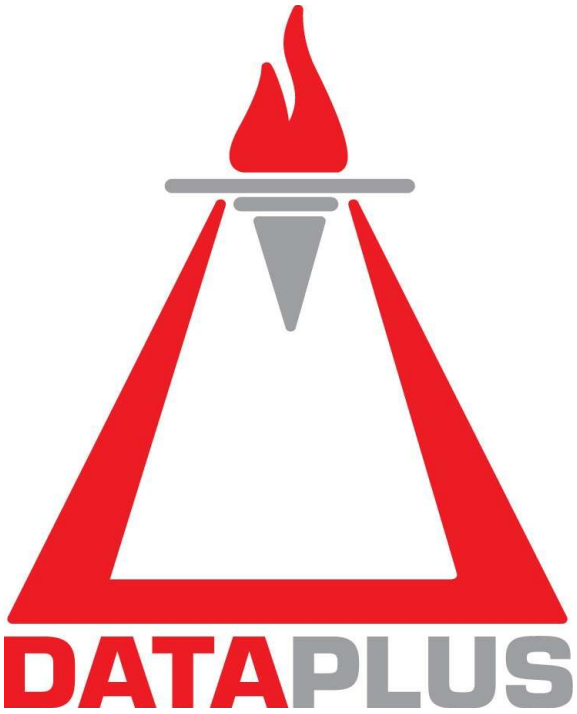
March, 2020

Omega DB Security Reporter ™

For Oracle Database



OMEGA DB Security Reporter

For Oracle Database

User's Guide

1.1.0

www.dataplus-al.com

TABLE OF CONTENTS

1 CHAPTER 1: Overview

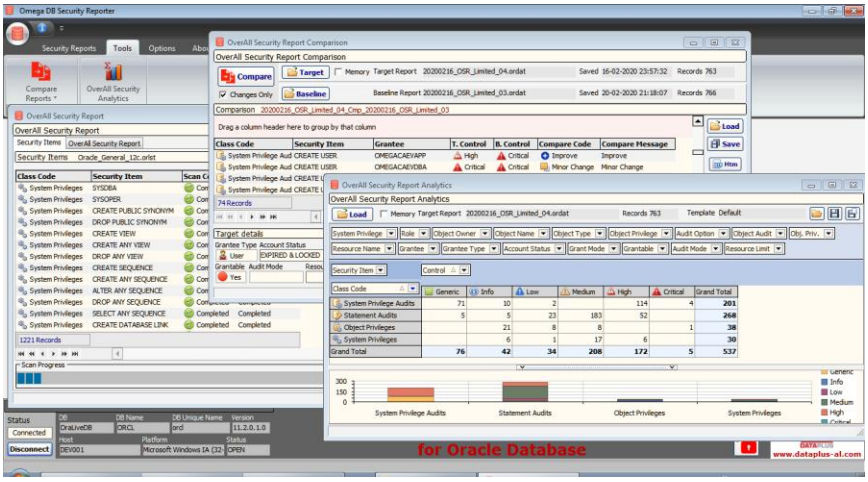
1.1 Introducing Omega DB Security Reporter

Omega DB Security Reporter is a security auditing and software-only solution for Oracle databases.
It is a SQL–PL/SQL network assessment tool.

It implements quick reporting, visualization and documentation of the security posture of the Oracle database on the following security areas of top importance:

Oracle Security Areas
(Security Items assessed):

- Privileges
  - System Privileges
  - Object Privileges
  - Role Privileges
- Audits
  - System Privileges
  - User Statements and Shortcuts
  - Object Privileges and Statements
- User Profiles
  - Password Resources



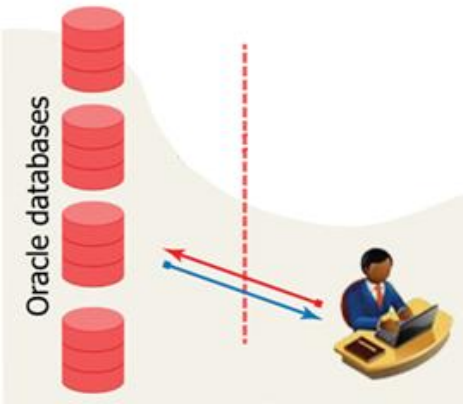
Omega DB Security Reporter is an out-of-box and software-only solution. It is implemented as a Windows Application, a simple client-side solution that is just deployed (no installation) on the user's PC, configured in few minutes, and ready to assess and report on the security posture of your Oracle databases.

Omega DB Security Reporter is Agent-less and accesses the target database in *read-only* mode.

Omega DB Security Reporter performs *not* just "browsing/viewing" of Oracle dictionary on security areas, but real assessing and reporting of the security posture of your mission-critical Oracle database!

1.2 Solution Architecture

Omega DB Security Reporter features the simplest possible architecture regarding the Oracle database.



(simplest) Architecture

A two-tier, Client-Server model, the Application directly connecting and assessing the target Oracle database. Fully standalone (can run from USB).

The security personnel assesses and reports on multiple databases; all configurations and results are stored locally.

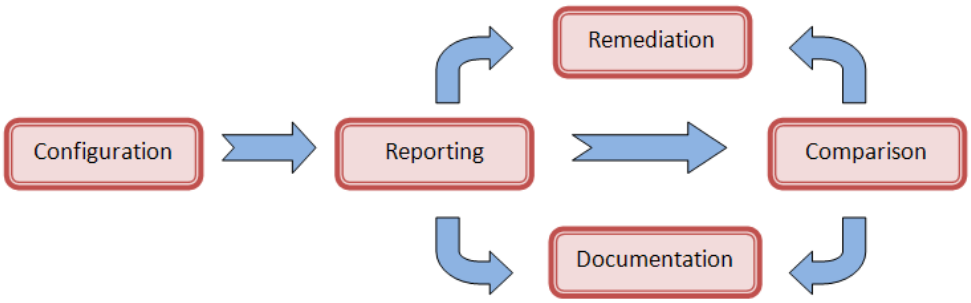
1.3 How it works

The Omega DB Security Reporter features a set of advanced, highly customizable and in-depth controls (Report Classes) on important Oracle database security areas, as listed above.

It enables user to:

- Quickly deploy, configure and connect to the target Oracle Database[s]
- Report by pre-defined templates for Overall Security Reports – immediate start
- Report ad-hoc by each Report Class – privileges, audits, password resources
- Assess and evaluate Security Items for each Grantee/User *
- Highlight differences between reports
- Complete detailed documentation
- Provide clear remediation information

* Field Control – common to each Report dataset – is the result of this evaluation.



Workflow

Configuration	a one-time configuration of DB connection.
Reporting	assess the target DB database
Comparison	compare two reports of different point in times to highlight differences between
Documentation	document your assessment
Remediation	performed by the DBA based on report and comparison

Such controls can be performed while connected on the target Database, for each and any available Security Item belonging to the supported Security Areas and being assessed, either in bulk or single mode.

The Security Item is evaluated for *every* Oracle User account (and optionally Role - when applies) and a Report Dataset is generated.

Account Status evaluation:

The status of an Oracle user account is a factor in evaluation making difference between *permanently Locked* statuses and others:

Permanently Locked:	LOCKED, EXPIRED & LOCKED, EXPIRED(GRACE) & LOCKED
Others:	OPEN, EXPIRED, EXPIRED(GRACE), LOCKED(TIMED), EXPIRED & LOCKED(TIMED), EXPIRED(GRACE) & LOCKED(TIMED)

Effective privilege (role hierarchy) evaluation:

A system, object or role privilege that is directly granted to a grantee (user account or role) is easily verifiable in respective Oracle dictionary views, which is the simplest approach; however a grantee might have effectively (!) the same privilege not granted (and verified) directly, but granted through a Role, or more, hidden after a "chain" of roles granted to each other and having the privilege granted to the last role at the end of this "chain".

The feature above ensures the evaluation considers not only a direct grant, but also an "inherited" one. It is present in most controls whenever privilege-related.

Account based evaluation:

Reporting on effective privilege grants instead of only on directly granted enables assessing at Oracle user account level only and not roles, as roles are just containers of privileges and do not represent operating entities per se, like humans or credentialed interfaces - as user accounts do.

Intelligent Assessment:

Combining all features, and specific ones, like when reporting on system privilege audits, the account effectively holding (or not) the privilege assessed impacts the report's result.

Others:

Public Grants highlight
Grantable Privileges
Audit user-wide highlight

Report Comparison (Change Management):

Reporting alone is unable to provide a clear view on the next item most important behind report itself: Change Management of the security posture. Use the Report Comparison to highlight and categorize the changes between two different reports - Target and Baseline.

Analytics and Integration

Graphical analytics of security reports is provided as a pivot grid and dynamic related chart.
Export of Reports and Comparisons is available in Htm, Txt, and Xls format.

1.4 Compliance

Omega DB Security Reporter's focusing and capabilities on Privileges, Audits and Passwords management, converge with the same control objectives assessed by common Oracle Security Checklists and general IT Security Frameworks and Standards.

It will perfectly perform the assessment of Privilege, Audit and Password management related controls for the following well known and authoritative Oracle Security Checklists:

CIS	CIS Benchmark for Oracle Database Server 11g, 2011
STIG-DISA	Oracle Database 11g Security Technical Implementation Guide, 2016
SANS	Oracle 10g Security Hardening Checklist 3.1, 2006

Beside the security checklists above, Omega DB Security Reporter capabilities facilitate the assessment of Oracle databases for compliance with the following, but not limited to, IT Security Frameworks/Standards:

ISO 27001/2	ISO 27002 2013, Security Techniques
ISACA (Cobit)	Oracle Database Security Checklist, Whitepaper, 2008
PCI-DSS	PCI DSS Quick Reference Guide, version 3, 2019
HIPAA	The HIPAA Security Rule, 2003

Note

Checklists and Frameworks/Standards named above contain controls other than those supported/addressed by Omega DB Security Reporter. There is *no* pretence in this application for a full match on all controls of the above checklists, but only for what is supported by Omega DB Security Reporter - which has its own way and focus!

For more details on Omega DB Security Reporter compliance to requirements of common Oracle Security Checklists and IT Security Frameworks/Standards, refer to Appendix A4 – Oracle Security Compliance.

1.5 Compatibility and Requirements

Oracle Database support

Omega DB Security Reporter supports Oracle Database versions from **11g R1 – 19c**.
It has been thoroughly tested on 11g R2 and 12c R2, and also on 18c.

Database support is independent of the operating system!

All editions of the Oracle database, Standard Edition (One) to Enterprise, and also the XE, are supported!

Application requirements

The OS and software requirements of Omega DB Security Reporter application are:

- All x86/x64 Windows NT-based systems.
- NLS_LANG operating system environment variable, optionally (*)

* refer to "Appendix A2 - Oracle Connection Settings"

Visit our website for news on current developments:

www.dataplus-al.com/omega-db-security-reporter

1.6 Software Editions – Standard vs Professional

Software Editions

The Omega DB Security Reporter deployment features in two editions:

Standard — This is the default-on-install edition and it is free to use in Live and Production environments, with some limitations, as in the table below.

Professional — The Professional Edition is a commercial solution and uses all features of the software.

Omega DB Security Reporter Features	Standard	Professional
Security Reports:		
Overall Security Reports	x	x
Overall Security (with pre-defined Templates)	x	x
Ad-hoc Security Reports (by Class)	x	x
Persistence/Integration:		
Save/Load	x	x
HTM Export	x	x
TXT, XLS, PDF, RTF Export	-	x
Comparison:		
Overall Security Reports	-	x
Ad-hoc Security Reports	-	x
Analytics:		
Overall Security Reports	-	x

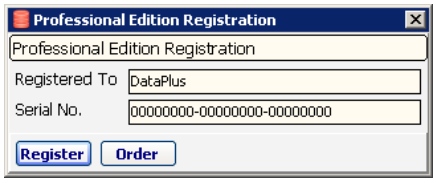
Omega DB Security Reporter - supported features by Edition

Professional Edition Activation

Initially the Omega DB Security Reporter will run in the Professional edition and day-Trial limited mode.

The Trial period is 30 days. After the trial period expires the application will switch to the Standard edition.

The Professional edition 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 Professional edition of the application. You will receive a confirmation on the right combination of Registered To/Serial.

2 CHAPTER 2: Deployment

2.1 Deployment and first run

Omega DB Security Reporter software package is deployed as a compressed file, named:

Omega_DB_SR_[VS]_[MN]_[PT].zip

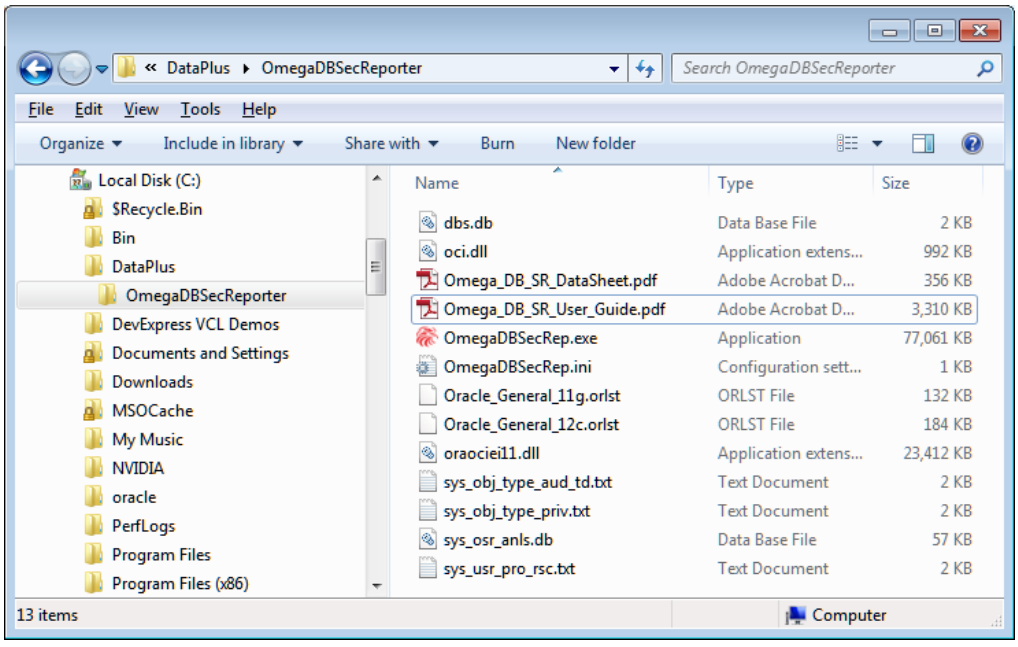
The acronyms are two digit numbers, 0 left padded, and stand for:

VS	Version
MN	Maintenance Release
PT	Patch Number

There is no installation routine in the proper sense, no installer and no registry entries created, just the files inside the compressed package. Just download the software from our website and extract the files to a Windows Explorer directory of your choice, for example:

C:\DataPlus\OmegaDBSecReporter

and put all the software package's files into this directory.



