmark	16390	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE
db_datawriter	OmegaCA_Benchmark	16391	DATABASE_ROLE	08-04-2003 09:10:42	13-04-2009 12:59:14	☑	NONE

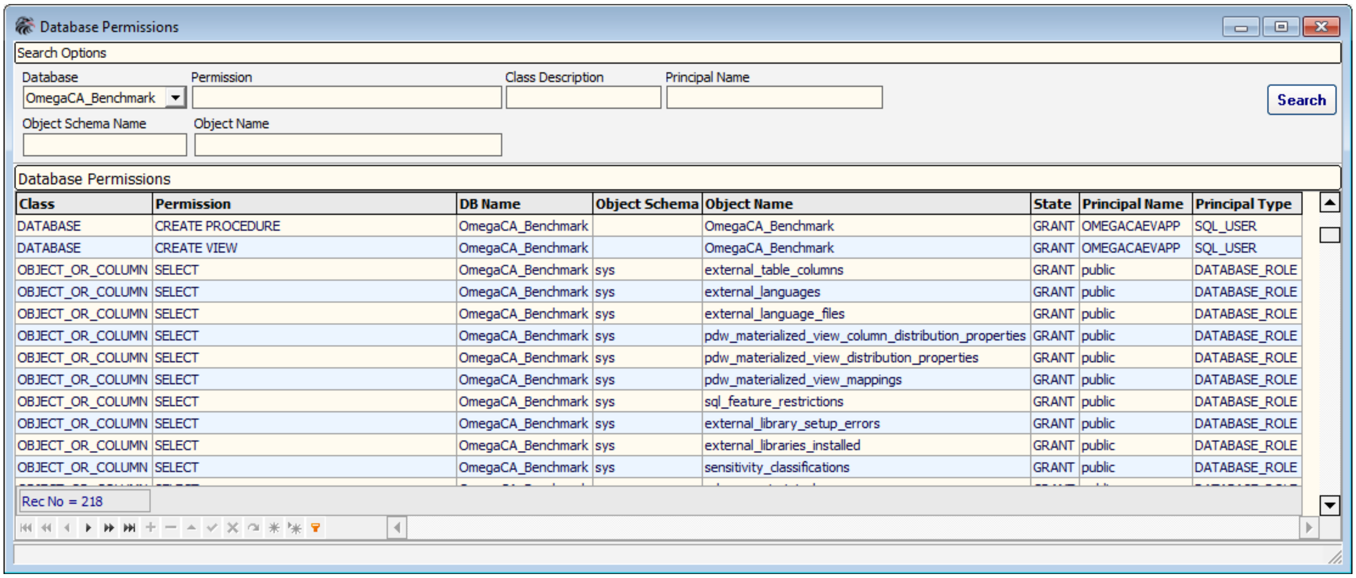
The following are the properties of the database principals:

Field Name	Field Description
Principal Name	Name of the principal
DB Name	Name of the database
Principal Id	Numeric ID of the principal
Principal Type	Type of the principal
Create Date	Date creation of the principal
Modify Date	Date last modify of the principal
Is Fixed Role	if the principal is a built-in database role
Authentication Type	Description of the authentication type

Press the Refresh button to refresh them.

7.2.2 Database Permissions

To view the database permissions, in the Application's main menu Security, tab Database click the menu button Database Permissions. This will open the Database Permissions form.



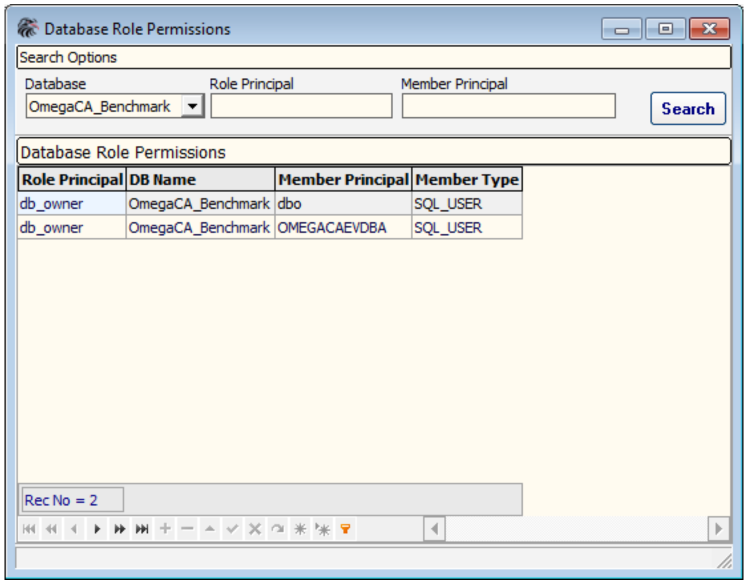
The following are the properties of the database permissions:

Field Name	Field Description
Class	Permission class
Permission	Permission name
DB Name	Name of the database
Object Schema	Object schema owner name
Object Name	Object name
State	Permission state. Options: DENY REVOKE GRANT GRANT_WITH_GRANT_OPTION
Principal Name	Principal grantee name
Principal Type	Principal grantee type

Press the Refresh button to refresh them.

7.2.3 Database Roles Permissions

To view the database role permissions, in the Application's main menu Security, tab Database click the menu button Database Role Permissions. This will open the Database Role Permissions form.



The following are the properties of the database role permissions:

Field Name	Field Description
Role Principal	Role Principal granted
DB Name	Name of the database
Member Principal	Principal grantee
Member Type	Principal grantee type

Press the Refresh button to refresh them.

8 CHAPTER 8: System Administration

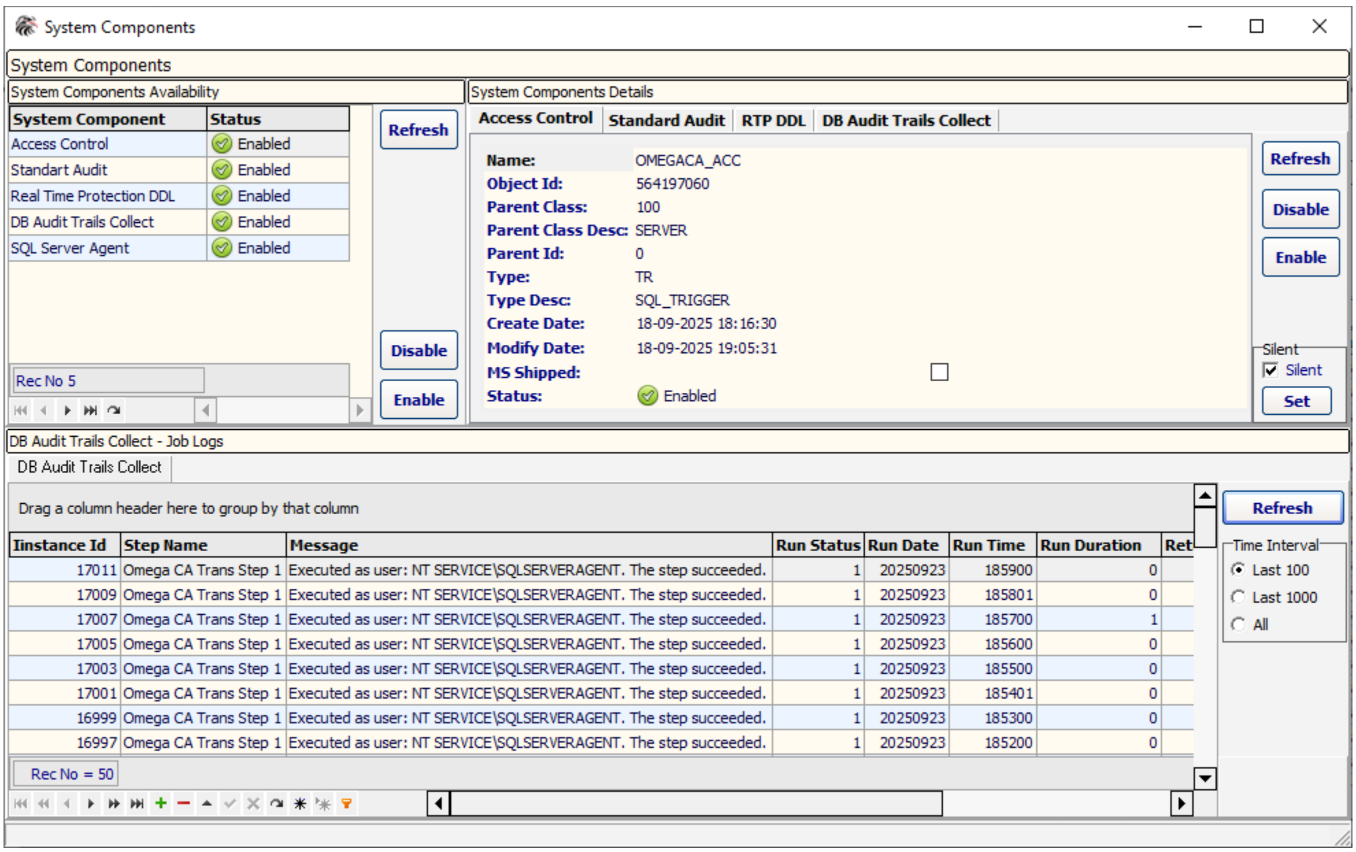
The System Administration module handles the management of core system functionalities and module availability, enabling the Omega Core Audit administrators to easily and quickly complete their tasks.