The application files deployed in this version are:

OmegaDBSecRep.exe	Application's executable file.
OmegaDBSecRep.ini	Application's initialization parameters file.
dbs.db	Target Databases configurations binary file.
Oracle libraries	Oracle 11g R2 Instant Client Win 32 binaries (oci.dll, oraociei11.dll).
Application data	data used by the application (sys_osr_anls.db and the .txt files)
Oracle General	ready to use Overall Security reports Templates on general Oracle security (Oracle_General_11g.orlst and Oracle_General_12c.orlst)
Documents	Software's Data-Sheet and (this) User Guide in PDF format.

It is advised that you place the Oracle General Templates in a special folder and not on the same with the executable. Lists can be changed by user and also new ones created.

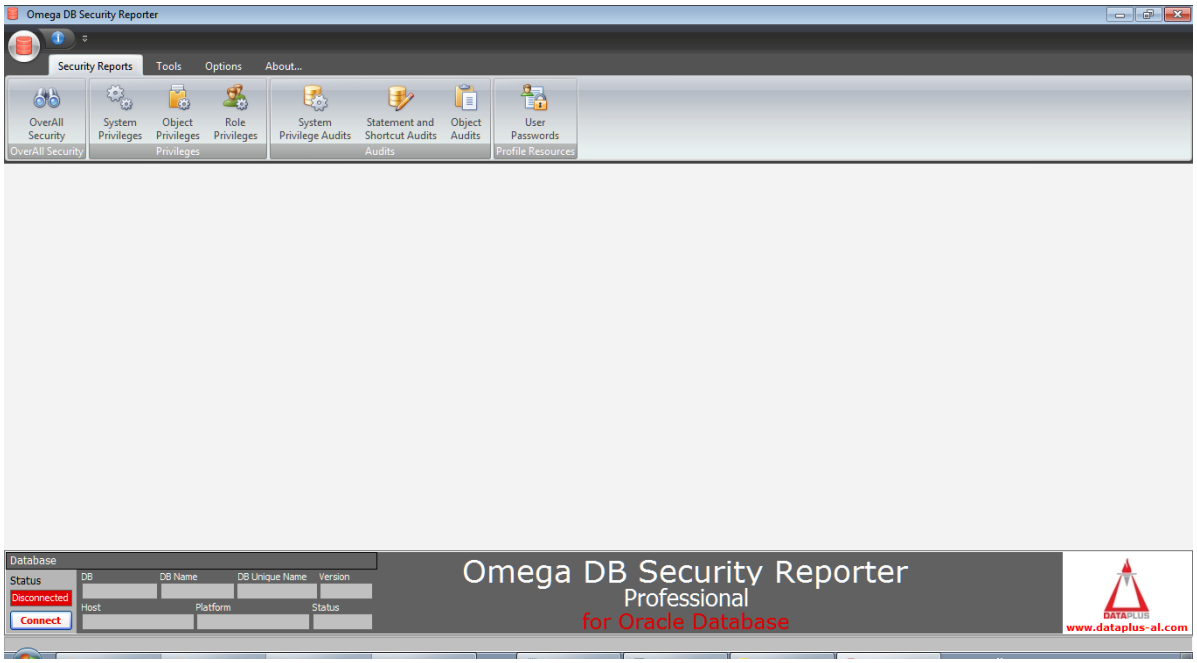
Same thing is required for other files that are persisted, like the Reports or Saved Searches, for which you are also advised to create your own directories, headed – for example – according to Target Database names as declared in your configurations!

Important Note!

Files deployed are opened and managed only by the executable! Compressing, modifying, or accessing them in any mode other than from the application or without permit and advise from DATAPLUS may permanently damage your data and also lead to abnormal and erroneous software behavior and results!

Double-click on the **OmegaDBSecRep.exe** (or its shortcut) to start the Omega DB Security Reporter application!

The Application's main form will open.



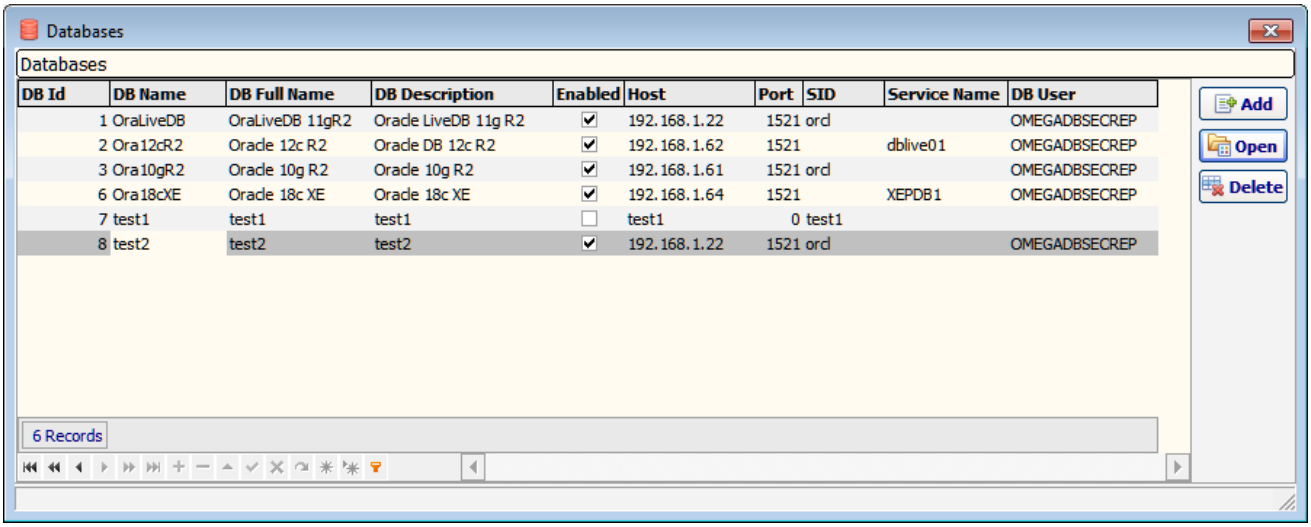
Omega DB Security Reporter – Professional edition

In the Application's main menu, the followings tabs are available:

Security Reports	Overall Security Reports Ad-hoc Security Reports
Tools	Comparison of Security Reports Analytics of Overall Security Reports
Options	Target Databases System configurations Application data Oracle Dictionary views
About	Information about this software Professional edition registration information

2.2 Target Databases

After the install, but also later, user must create and maintain its own records of Oracle target Databases that will be assessed and reported by Omega DB Security Reporter. To view the registered Databases, in the Application's main menu tab Options, group Databases, click on the button Databases. Form Databases (empty on deploy) will open.



Target Database main fields:

Name	Description
DB Id	Database unique number, incremental and auto-assigned
DB Name	Application common name of the target Oracle Database
DB Full Name	Application common full name of the target Oracle Database
DB Description	Application common description of the target Oracle Database, optional.
Enabled	In use or not, controls appearance on System Authentication (logon) form
Host	Machine's Hostname or IP Address of the target Oracle database server
Port	Oracle Listener Port of the target Oracle database, default 1521
SID	Target Oracle Database Instance name, used by default. Valid for non-CDBs and non-RAC
Service Name	Target Oracle Database Service name, used for RAC database instances and PDBs. Default is Null. Effective only when SID is left NULL!
DB User	Target Oracle database user account used for reporting *
DB Auth	Target Oracle database user account password used for reporting **

* The only thing required in the target database; refer to "Appendix A1 - Oracle Database Account for Reporting"!
** Invisible on Grid. Optional entry at System Authentication on each connection - same for DB User.

Database functionalities (buttons):

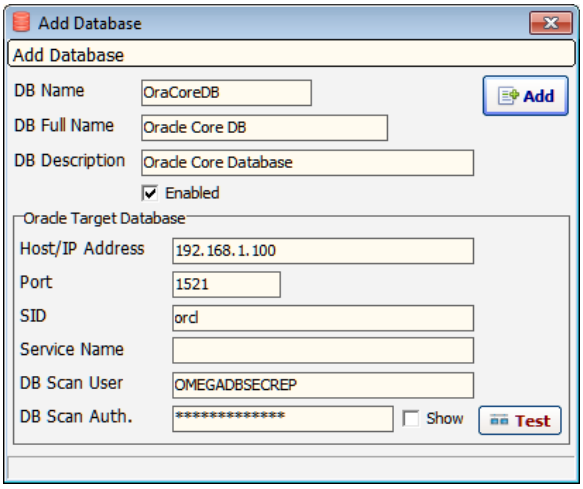
Add opens form Add Database to register a new one (refer to topic below)

Open opens form Database for view and modification (refer to topic below)

Delete deletes the registered Target Database

Add New Database

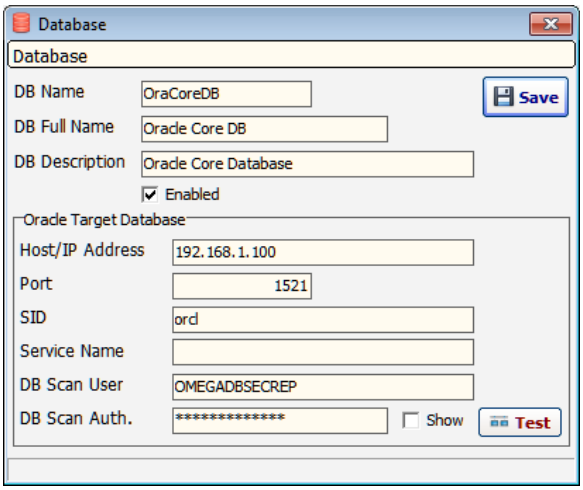
To register a new target Oracle Database, in the form Add Database complete the common target Database naming and (optionally) description fields. Complete the target database connection setup entries in the Oracle Target Database group box. The Test button will test the connectivity and authentication to the target Database.



Press the button Add to register the new Database.

Open Database

To open an existing target Oracle Database for view or modification, open it in the form Database.

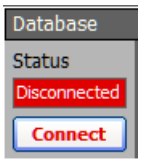


If you make changes and want to save them – press the button Save.

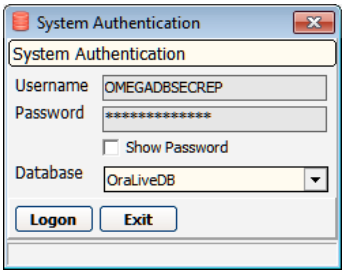
2.3 Connecting to a Database

With the Omega DB Security Reporter you can connect one-at-a-time to all target Oracle databases which you have previously configured in the form Databases.

To connect to an Oracle database, at application's main form on the bottom-left press the button Connect.



This will invoke the target database System Authentication form. The Database combo box loads the enabled Target Databases by DB Name, and auto-selects the last one successfully connected. The Username and Password edits are respectively completed or opened, depending if they have been set on the respective target Database entry.

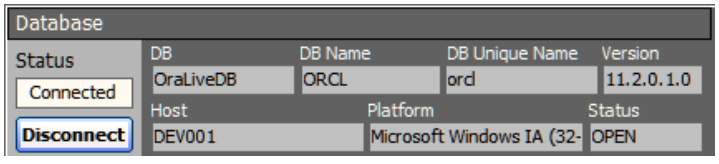


Press the Logon button to connect to the target database.

Note

For more details on Oracle database connection settings refer to topics "System Settings" and "Appendix A2 - Oracle Connection Settings."

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



The Database panel fields are:

DB	DB Name for the Target Database
DB Name	Database name
DB Unique Name	Database unique name
Version	Database full version
Host	Database host name
Platform	Database platform
Status	Status of the Database

3 CHAPTER 3: Security Reports

3.1 Common Report Features

3.1.1 Report Classes

Reports are classified by available Report Classes according to the type of the Oracle Security Item that is being assessed, which can be a privilege (system, object, role), an audit (of a system privilege, statement, shortcut, object privilege/statement), or a password resource; this - logically - determines the technical approach of the assessment and impacts the format and content of the report result.

As a last (technical) resource a Report Class is a specific Oracle PL/SQL routine that is invoked by the application to assess each security item belonging on the Target Database. During the report, the Security Item is evaluated for *every* Oracle User account (and optionally Role - when applies) and a Report Dataset is generated. The Security Item assessed relates to one, many, or none of the Report Dataset records – depending on the Report Class approach, Security Item and Grantee/User being evaluated.

The Report Classes available in this version are:

1. System Privileges
2. Object Privileges
3. Role Privileges
4. System Privileges Audits
5. Statements and Shortcuts Audits
6. Object Audits
7. Password Resources

Note:

The Audit Classes (4-6) support the Oracle Database Traditional Audit only! The new Unified Audit, starting with Oracle Database 12c Release 1, is scheduled in our plans and will be available in the next versions!

So is another Report Class dedicated to the database Initialization Parameters – security-related.

3.1.2 Report Types

Two general Report types are available in this application:

Overall Security Reports	integrating different/all classes into an overall report, with security items loaded from a pre-defined Template, either deployed or user-defined.
Ad-hoc Security Reports	performing Reports by each Class, with security items retrieved from a direct search on the target database

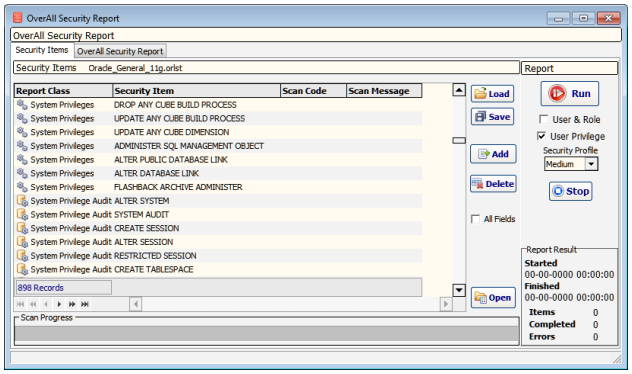
The first are ideal for periodic assessment and reporting
The second – as the name implies – for ad-hoc of the same.

However, their features are applicable and find their way in both situations.

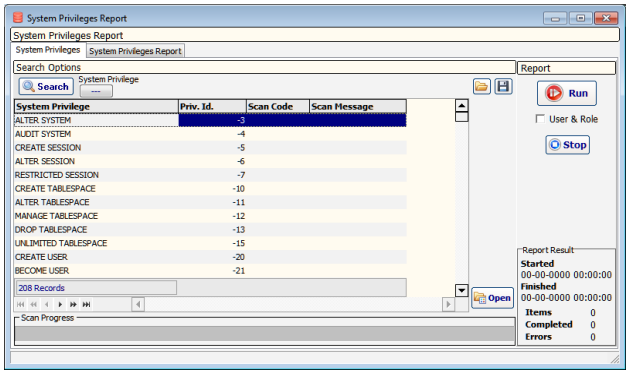
3.1.3 Operation and Presentation

Security Report forms have common features, starting with being comprised of two main tabs.

In the first, a list of Security Items is either loaded from a pre-defined Template, or created, as in the case of the Overall Security Report, or searched directly from the Oracle Target Database dictionary, as in the case of ad-hoc Reports. Application data are also used in case of Object Privileges/Audits, and of Password Resources Classes.



Overall Security Report – loaded Security Items



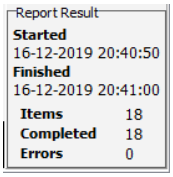
System Privileges ad-hoc Report – searched Security Items

Field[s] on the left describe[s] the Security Item assessed, specific to each Report Class. The last two on the right, Scan Code and Scan Message - common to all reports - describe report item operation. They are initialized as Null on every Load/Search, and completed only after the next Report Run.

On the right side of the same first tab, the Report group provides report operations and information. Common functionalities are:

Starts a new report.

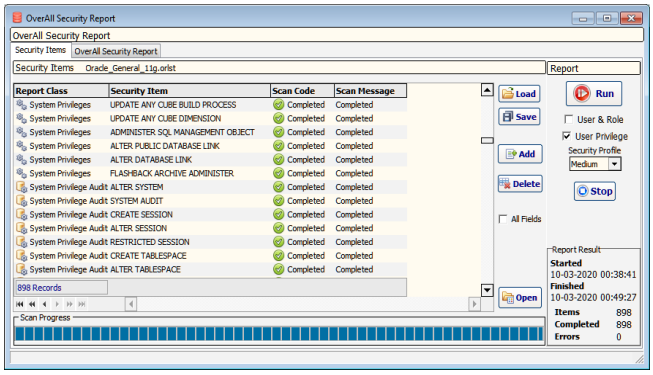
Stops a running report



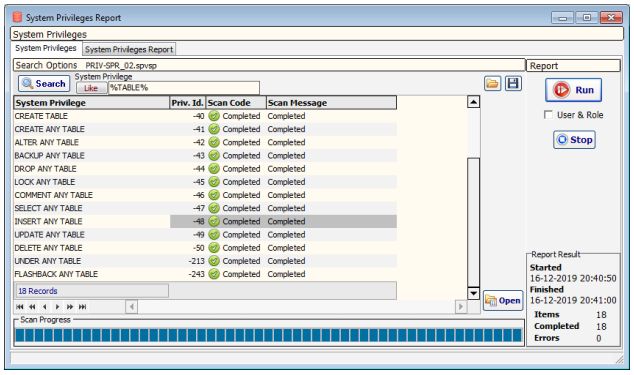
Report execution and general summary information

Report Input parameters are specific and valid for each class, and more detailed in Overall Security Report topic, and on each ad-hoc Report one.

Press the button Run to generate a new Report. All Security Items will be processed, first to last, the bar on the form's bottom will display the operation's progress, and a final Information Message box will show in the end.



Overall Security Report – completed



System Privileges ad-hoc Report – completed

Reporting will update fields Scan Code and Scan Message for each Security Item while processing.

Scan Code and Scan Message fields:

Scan Code — Result Code of the Item's report, available options:

Completed	Completed successfully
System Error	Program error
Oracle Error	Oracle error

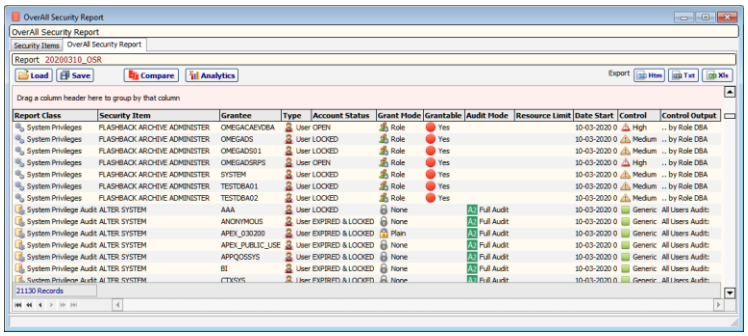
Scan Message — Success confirmation, or system/Oracle error message

Notes:

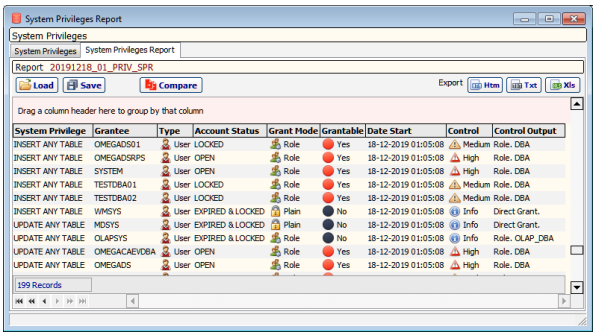
1. Do not to interact with the application while the report is running! Stopping is the only exception!
2. Sorting is reset on report run. Filtering of Security Items is suspended, all records are assessed.

After Report run, the first tab's grid, with its Scan Code and Scan Message completed, will summarize information on individual Item operation level. The "real" Report – record details for Security Items – is found on the next tab.

In the second tab, the Report records, generated on the assessed Security Items on the previous, are displayed.



Overall Security Report – records



System Privileges ad-hoc Report - records

Field[s] on the left (System Privilege only in this example) describe[s] the Security Item assessed, specific to each Report Class. The last three on the right - common to all reports – display Date-time and Control information on reported Security Item/Grantee couple.

Date Start	DateTime of Item report (from target DB)
Control	Evaluated Result of Report Item for Grantee
Control Output	Details on Report Item for Grantee

The following functionalities are common to all reports:

Load	Loads the report from disk
Save	Saves the report to disk (binary file)
Compare	Opens report's respective Comparison form; current report loaded as Target
Export Htm Txt Xls	Export the report respectively as Htm, Txt and Xls files

3.2 Overall Security Report

To perform an Overall Security Report on the Target Oracle Database, in the application's main menu, first tab Security Reports, group Overall Security, click on the button with same name. Form Overall Security Report will open.

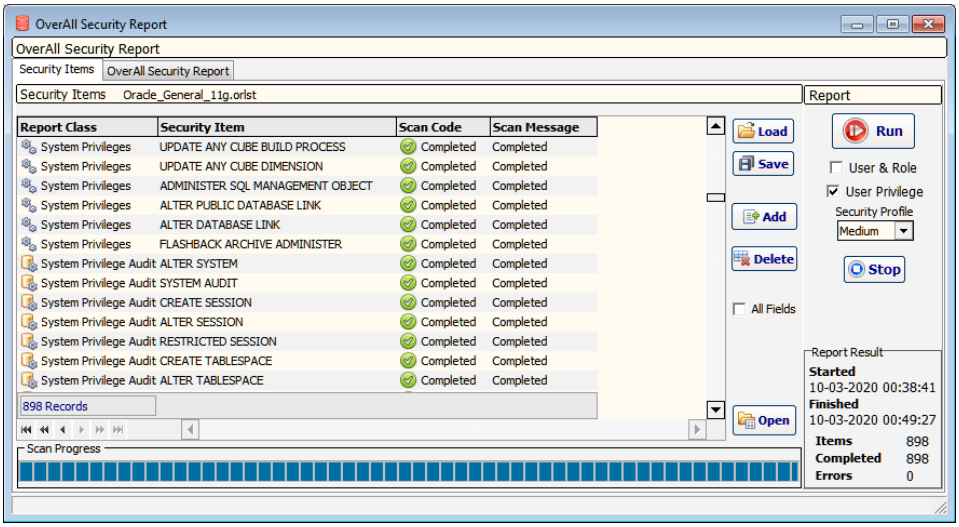
The first tab Security Items, as the name implies, features an integrated list comprised of items from one, more, or all available Report Classes. It can be loaded from an Overall Security Template, or created on the run, respectively by using buttons Load and Add, later explained.

A new Report is run on the Report group on the right. Report inputs – specific to each Report Class – are:

All Privilege-like	Users only or Roles also assessed
System Privilege Audits	Evaluated or not for effective grant
User Password Resources	Security Level used for assessment

For more details on Report Inputs refer on each (class-specific) ad-hoc Report topic!

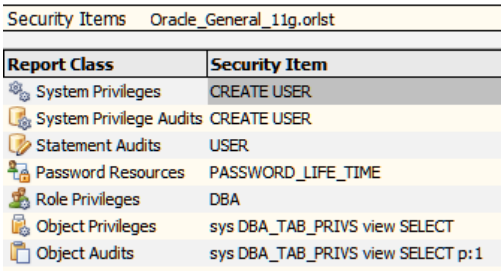
Press the button Run to generate a new Report and wait until all Items complete.



Specific Overall Security Items fields are:

Report Class	indicates the Class of the report
Security Item	specific by Report Class, ex. System Privilege, …, Password Resource.

Content format of the Security Item field goes by Report Class:



Report Classes and Security Items

```
<SYSTEM PRIVILEGE>
<SYSTEM PRIVILEGE AUDIT OPTION>
<STATEMENT/SHORTCUT AUDIT OPTION>
<PASSWORD RESOURCE NAME>
<ROLE>
<owner> <OBJECT NAME> <object type> <OBJECT PRIV.>
<owner> <OBJECT NAME> <object type> <OBJECT AUDIT> p:[x]*

* p[x] is object privilege [0-no, 1-yes]
```

Security Item content format by Report Class

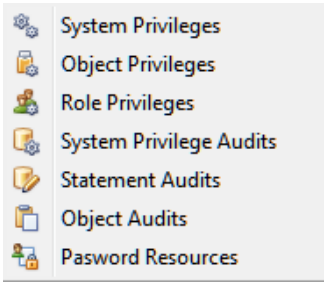
On the Security Items grid right, the following functionalities are available:

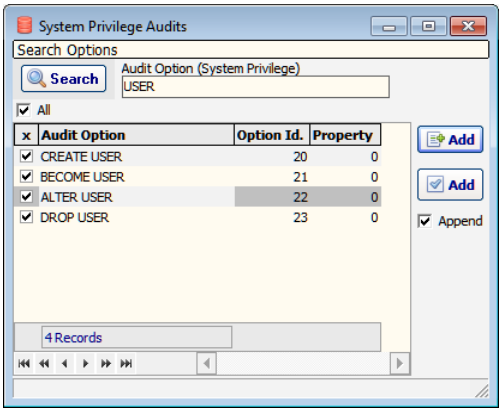
Loads an Overall Security Template from disk, application provided, or user-created. In this version the application provides the following templates:

- Oracle General 12c Template
  (can also, except for few items, be used for 18c and higher versions)
- Oracle General 11g Template

Saves the Security Template permanently to disk, needed after changes to the deployed ones, or when creating/changing user defined.

Displays a drop-down menu to add a new Security Item



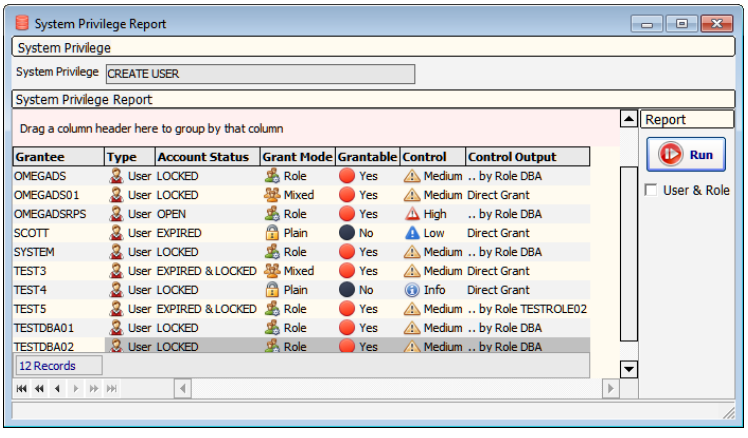


For example, the form on the right, invoked by the menu item named the same, enables adding new Security Items of Report Class System Privilege Audit. Respectively, forms for each other class offer the same functionality

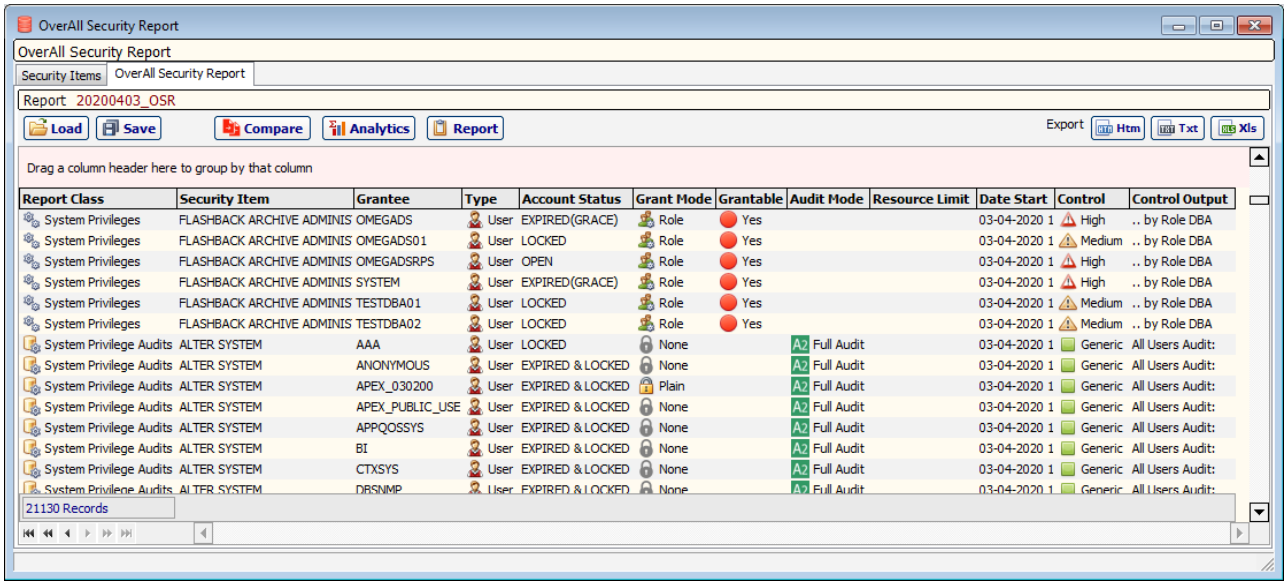
Search queries Oracle dictionary
(Check) All selects/unselects items
Add single adds selected record to list
Add multiple adds selects items to list
Append appends new record to the end of list when checked, previous record otherwise

Deletes the selected Security Item record

Other than a bulk reporting on all Security Items, a single-item reporting application form is available for all available Report Classes. It can be invoked from the Overall Security Report, or by any Ad-hoc Security Report, via button Open, on the right and below to the Security Items list.