The managed functionalities are:

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

8.1 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.



Core modules and components availability is displayed in the System Components Availability grid.

The main Omega Core Audit system components and functionalities managed in this form are:

1. Access Control - Access Control module.
2. Standard Audit - MS SQL server audits availability.
3. Real Time Protection DDL - Real Time Protection DDL module.
4. DB Audit Trails Collect Job - Audit events collection job from OS dir to Repository.
5. SQL Server Agent - monitored only; not managed.

Press the Refresh button to refresh all of them.

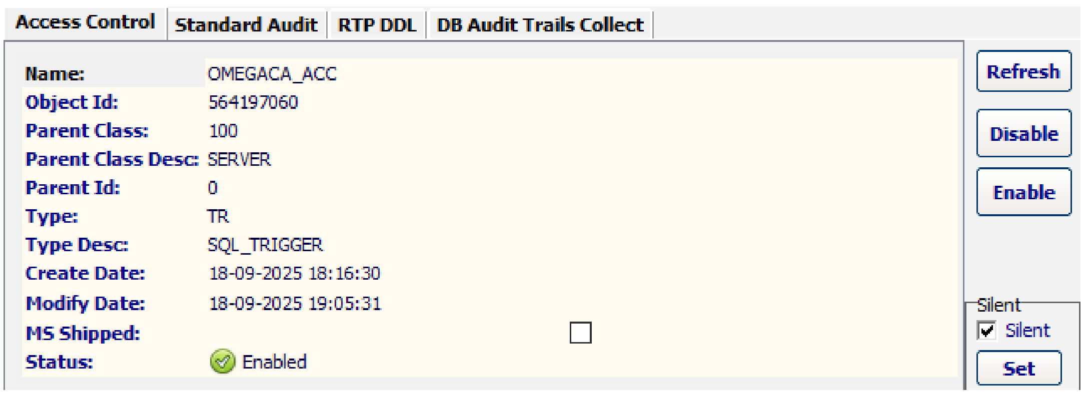
Use buttons Enable / Disable to respectively enable or disable:

- Access Control - Access control module.
- Standard Audit - MS SQL Server Audits.
- Real Time Protection DDL - Real Time Protection DDL module.
- DB Audit Trails Collect Job - Audit events collection job.

Detailed specific information for each of the above is presented in the respective tabs of the tab group System Components Details. Double click each record of System Components Availability grid to focus on the respective tab.

8.1.1 Access Control

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



In this Card View on the left you can see the details of the OMEGACA_ACC server-level FOR LOGON trigger that implements the Access Control module.

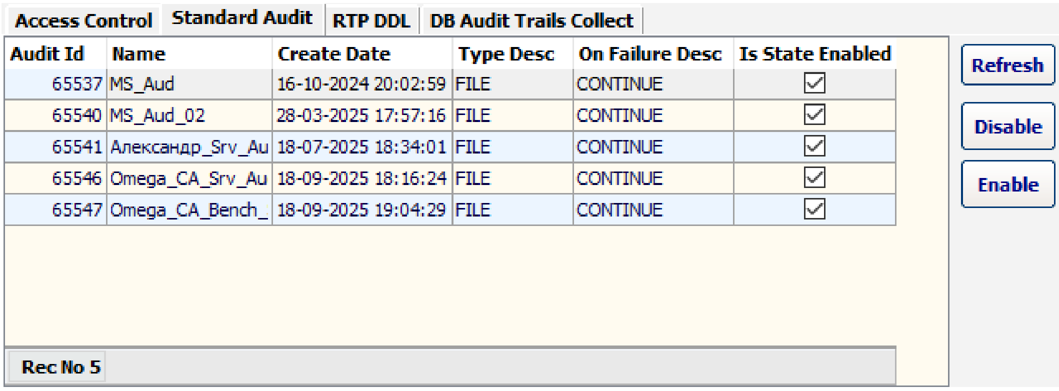
Start and stop the module with the Enable / Disable buttons. Press the Refresh button to refresh module's details.