In the second tab Overall Security Report, the completed report is displayed. Listing for each Security Item are: Grantees of the privileges (effective grant!), or User (although Grantee column is used) for Audits and Password Resources – as for each specific Report Classes.



Overall Security Report fields:

Name	Description
Report Class	Class of the Report System Privileges Object Privileges Role Privileges System Privilege Audits Statement Audits Object Audits Password Resources
Security Item	Security Item specific by each Class
Grantee *	Grantee – User or Role for privilege-like Classes, User for others
Type	Grantee Types. Public Grantee is Public User Grantee is an User account Role Grantee is a Role
Account Status	User Account Status
Grant Mode	Mode of Privilege (effective) grant: Plain Granted directly Role Granted through Role[s] Mixed Granted directly and through Role[s]
Grantable	If the Privilege is (effectively) transferrable No Is not grantable Yes Is grantable
Audit Mode	Mode of User Audit 0 A0 No Audit Not audited 1 A1 Partial Audit Partial Audit 2 A2 Full Audit Full Audit

Resource Limit	User Resource Limit
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for Grantee. 0 Generic 1 Info 2 Low 3 Medium 4 High 5 Critical Generic represents a correct security posture. All others, from Info-Critical indicate increasing levels of criticality!
Control Output	Details of Control Output.

* In the result dataset of the Overall security Report, field Grantee features fields Grantee from privilege-like classes, System, Object and Role Privileges, while User for others - Audit and Password Resources.

Important Note

For more details on Grant Mode, Audit Mode, Resource Limit and Control fields (Control and Control Output), refer to topic Appendix A3 - Report Classes and Application Codes.

Report Class Specific Fields

Fields Grantee, Type, Account Status, Grant Mode, Grantable, Audit Mode and Resource Limit are completed depending on the Report Class in use. However, they are the one visible, but not the only ones.

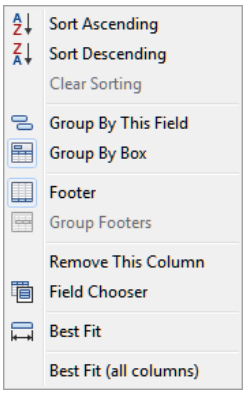
Checking the All Field checkbox on the first tab will display the following other fields, present in both Security Items and Report records:

System Privilege, Role, Object Owner, Object Name, Object Type, Object Privilege, Audit Option, Object Audit, Obj. Priv., Resource (Name).

More details on these fields is provided on respective ad-hoc Reports topics!

Hint:

Alternatively, in the Overall Security Report grid the fields appearance can also be selected by right-clicking on any field header and invoking the grid's right-click menu. The later, that includes other feature other then field appearance, is available also to all ad-hoc Security Reports.

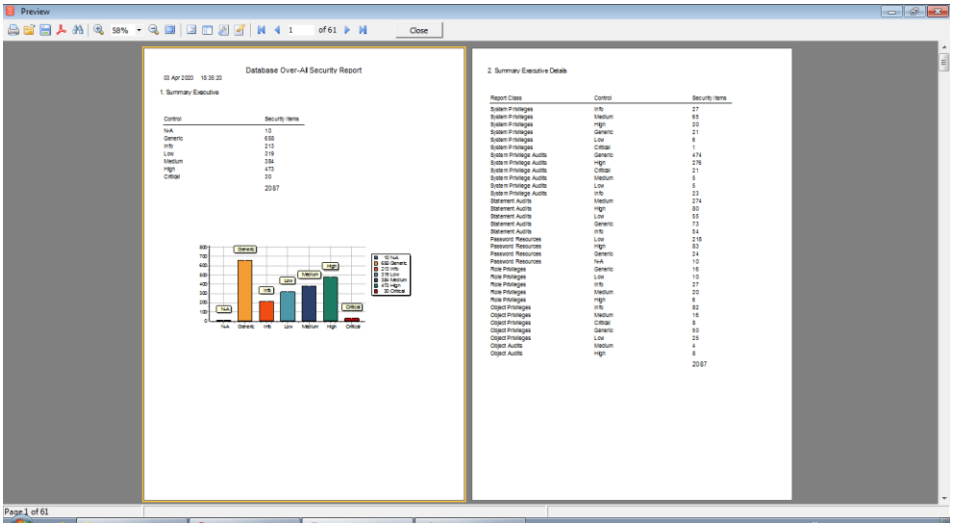


"Classic" Report Print/Preview

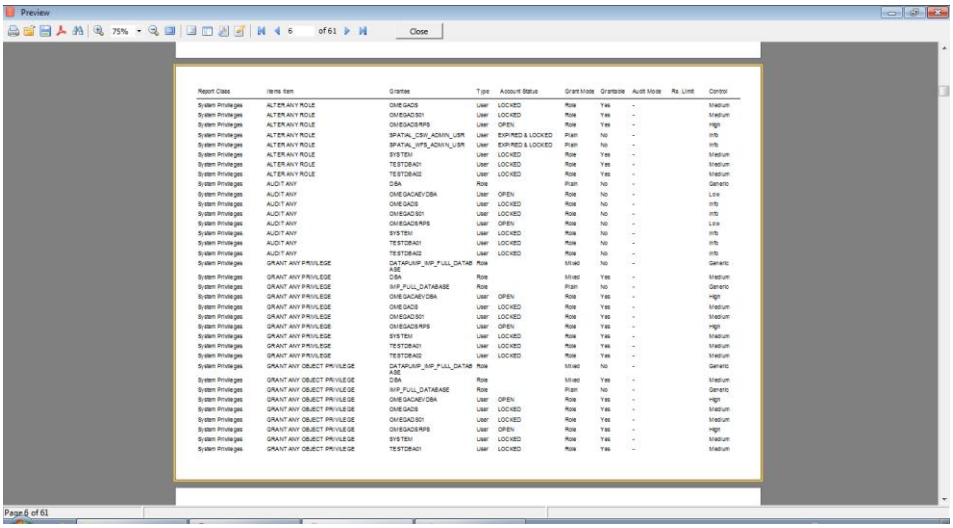
Print and Preview – on classic style – is an available feature of the Overall Security Reports. In the second tab Overall Security Report, after you have generated or loaded a report, press the button Report on top. By default a preview of the Report will show in its own report-style form.

The Database Overall Security Report contains three sections:

1. Summary Executive
2. Summary Executive Details
3. Report Items



Summary Executive (and details) above, Report record Items below



The following functionalities – between others – are found on the top-left of the report preview form:

 opens the Print dialog to print the report

 In the drop-down menu can choose the RTF file... option to save as a file in Rich Text format

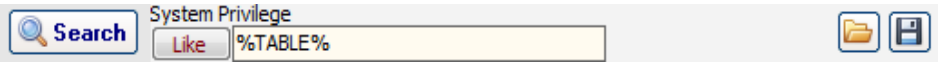
 opens the PDF export dialog to save as a file in Portable Document format

3.3 Ad-hoc Security Reports

3.3.1 System Privileges Report

To assess and report on Oracle Database System Privileges, in the application's main menu, first tab DB Security Reports, group Privileges, click on the button System Privileges. Form System Privileges Report will open.

In the first tab System Privileges, complete the search inputs, or load them from disk, and press the button Search to retrieve the System Privileges that will be reported from the Target Database.

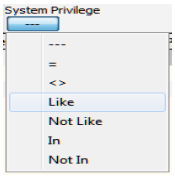


The search functionalities are common to all ad-hoc Reports:

Searches and retrieves Security Items

Loads Search Options from disk.

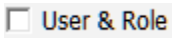
Saves Search Options to disk.



Operator drop-down buttons defines different combinations of search options.

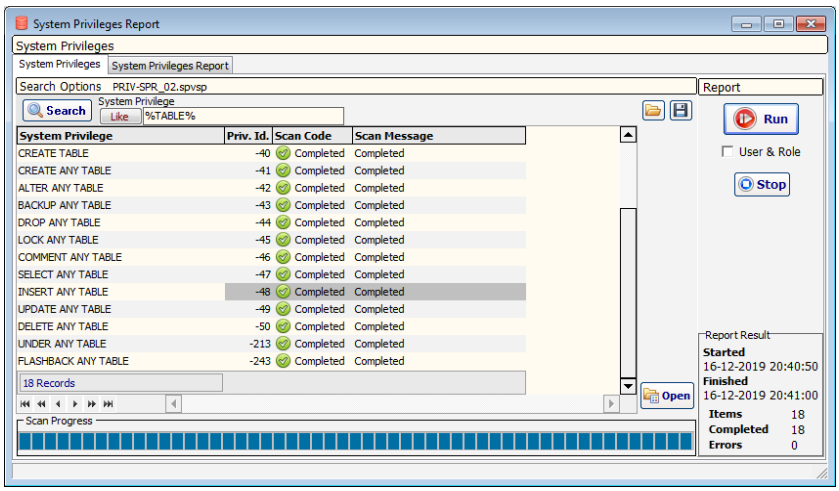
Semicolon (;) is used to separate IN/ NOT IN-s

A new Report is run on the Report group on the right. Report inputs are:

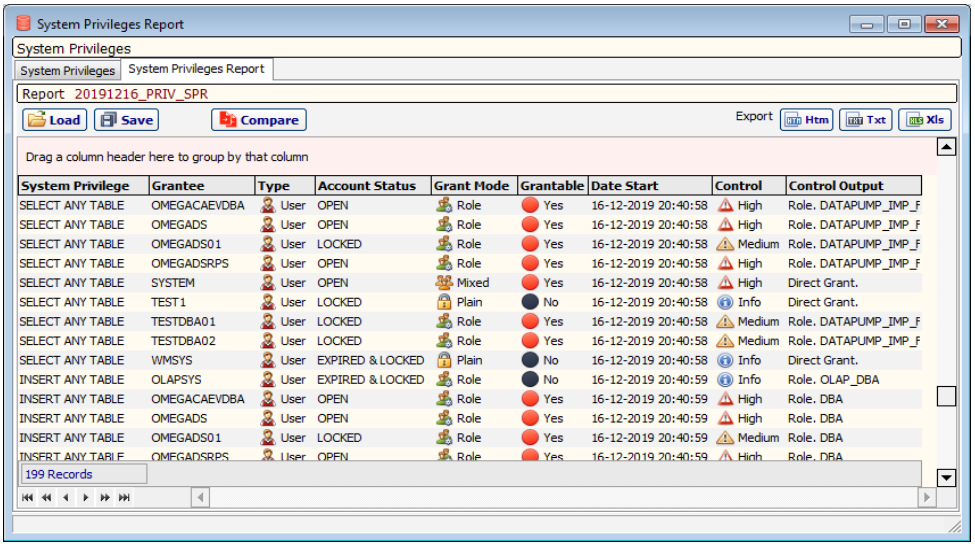


Unchecked	Users accounts only assessed – default (and advised)
Checked	Users accounts and Roles assessed (for a specific focus on Roles)

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab System Privileges Report, the completed report is displayed. Listed for each System Privilege are: Grantees of the privilege (effective grant!).



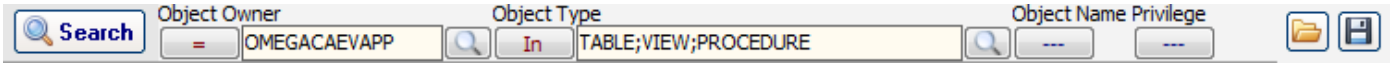
System Privileges Report fields:

Name	Description
System Privilege	System privilege name
Grantee	Grantee of the privilege
Type	Grantee Types. Public — Grantee is Public User — Grantee is an User account Role — Grantee is a Role
Account Status	User Account Status
Grant Mode	Mode of Privilege (effective) grant: Plain — Granted directly Role — Granted through Role[s] Mixed — Granted directly and through Role[s]
Grantable	If the Privilege is (effectively) transferrable No — Is not grantable Yes — Is grantable
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for Grantee. 0 Generic — Grantee is Role, Privilege not Grantable 1 Info — Grantee is Locked User, Privilege not Grantable 2 Low — Grantee is Unlocked User, Privilege not Grantable 3 Medium — Grantee is Locked User or Role, Privilege is Grantable 4 High — Grantee is Unlocked User, Privilege is Grantable 5 Critical — Granted to PUBLIC
Control Output	Grantee details on effective privilege.

3.3.2 Object Privileges Report

To assess and report on Oracle Database Object Privileges, in the application's main menu, first tab DB Security Reports, group Privileges, click on the button Object Privileges. Form Object Privileges Report will open.

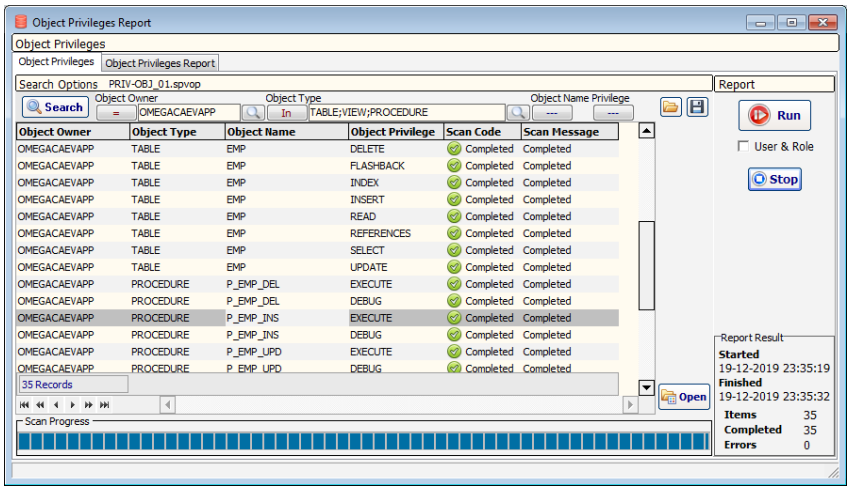
In the first tab Object Privileges, complete the search inputs, or load them from disk, and press the button Search to retrieve the Object Privileges that will be reported from the Target Database.