Silent Access Control

The Silent mode of the Access Control module is managed in the group box Silent, which controls the setting of the system parameter "Silent Access Control". Check to enable the Silent Mode, uncheck to disable and run in non-Silent mode! Press the button "Set" to make changes effective! This feature is by default Silent on Omega Core Audit install.

8.1.2 Standard Audit

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



Audit Id	Name	Create Date	Type Desc	On Failure Desc	Is State Enabled
65537	MS_Aud	16-10-2024 20:02:59	FILE	CONTINUE	☑
65540	MS_Aud_02	28-03-2025 17:57:16	FILE	CONTINUE	☑
65541	Александр_Srv_Au	18-07-2025 18:34:01	FILE	CONTINUE	☑
65546	Omega_CA_Srv_Au	18-09-2025 18:16:24	FILE	CONTINUE	☑
65547	Omega_CA_Bench_	18-09-2025 19:04:29	FILE	CONTINUE	☑

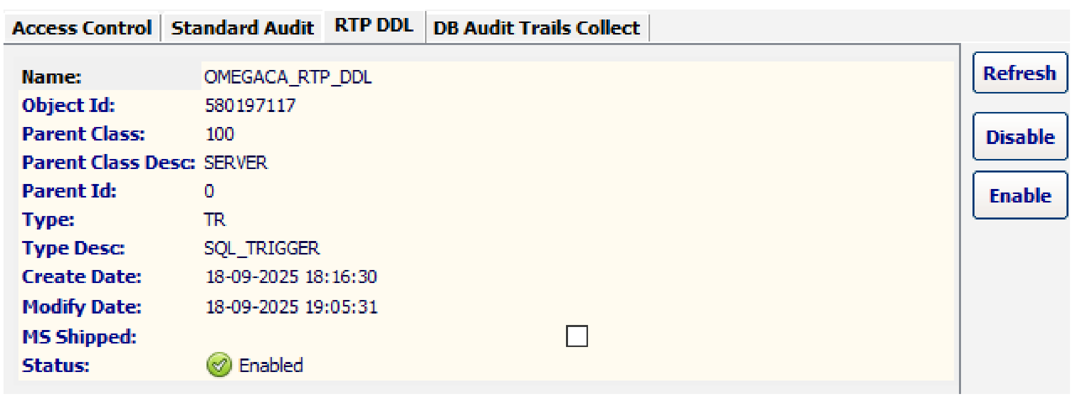
In this Card View on the left you can see the details of all available FILE-based Server Audits.

Press the Disable button to disable all server audits.
Press the Enable button to enable all server audits.

Press the Refresh button to refresh module's details.

8.1.3 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, choose tab RTP DDL.



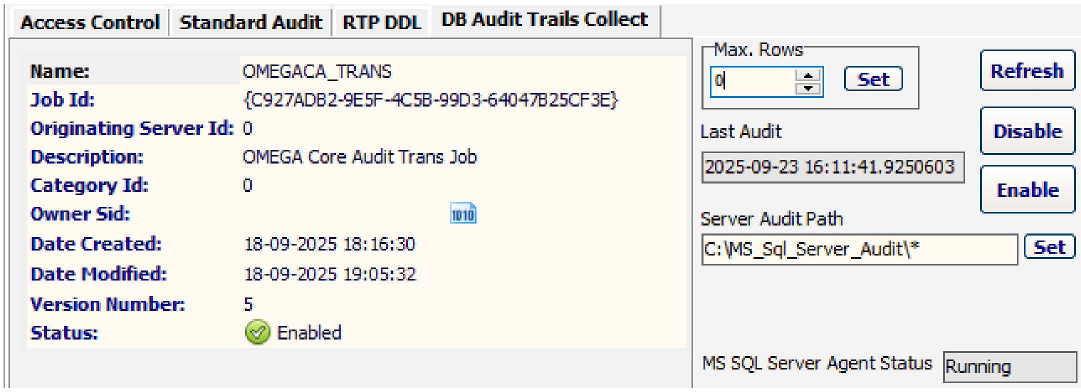
In this Card View on the left you can see the details of the OMEGACA_RTP_DDL server-level FOR DDL_EVENTS trigger that implements the Real-Time Protection DDL module.

Start and stop the module with the Enable / Disable buttons. Press the Refresh button to refresh module's details.

8.1.4 DB Audit Trails Collect

The DB Audit Trails Collect Job reads audit events from the OS files and loads them to the Omega Core repository table.

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



In the Card View on the left you can see the details of the Scheduler Job OMEGACA_TRANS that implements the DB Audit Trails Collect job functionality.
Use the Enable / Disable buttons to start and stop the DB Audit Trails Collect job.
Press the Refresh button to refresh module's details.

Job Elements:

Name	Description
Max. Rows	Maximum number of events to retrieve in a job run. 0 for all events available.
Last Audit	UTC Date and time of the last event retrieved
Server Audit Path	OS Path on which Omega Core Audit reads the FILE-based audit events

Important Notes:

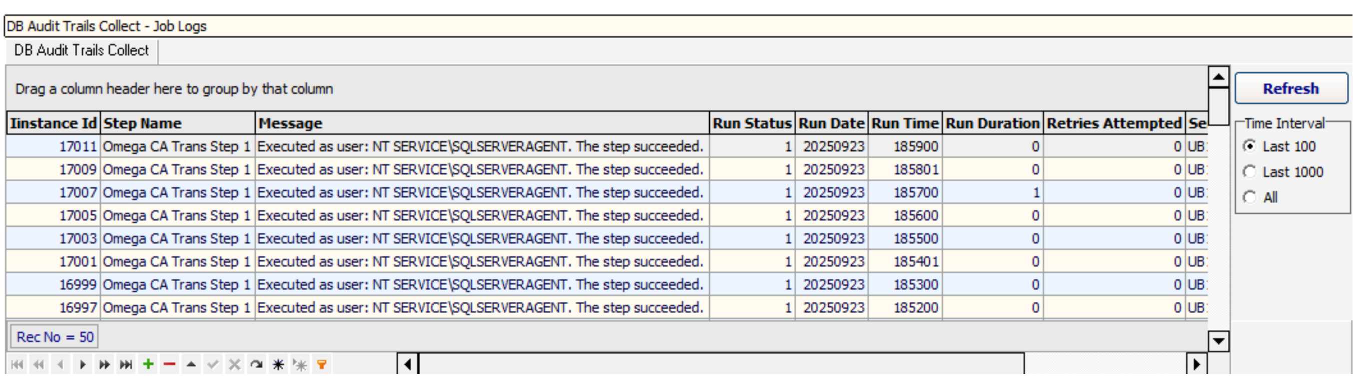
1. All Server Audits from which you want to collect events must have their File Path to this directory.
2. You must put an asterisk (*) after the last anti-slash of the fully qualified path of OS audit folder.
3. Press the Set button to save the configuration of Max Rows and Server Audit Path

Job Run Interval Hint:

The job's run interval is set to 60 seconds by default on install. You can change it via the SSMS (SQL Server management Studio).

8.1.5 DB Audit Trails Collect Job logs

In the lower tab Collection Schedule Job Details you can see the execution logs of the Scheduler Job OMEGACA_TRANS in the DB Audit Trails Collect – Job Logs tab, bottom of the form.

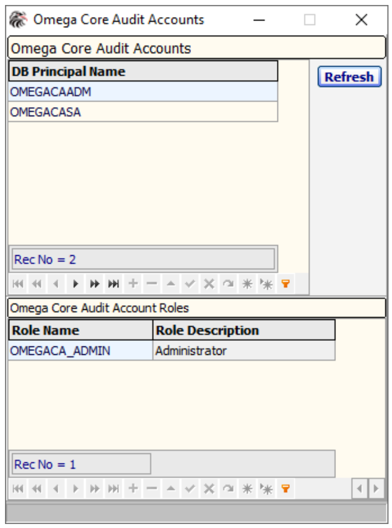


Press the Refresh button to retrieve job logs defined by the selected time interval into the Time Interval radio box group. Switching the Time Interval will reload data with the selected time range.