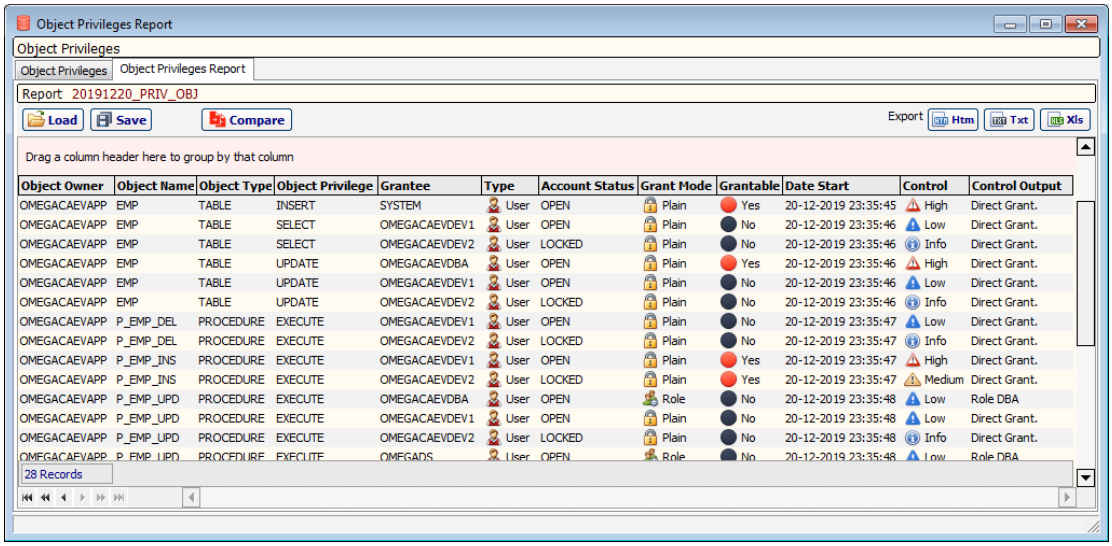
A new Report is run on the Report group on the right. Report inputs are:

☐ User & Role	Unchecked	Users accounts only assessed – default (and advised)
	Checked	Users accounts and Roles assessed (for a specific focus on Roles)

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab Object Privileges Report, the completed report is displayed. Listed for each Object Privilege are: Grantees of the privilege (effective grant!).



Object Privileges Report fields:

Name	Description
Object Owner	Owner of the object
Object Name	Name of the object
Object Type	Type of the object
Object Privilege	Object Privilege
Grantee	Grantee of the privilege
Type	Grantee Types. Public Grantee is Public User Grantee is an User account Role Grantee is a Role
Account Status	User Account Status
Grant Mode	Mode of Privilege (effective) grant: Plain Granted directly Role Granted through Role[s] Mixed Granted directly and through Role[s]
Grantable	If the Privilege is (effectively) transferrable No Is not grantable Yes Is grantable
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for Grantee. 0 Generic Grantee is Role, Privilege not Grantable 1 Info Grantee is Locked User, Privilege not Grantable 2 Low Grantee is Unlocked User, Privilege not Grantable 3 Medium Grantee is Locked User or Role, Privilege is Grantable 4 High Grantee is Unlocked User, Privilege is Grantable 5 Critical Granted to PUBLIC
Control Output	Grantee details on effective privilege.

Hint

As in every fully client-side data-aware application, the Report's dataset size is subject to size limitations, which however exceeds 1,000,000 records, a number which you are not supposed to encounter, unless in usages of Object-like Report Classes – Object Privileges and Object Audits – and for a very big number of Security Items returned by the search, Privileges or Audits. In this case you should reduce the Security items assessed by narrowing the scope of the search.

3.3.3 Role Privileges Report

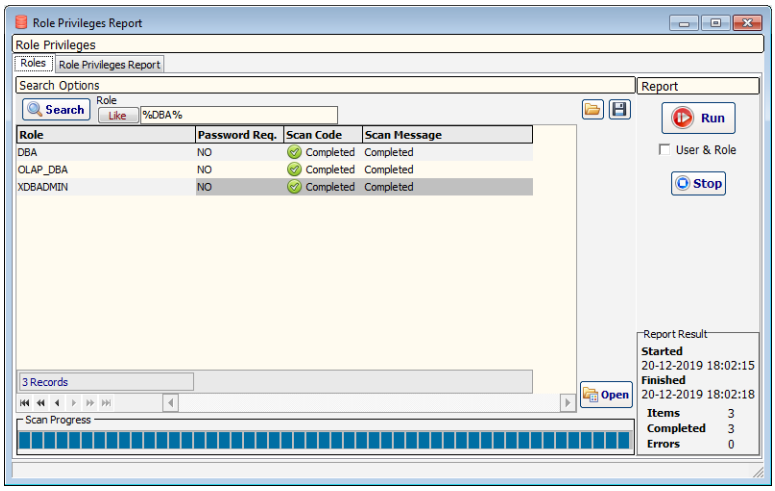
To assess and report on Oracle Database Role Privileges, in the application's main menu, first tab DB Security Reports, group Privileges, click on the button Role Privileges. Form Role Privileges Report will open.

In the first tab Roles, complete the search inputs, or load them from disk, and press the button Search to retrieve the Roles Privileges that will be reported from the Target Database.

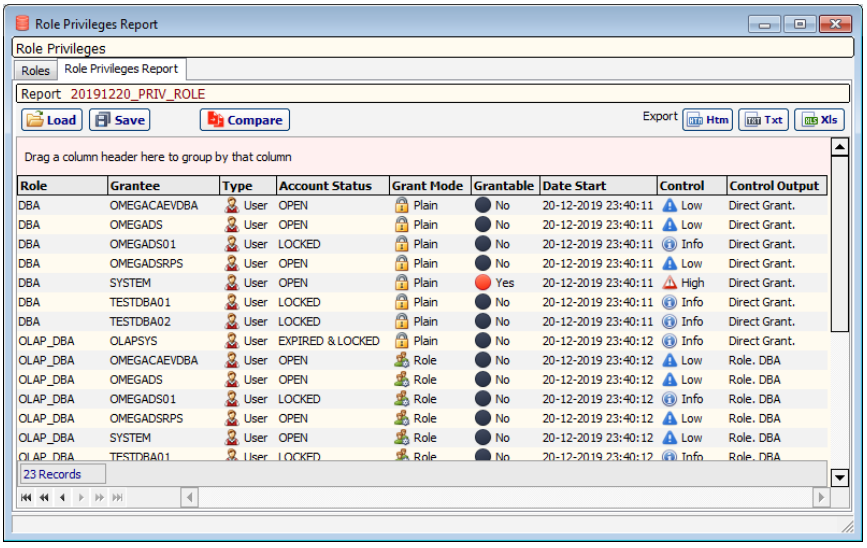
A new Report is run on the Report group on the right. Report inputs are:

☐ User & Role	Unchecked	Users accounts only assessed – default (and advised)
	Checked	Users accounts and Roles assessed (for a specific focus on Roles)

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab Role Privileges Report, the completed report is displayed. Listed for each Role (privilege are): Grantees of the privilege (effective grant!).



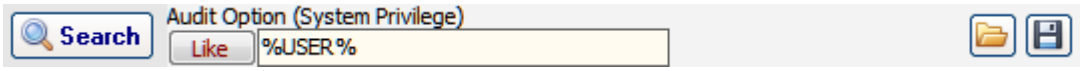
Role Privileges Report fields:

Name	Description
Role	Role name
Grantee	Grantee of the (Role) privilege
Type	Grantee Types. Public Grantee is Public User Grantee is an User account Role Grantee is a Role
Account Status	User Account Status
Grant Mode	Mode of Privilege (effective) grant: Plain Granted directly Role Granted through Role[s] Mixed Granted directly and through Role[s]
Grantable	If the Privilege is (effectively) transferrable No Is not grantable Yes Is grantable
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for Grantee. 0 Generic Grantee is Role, Privilege not Grantable 1 Info Grantee is Locked User, Privilege not Grantable 2 Low Grantee is Unlocked User, Privilege not Grantable 3 Medium Grantee is Locked User or Role, Privilege is Grantable 4 High Grantee is Unlocked User, Privilege is Grantable 5 Critical Granted to PUBLIC
Control Output	Grantee details on effective privilege.

3.3.4 System Privilege Audits Report

To assess and report on Oracle Database System Privilege Audits, in the application's main menu, first tab DB Security Reports, group Audits, click on the button System Privilege Audits. Form System Privilege Audits Report will open.

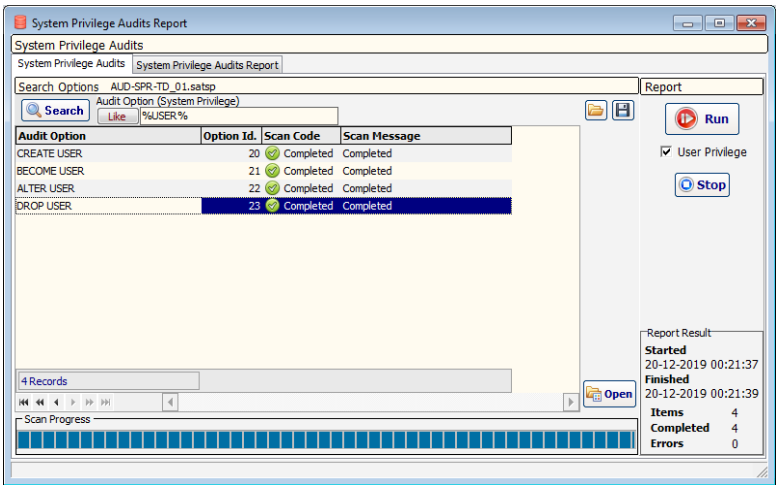
In the first tab System Privilege Audits, complete the search inputs, or load them from disk, and press the button Search to retrieve the System Privilege Audits that will be reported from the Target Database.



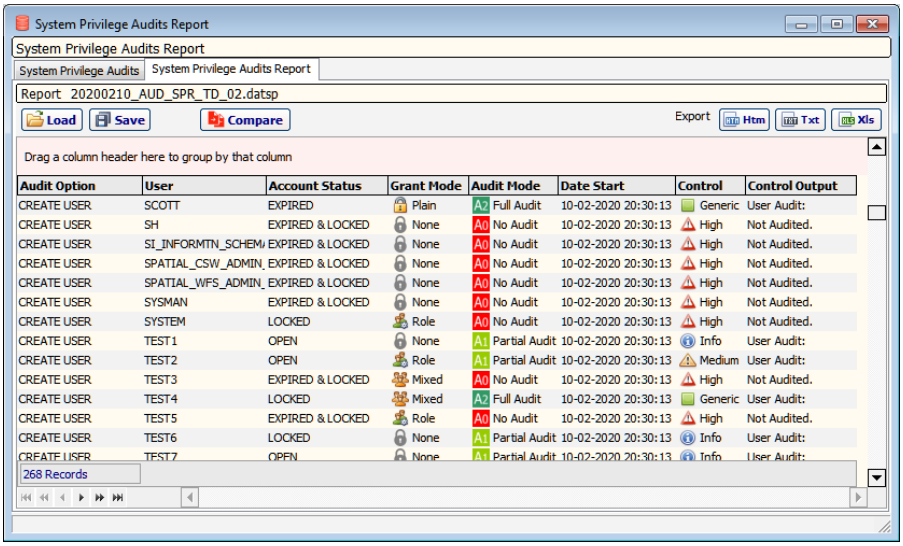
A new Report is run on the Report group on the right. Report inputs are:

☑ User Privilege	Checked	System Privilege evaluated for effective grant (default and advised)
	Unchecked	System Privilege not evaluated (will count as *not* granted)

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab System Privilege Audits Report, the completed report is displayed. Listed for each System Privilege Audit Option: All Users – either audited or not.



System Privilege Audits Report fields:

Name	Description
Audit Option	Audit option (System Privilege)
User	User account
Account Status	User Account Status
Grant Mode *	Mode of Privilege (effective) grant: No Grant — Not Granted Plain — Granted directly Role — Granted through Role[s] Mixed — Granted directly and through Role[s] Public — Granted through PUBLIC N/A — Not Applicable
Audit Mode	Mode of User Audit 0 A0 No Audit — Not audited 1 A1 Partial Audit — Partial Audit 2 A2 Full Audit — Full Audit
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for User. 0 Generic — User Fully Audited 1 Info — User Partially Audited, Privilege not Granted 2 Low — User Partially Audited, Account is Locked, Privilege is Granted 3 Medium — User Partially Audited, Account is Unlocked, Privilege is Granted 4 High — User not Audited, Account is Locked OR Privilege not Granted 5 Critical — User not Audited, Account is Unlocked AND Privilege is Granted
Control Output	User audit and effective privilege details.

* The System Privilege Audit (option) Report features integration with the System Privilege one. The effective (!) Grant of the Privilege *impacts* the Control evaluation of the System Privilege Audit option, at least when the User Privilege option is checked – as a default and recommended.

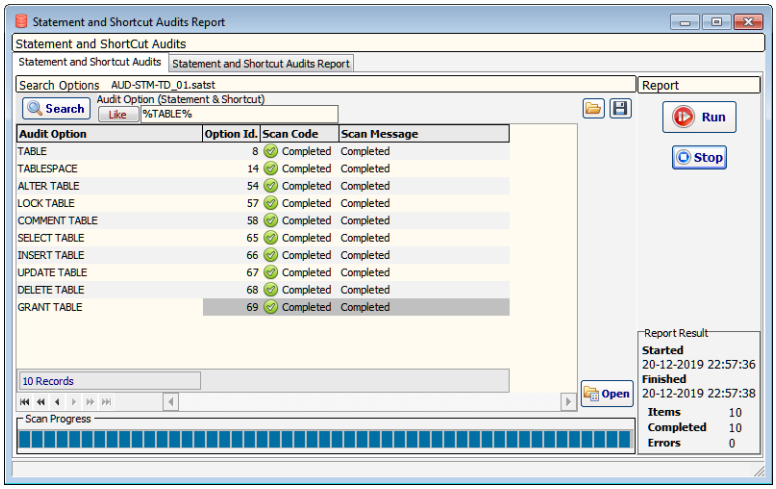
3.3.5 Statement and Shortcut Audits Report

To assess and report on Oracle Database Statement and Shortcut Audits, in the application's main menu, first tab DB Security Reports, group Audits, click on the button Statement and Shortcut Audits. Form Statement and Shortcut Audits Report will open.

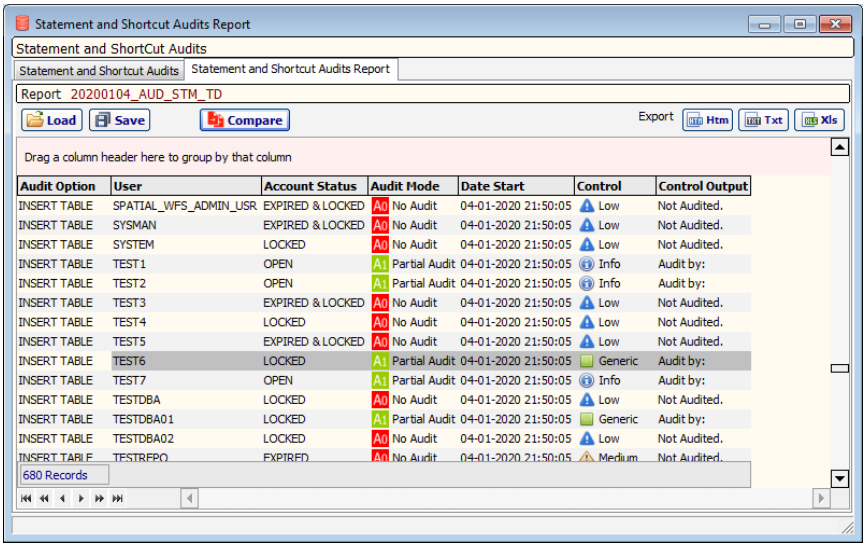
In the first tab Statement and Shortcut Audits, complete the search inputs, or load them from disk, and press the button Search to retrieve the Statement and Shortcut Audits that will be reported from the Target Database.

A new Report is run on the Report group on the right.

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab Statement and Shortcut Audits Report, the completed report is displayed. Listed for each Statement/Shortcut Audit Option are: All Users – audited or not.



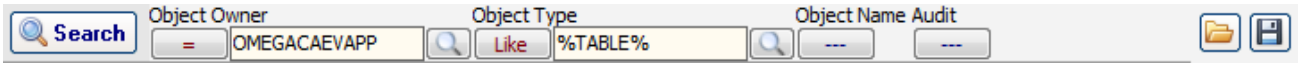
Statement and Shortcut Audits Report fields:

Name	Description
Audit Option	Audit option (Statement/Shortcut)
User	User account
Account Status	User Account Status
Audit Mode	Mode of User Audit 0 A0 No Audit Not audited 1 A1 Partial Audit Partial Audit 2 A2 Full Audit Full Audit
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for User. 0 Generic User Fully Audited 1 Info User Partially Audited, Account is Locked 2 Low User Partially Audited, Account is Unlocked 3 Medium User not Audited, Account is Locked 4 High User not Audited, Account is Unlocked
Control Output	User audit details.

3.3.6 Object Audits Report

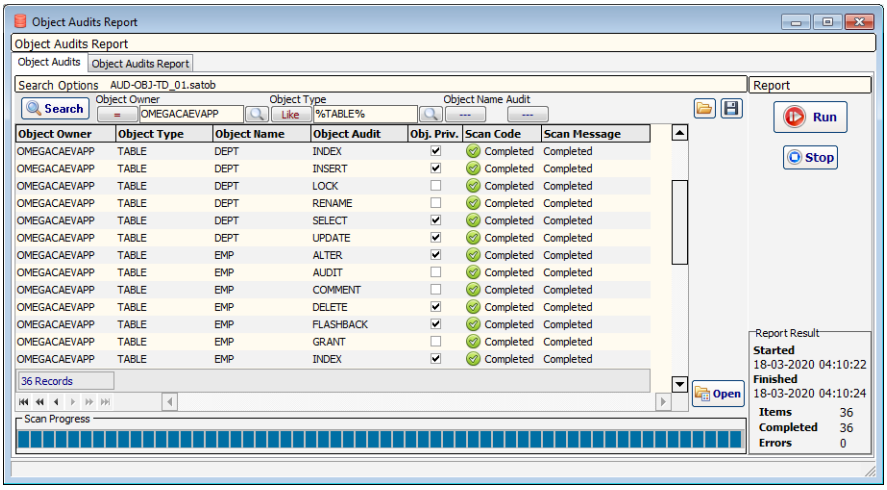
To assess and report on Oracle Database Object Audits, in the application's main menu, first tab DB Security Reports, group Audits, click on the button Object Audits. Form Object Audits Report will open.

In the first tab Object Audits, complete the search inputs, or load them from disk, and press the button Search to retrieve the Object Audits that will be reported from the Target Database.

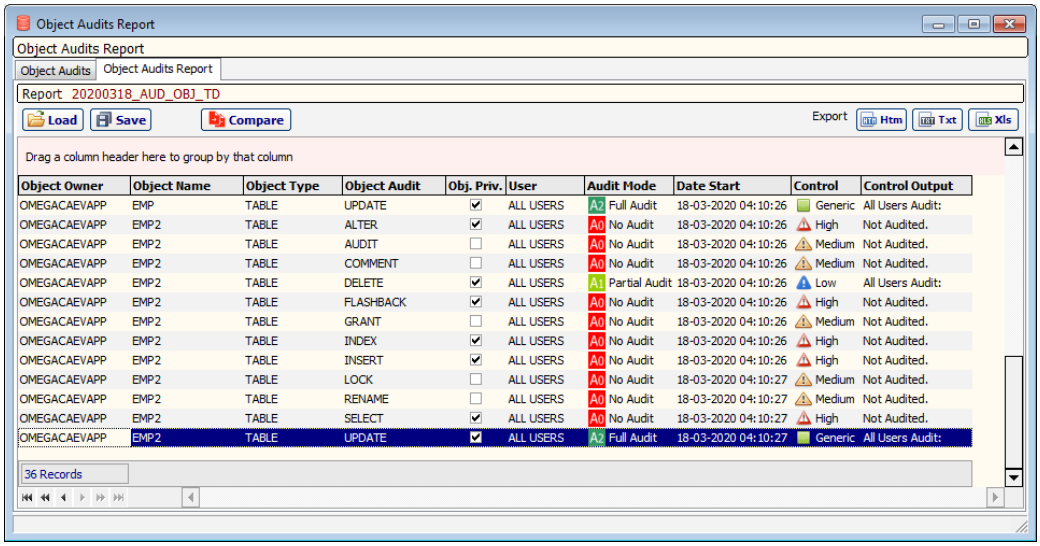


A new Report is run on the Report group on the right.

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab Object Audits Report, the completed report is displayed. Listed for each Object Audit is: single ALL Users entry (traditional object Audit goes for any user) – audited or not.



Object Audit Report fields:

Name	Description
Object Owner	Owner of the object
Object Name	Name of the object
Object Type	Type of the object
Object Audit	Object Audit Option
Obj. Priv. *	Is object privilege
User	ALL Users
Audit Mode	Mode of Object Audit 0 A0 No Audit Not audited 1 A1 Partial Audit Partial Audit 2 A2 Full Audit Full Audit
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for Object Audit ** 0 Generic Object Fully Audited 1 Info Object Partially Audited, is not Object Privilege 2 Low Object Partially Audited, is Object Privilege 3 Medium Object is not Audited, is not Object Privilege 4 High Object is not Audited, is Object Privilege
Control Output	Object audit details.

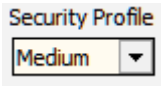
* The Object Audit option as an explicit Object Privilege impacts the Control evaluation.
** In Traditional Audit an audit set on an object is effective for ALL user accounts!

3.3.7 User Password Resources Report

To assess and report on Oracle Database User Password Resources, in the application's main menu, first tab DB Security Reports, group Profile Resources, click on the button User Passwords. Form User Password Resources Report will open.

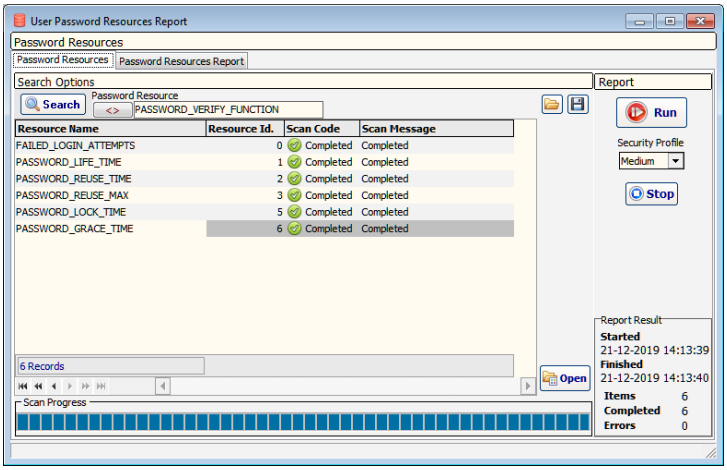
In the first tab Password Resources, complete the search inputs, or load them from disk, and press the button Search to retrieve the Password Resources that will be reported from the Target Database.

A new Report is run on the Report group on the right. Report inputs are:

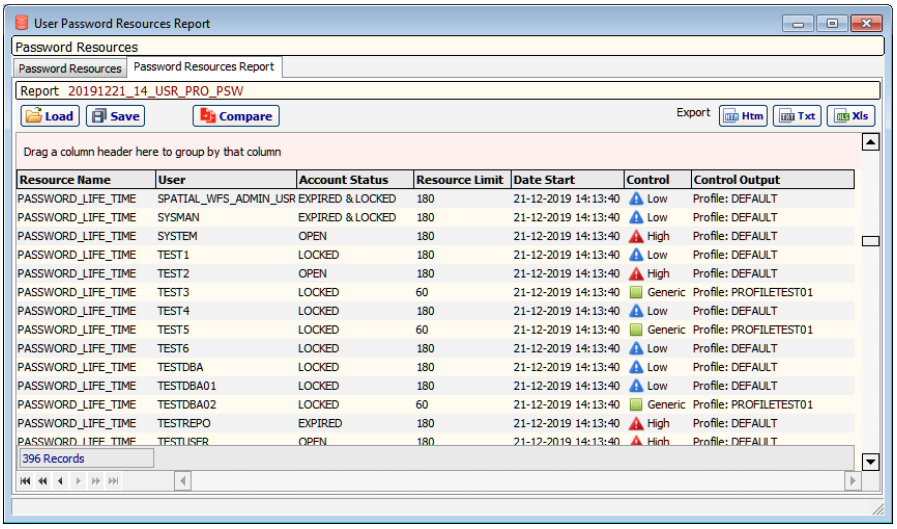


will define Resource Limit threshold Values used to match reported ones for each User account. Persisted as application data and visible on form "Password Resources Security Levels".

Press the button Run to generate a new Report and wait until all Items complete.



In the second tab Password Resources Report, the completed report is displayed. Listed for each Password Resource are: All users, within or exceeding the Security Profile Limit.



Password Resources Report fields:

Name	Description
Resource Name	System privilege name
User	User account
Account Status	User Account Status
Resource Limit	User Resource Limit *
Date Start	DateTime of Item report
Control	Evaluated Result of Report Item for User. 0 Generic Resource Limit not exceeded 2 Low Resource Limit exceeded, Account is Locked 4 High Resource Limit exceeded, Account is Unlocked
Control Output	User details on password resource

* evaluation of the User's reported resource vs the Security Level limit is evaluated for each Resource Name as in the table below:

Resource Name	Limit exceeded when:
PASSWORD_VERIFY_FUNCTION	NULL (no function) found
FAILED_LOGIN_ATTEMPTS	UNLIMITED found or Greater Then (>) Security Limit
PASSWORD_LIFE_TIME	UNLIMITED found or Greater Then (>) Security Limit
PASSWORD_GRACE_TIME	UNLIMITED found or Greater Then (>) Security Limit
INACTIVE_ACCOUNT_TIME	UNLIMITED found or Greater Then (>) Security Limit
PASSWORD_LOCK_TIME	Less Then (<) Security Limit
PASSWORD_REUSE_TIME *	Less Then (<) Security Limit
PASSWORD_REUSE_MAX *	Less Then (<) Security Limit

* these last two Password Reuse resources work in conjunction with each other. The evaluation above is performed only when both values have been set (UNLIMITED as default). If one of them has been set while the other is UNLIMITED this is *not* considered as an "limit exceed" because the user will not be able to reuse any of its previous passwords. When both UNLIMITED this is a "limit exceed" for both.

Note

User accounts of Authentication Type different from Password (ex. eternal/global) will always evaluate as Generic!

For more details, refer to Oracle (12c R2) Documentation on:

CREATE PROFILE
https://docs.oracle.com/en/database/oracle/oracle-database/12.2/sqlrf/CREATE-PROFILE.html#GUID-ABC7AE4D-64A8-4EA9-857D-BEF7300B64C3

… specifically on topic:
PASSWORD_REUSE_TIME and PASSWORD_REUSE_MAX

4 CHAPTER 4: Tools

4.1 Security Reports Comparison

Reporting is of top-importance in providing a snapshot of the current situation – assessment time – of the security posture of the Database. But alone it is unable to provide a clear view on the next item most important behind report itself: Change Management of the security posture.

Reports can involve thousands of records. A visual-only comparison would find it impossible (even with hundreds) to distinguish with clarity and precision the changes performed between the two reports. Report Comparison – a feature available to all Report Classes and Types – Overall and ad-hoc – highlights and categorizes the changes, from the slightest to most important, between two different reports - Target and Baseline.

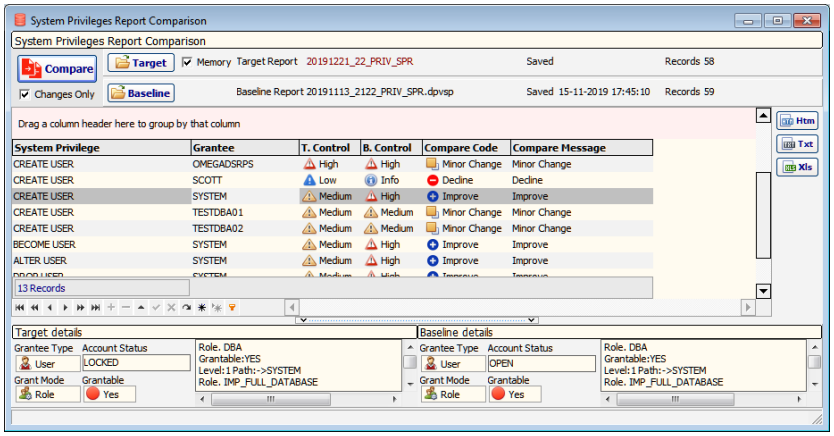
Comparison consists in matching individual items of a Target Report vs those of a Baseline one and making an evaluated and categorized decision on the quality and scope of the (eventual) change – from minor to important.

4.1.1 Common Comparison Features

All Security Report Comparison forms, like the Reports, share common features.