8.2 Omega Core Audit Accounts and Roles

8.2.1 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.



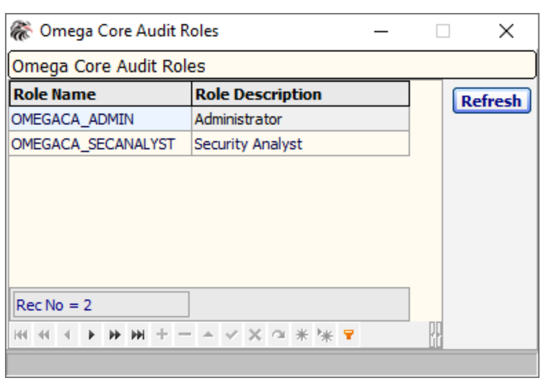
The result will be listed in the Omega Core Audit Accounts Grid in the upper part of the form. Omega Core Audit accounts are MS SQL logins which have been granted at least one Omega Core Audit MS SQL server role.

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.

8.2.2 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.

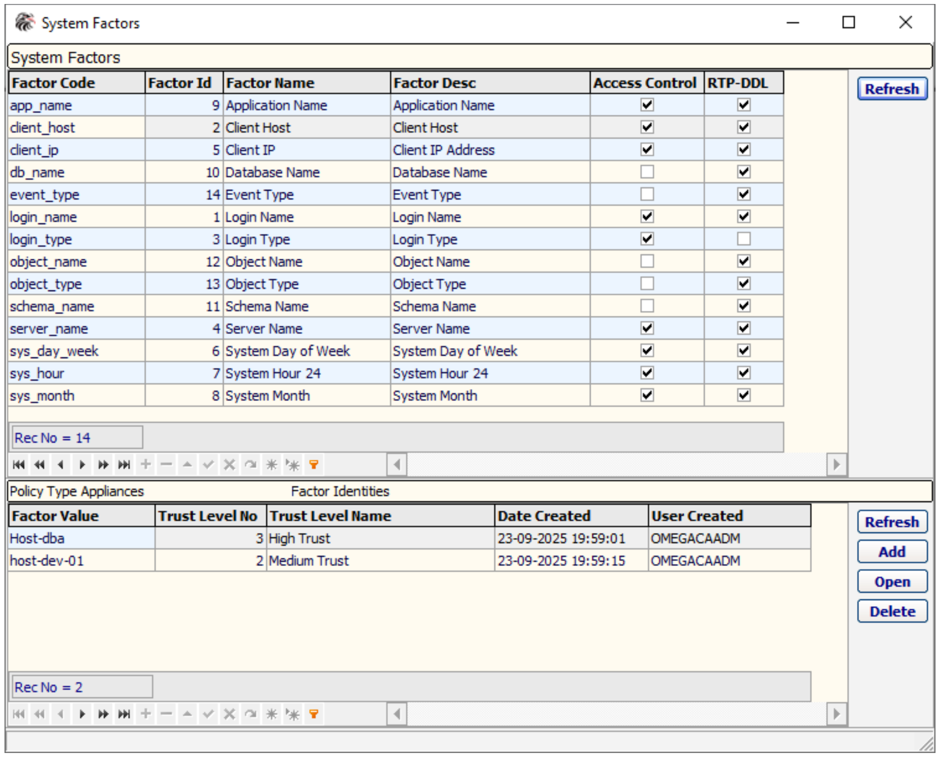


The Omega Core Audit roles are:

- OMEGACA_ADMIN Administrator, full functionalities.
- OMEGACA_SECANALYST Security Analyst, overall (read-only) monitoring.

8.3 System Factors

To view the Omega Core Audit system factors, in the main menu Administration, Miscellaneous 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.
Access Control	Applies or not to the Access Control module
RTP DDL	Applies or not to the Real-Time Protection DDL module

Press the Refresh button to refresh them.