Initially the Target and Baseline Reports are loaded from disk with the respective buttons. The Target Report can also be loaded from Memory - the last report run on the respective Report form, or alternatively, from the same form, using the Compare button on top of Report records in the second tab.

Press the button Compare to generate a new Comparison Report between Target and Baseline ones.
Wait for the Comparison to complete!
You can display changes only (Changes only - default), or all records.



Field[s] on the left (System Privilege in this example) describe[s] the Security Item compared for the Grantee/User, specific to each Report Class. Next are the Control fields for each Report - Target and Baseline. The last two on the right describe the records comparison: Compare Code and Compare Message

Export the comparison in:

Htm, Txt and Xls formats

System Privileges ad-hoc Reports - Comparison

Target Details and Baseline Details bottom groups display other fields respectively from the Target and Baseline Reports. DB memos feature fields Control Output. Comparison Report is exportable as Htm, Txt and Xls files.

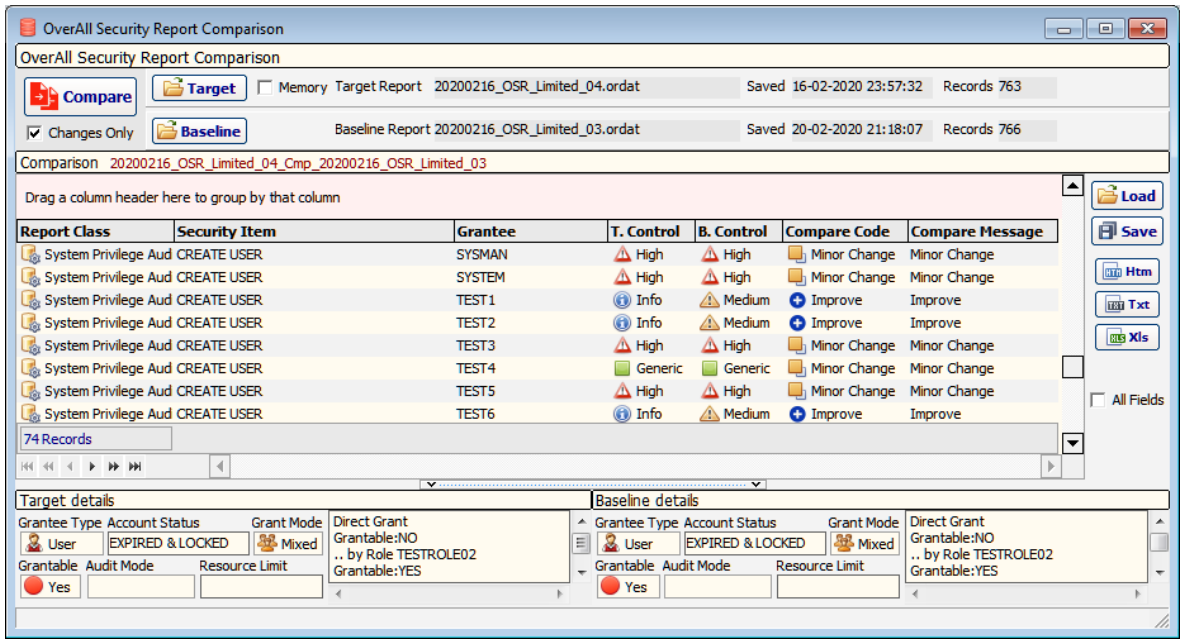
Reminder

Target and Baseline Reports being compared must (obviously) belong to the same Report Class, and their Security Items input lists must have been initially searched with the same (similar, improved or changed) Search Options, and, where applies, also with the same Report Input parameters!

4.1.2 Overall Security Reports Comparison

To compare two Overall Security Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button Overall Security. Form Overall Security Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



Loads an Overall Security Comparison Report from disk.

Saves an Overall Security Comparison Report to disk.

Checked will display the class-specific Report fields

Overall Security Report Comparison fields:

Name	Description
Report Class	Class of the Report
Security Item	Security Item specific by each Class
Grantee	Grantee – User or Role for privilege-like Classes, User for others
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code *	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed 2 Improve — Control decremented Old Grantee/User 3 Public Improve — Old PUBLIC Grantee 5 Decline — Control incremented New Grantee/User 6 Public Decline — New PUBLIC Grantee
Compare Message	Comparison message

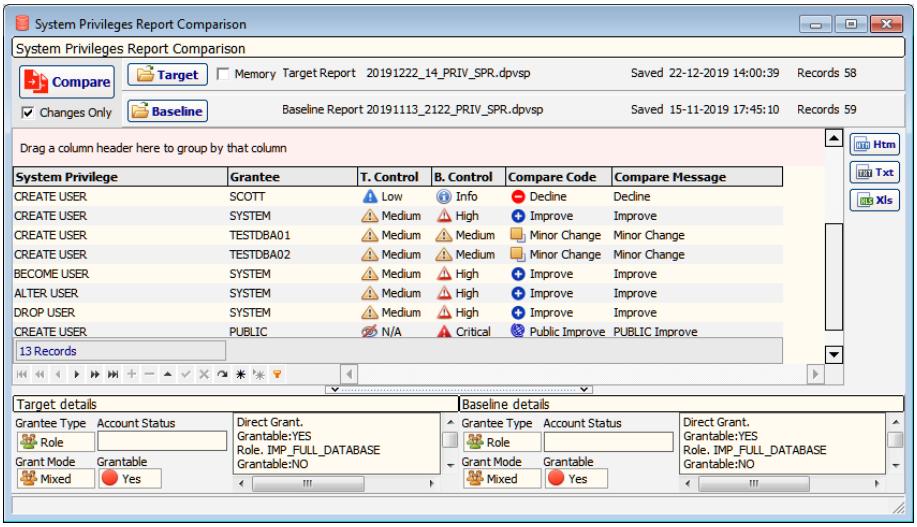
* For more details on Compare Codes refer to each class-specific topic of ad-hoc Report Comparison, and also to Appendix A3 - Report Classes and Application Codes.

4.1.3 Ad-hoc Reports - Comparison

4.1.3.1 System Privileges - Comparison

To compare two System Privileges Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button System Privileges. Form System Privileges Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



System Privileges Comparison Report fields:

Name	Description
System Privilege	System privilege name
Grantee	Grantee of the privilege
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed 2 Improve — Control decremented (5->0) Old Grantee * 3 Public Improve — Old PUBLIC Grantee 5 Decline — Control incremented (0->5) New Grantee ** 6 Public Decline — New PUBLIC Grantee
Compare Message	Comparison message

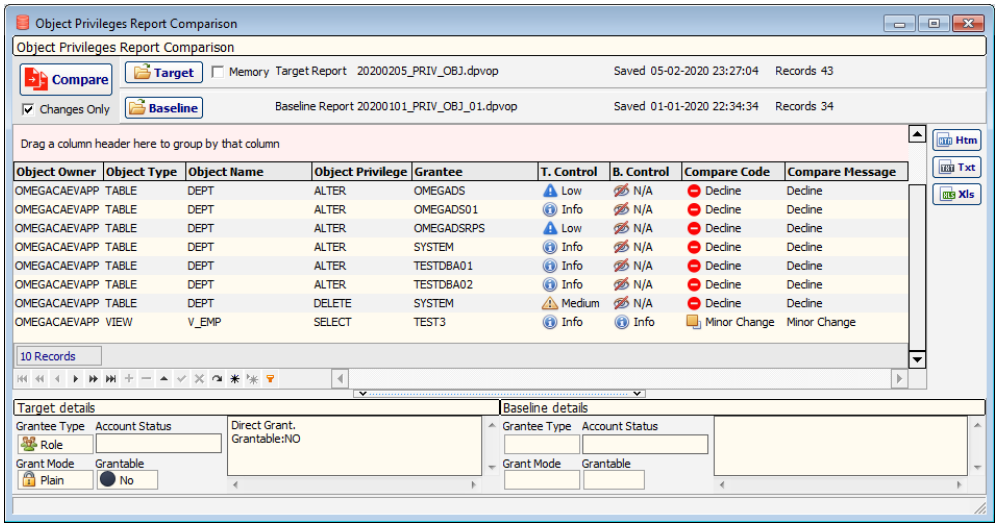
Legend (valid for all Comparisons Reports of Privilege type):

* Old Grantee — Privilege not found for Grantee in Target
** New Grantee — Privilege not found for Grantee in Baseline

4.1.3.2 Object Privileges - Comparison

To compare two Object Privileges Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button Object Privileges. Form Object Privileges Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



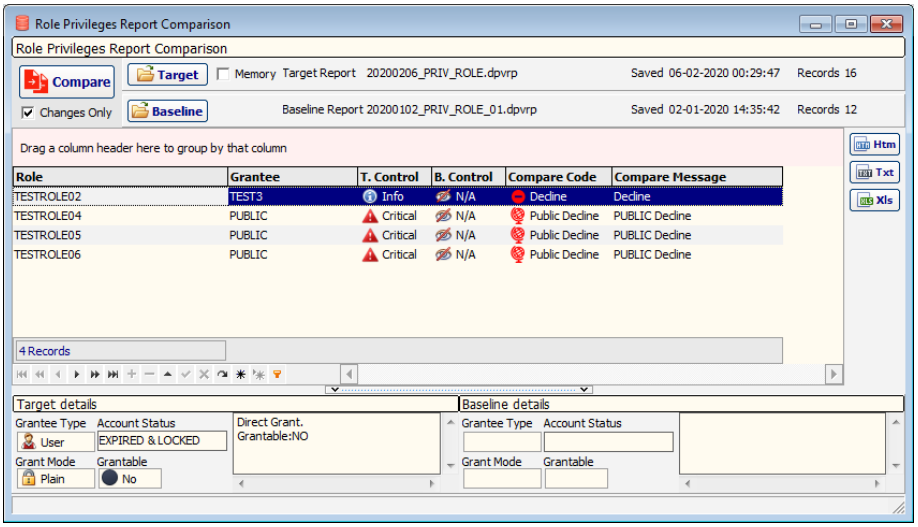
Object Privileges Comparison Report fields:

Name	Description
Object Owner	Owner of the object
Object Name	Name of the object
Object Type	Type of the object
Object Privilege	Object Privilege
Grantee	Grantee of the privilege
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed 2 Improve — Control decremented (5->0) Old Grantee 3 Public Improve — Old PUBLIC Grantee 5 Decline — Control incremented (0->5) New Grantee 6 Public Decline — New PUBLIC Grantee
Compare Message	Comparison message

4.1.3.3 Role Privileges - Comparison

To compare two Role Privileges Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button Role Privileges. Form Role Privileges Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



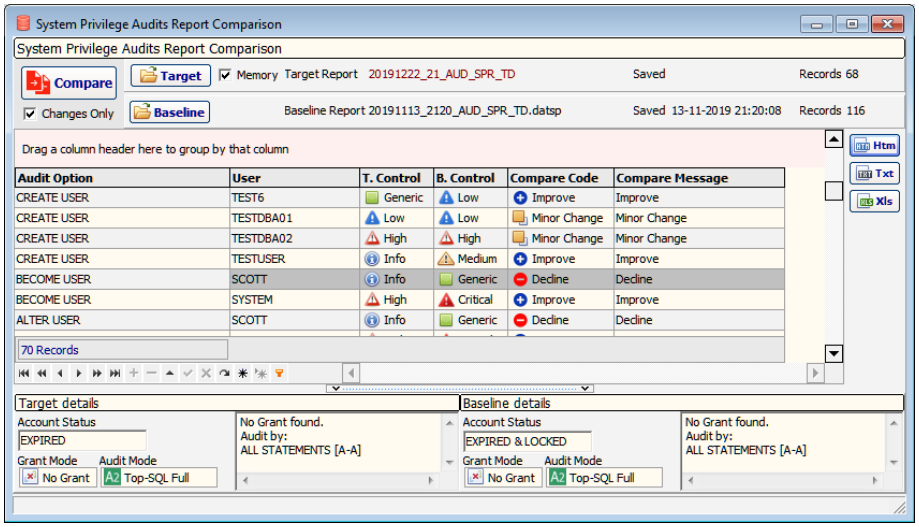
Role Privileges Comparison Report fields:

Name	Description
Role	Role Name
Grantee	Grantee of the privilege
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed 2 Improve — Control decremented (5->0) Old Grantee 3 Public Improve — Old PUBLIC Grantee 5 Decline — Control incremented (0->5) New Grantee 6 Public Decline — New PUBLIC Grantee
Compare Message	Comparison message

4.1.3.4 System Privilege Audits - Comparison

To compare two System Privilege Audits Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button System Privilege Audits. Form System Privilege Audits Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



System Privilege Audits Comparison Report fields:

Name	Description
Audit Option	Audit option (System Privilege)
User	User account
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed Old/New User Control=0 2 Improve — Control decremented (5->0) Old User Control in 1-5 * 5 Decline — Control incremented (0->5) New User Control in 1-5 **
Compare Message	Comparison message

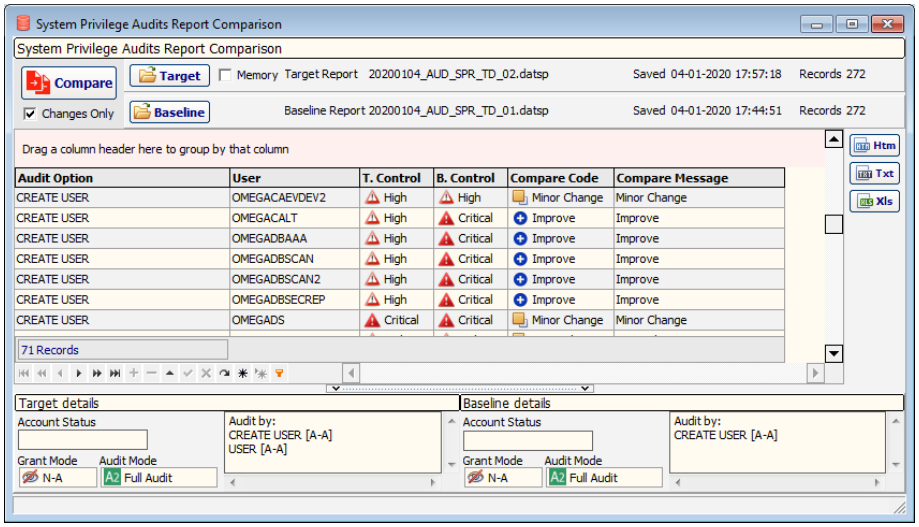
Legend (valid also for Statement and Shortcut Audit Report):

* Old User — Audit Option not found for User in Target
** New User — Audit Option not found for User in Baseline