Factor Identities and Trust levels

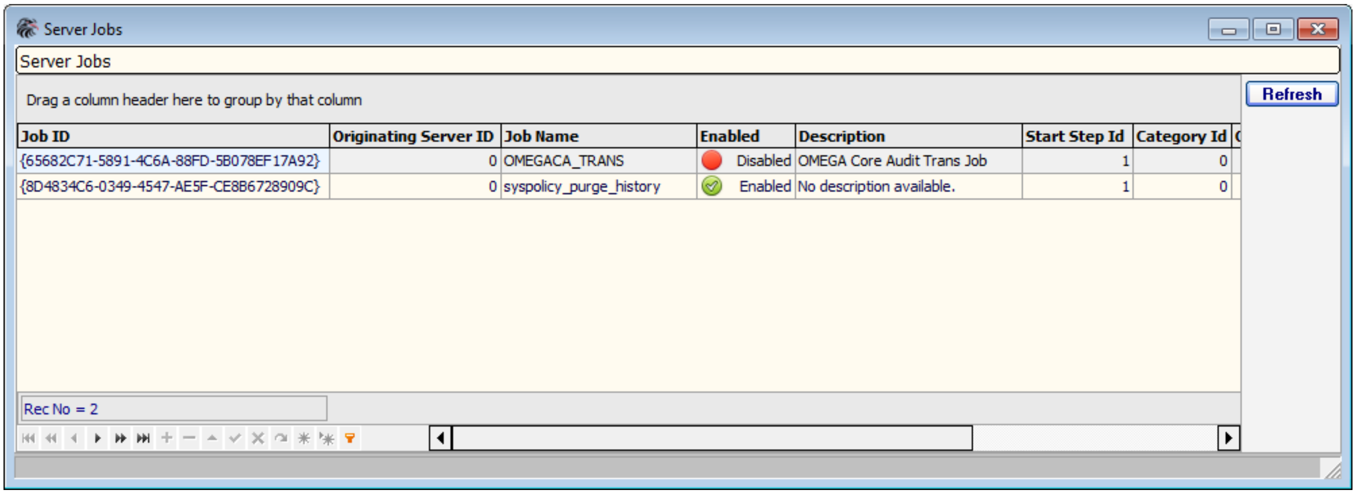
On the lower right part of the form in the grid "Factor Identities", declared identities are displayed for the above selected system factor. System factor identities are used to evaluate condition's with a Condition Evaluate type of Trust Level. Use the respective buttons on the right of this tab to manage system factor's identities.

The following are the trust levels of the system factor's identities:

-1 - Undefined
0 - Untrusted
1 - Low Trust
2 - Medium Trust
3 - High Trust

8.4 Database Jobs

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



Press the Refresh buttons to refresh them.

9 Appendixes

9.1 Appendix A. Abbreviations

The following abbreviations are used in this document:

Omega CA	Omega Core Audit
MS SQL	MS SQL Server
ACC	Access Control
AUD	Auditing
RTP	Real-Time Protection
DDL	Data Definition Language
DML	Data Manipulation language
RTP DDL	Real-Time Protection DDL

9.2 Appendix B. Development History

9.2.1 New in 1.0

New in 1.0:

This is the first release of Omega Core Audit for MS SQL Server.

Fixes in 3.0:

This is the first release of Omega Core Audit for MS SQL Server.

9.3 Appendix C. Support and Licensing

9.3.1 Support

Omega Core Audit clients are entitled to:

- new versions
- upgrades and fixes
- new features
- online support

SLA:

Response Time SLA:	2 Business Days
Support Call/Online:	09:00 GMT to 21:00 GMT, Monday to Friday
Emergencies:	we are here to help
Resolution Time:	case-related

For product documentation, forum and knowledge base, visit our site:
www.dataplus-al.com/omega-core-audit

For technical issues, comments, ideas and impressions, e-mail us at:
support@dataplus-al.com

Also follow us on the next social media sites where DATAPLUS is present:

YouTube	https://www.youtube.com/channel/UCa59qQuGg5tvd2vIe1MsMOw
LinkedIn	https://www.linkedin.com/company/dataplus-al

9.3.2 Licensing

Omega Core Audit license is perpetual. It allows the customer to use the licensed software indefinitely and not tied to the product version.

Omega Core Auditing for MS SQL Server licenses number is the same as the number of licenses of your MS SQL Server.

For pricing and licensing information, contact our Sale specialists at:
sales@dataplus-al.com