4.1.3.5 Statement and Shortcut Audits - Comparison

To compare two Statement and Shortcut Audits Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button Statement and Shortcut Audits. Form Statement and Shortcut Audits Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



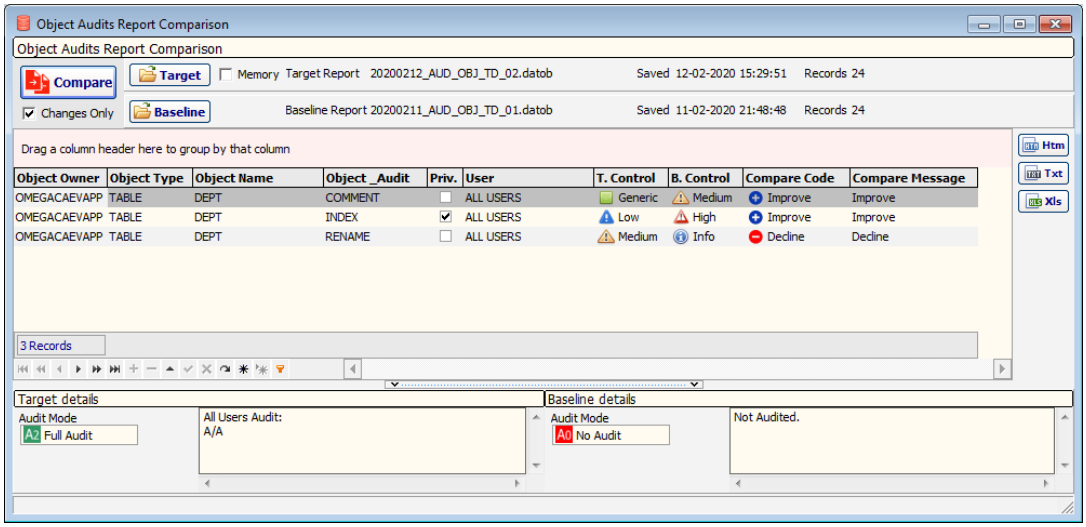
Statement and Shortcut Audits Comparison Report fields:

Name	Description
Audit Option	Audit option (System Privilege)
User	User account
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed Old/New User Control=0 2 Improve — Control decremented (4->0) Old User Control in 1-4 5 Decline — Control incremented (0->4) New User Control in 1-4
Compare Message	Comparison message

4.1.3.6 Object Audits - Comparison

To compare two Object Audits Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button Object Audits. Form Object Audits Report Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



Object Audits Comparison Report fields:

Name	Description
Object Owner	Owner of the object
Object Name	Name of the object
Object Type	Type of the object
Object Audit	Object Audit Option
Priv.	Is object privilege
User	User account
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed Old/New Object Control=0 2 Improve — Control decremented (4->0) Old Object Control in 1-4 * 5 Decline — Control incremented (0->4) New Object Control in 1-4 **
Compare Message	Comparison message

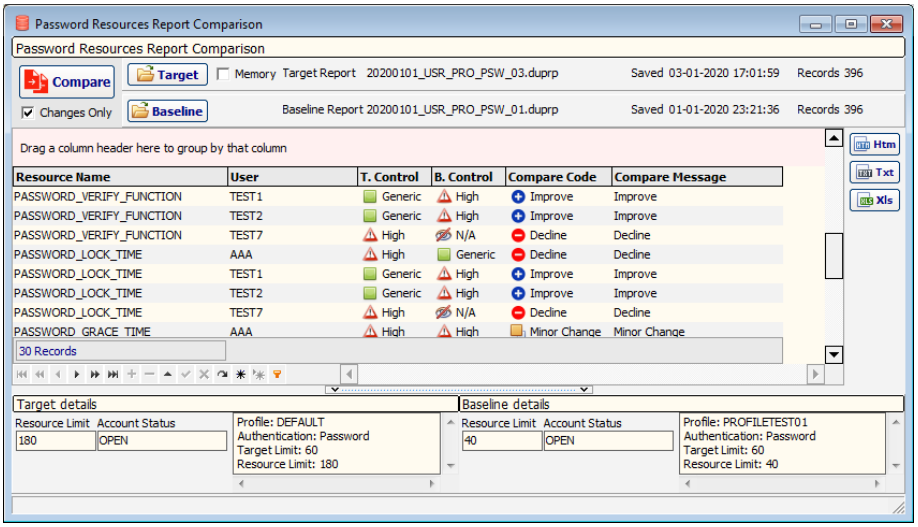
Legend:

* Old Object Audit Option not found for Object in Target
** New Object Audit Option not found for Object in Baseline

4.1.3.7 User Password Resources - Comparison

To compare two Password Resources Reports, in the application's main menu, second tab Tools, drop-down list Compare Reports, and click on the button Password Resources. Form User Password Resources Comparison will open.

Load the Target and Baseline Reports and press the button Compare to generate the Comparison Report.



Password Resources Comparison Report fields:

Name	Description
Resource Name	Password Resource name
User	User
T. Control	Control result of Target Report
B. Control	Control result of Baseline Report
Compare Code	Comparison Result Code 0 Unchanged — Control and Control Output unchanged 1 Minor Change — Control unchanged, Control Output changed Old/New User Control=0 2 Improve — Control decremented (4->0) Old User Control in 2,4 * 5 Decline — Control incremented (0->4) New User Control 2,4 **
Compare Message	Comparison message

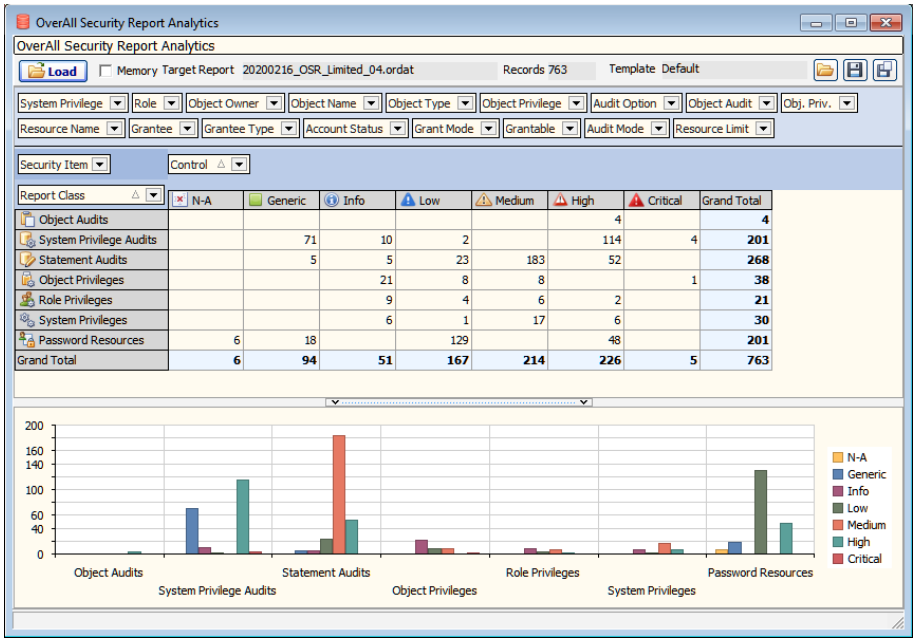
Legend:

* Old User Password Resource not found for User in Target
** New User Password Resource not found for User in Baseline

4.2 Overall Security Analytics

Graphical analytics of Overall Security Report's data is another important feature of this application. It is accessible in the Application's main menu, second tab Tools, clicking on the button Overall Security Analytics. Form Overall Security Report Analytics will open.

Use button Load to load the Overall Security Report from disk. The Report can also be loaded from Memory - the last report run on the Overall Security Report form, or alternatively, from the same form, using the Compare button on top of Report records in the second tab.



Pivot grid

On the top Pivot grid enables end-user to re-arrange report data fields in rows and columns with drag-and-drop functionality and having row, column and grand totals (as Counts) calculated on the fly. Can interchange columns and rows on the fly, filter and sort items in different ways, and also collapse and expand data at different levels.

Areas of the pivot:

Filter Header Area	filter operations only fields, shows not on pivot
Data Header Area	measure field "Security Items", Count.
Row Header Area	dimension row fields, default "Report Class"
Column Header Area	dimension column fields, default "Control"

Pivot Chart

Below a report data chart component responds dynamically to the related pivot. Chart's vertical axis is the pivot Data Area measure (Count) field Security Items; in the horizontal axis are the pivot's rows, while the diagram's vertical bars represent the pivot's columns. In both later expand and collapse is reflected.

On form's top on right, the Analytics Template (setup for pivot and chart) is displayed. Functionalities are:

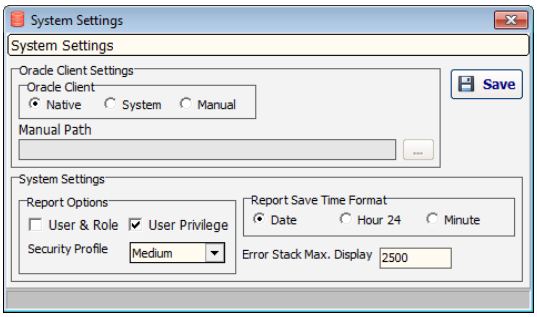
Open	loads an Analytics Template. Three available, other than Default.
Save	saves the loaded Analytics Template
Save As	saves the Analytics Template as a new entry

Analytics Template are visible in form Overall Security Analytics Templates!

5 CHAPTER 5: Others

5.1 System Settings

To view the system settings, in the Application's main menu tab Options, group System, click on the button Settings. Form System Settings will open.



Oracle Client Settings:

Oracle Client — Oracle client connectivity settings, available options are:

- Native — built-in application connectivity, OCI deployed files
- System — operating system installed and default Oracle client
- Manual — manual Oracle client oci.dll path specification, usually for Oracle Instant Client, but others (non-Instant) can be referenced too.

Note:
Changing the Oracle Client requires an application restart to take effect!
Refer to the "Appendix A2 - Oracle Connection Settings".

System Settings:

Report Options

User & Role	default (and recommended) parameter for all Privilege Reports
User Privilege	default (and recommended) parameter for System Privilege Audits report
Security Profile	default input Security Profile for Password Resources report

Report Save Time Format — will set the first part of the Report File Name * according to options:

• Date	yyyymmdd	ex. 20170901
• Hour 24	yyyymmdd_hh24	ex. 20170901_19
• Minute	yyyymmdd_hh24mi	ex. 20170901_1933

Error Stack Max. Display — Maximum length for Prompt (message display) of full Exception Stack. Will display only that first number of characters for screen convenience. No impact on Clipboard copy – refer next topic

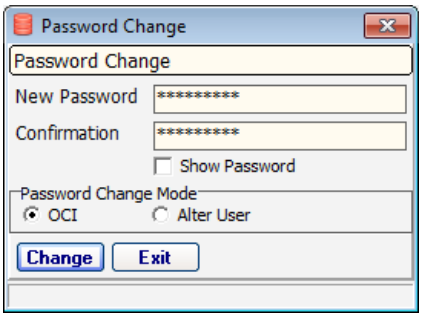
*** Report File Name:**

The first time a new report is run, its name is automatically generated according to its Report Class Code (refer to Appendix A3 - Report Classes and Application Codes!) and to the initialization parameter "Report Save Time Format". For example, for a later set to "Date", and a System Privileges ad-hoc Report, running a new report on 14 February 2020, will generate a name as: 20200214_PRIV_SPR. This is the prompted filename you will see in the save dialog when you first save the report to disk after run! The OSR is used as Class Code for Overall Security Reports.

Press the button Save to permanently save your settings!

5.2 Password Change

When connected to the Target Database, you can change the connected user's password; in the Application's main menu tab Options, group System, click on the button Password Change. Form Password Change will open.

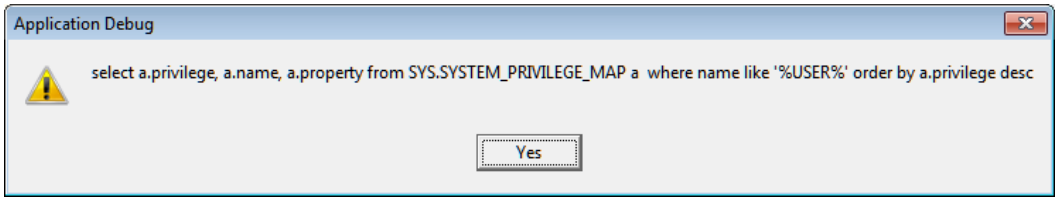


Enter the new Password and confirm it. The mode of password change can be OCI (default and recommended) or an ALTER USER… SQL command – user changing its own password. Press button Change.

5.3 Application Debug

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



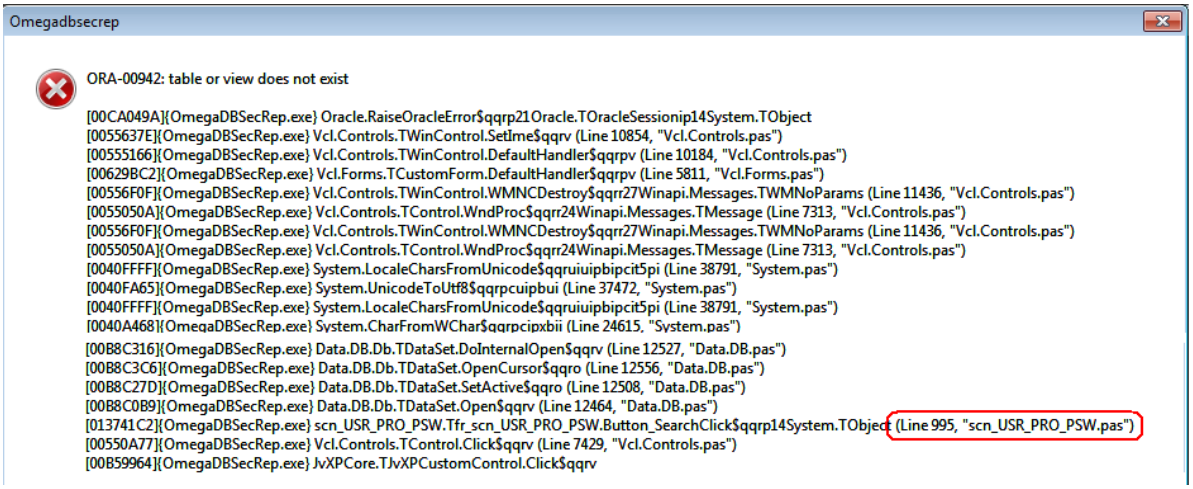
Debug example of SQL retrieving System Privileges for report input

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

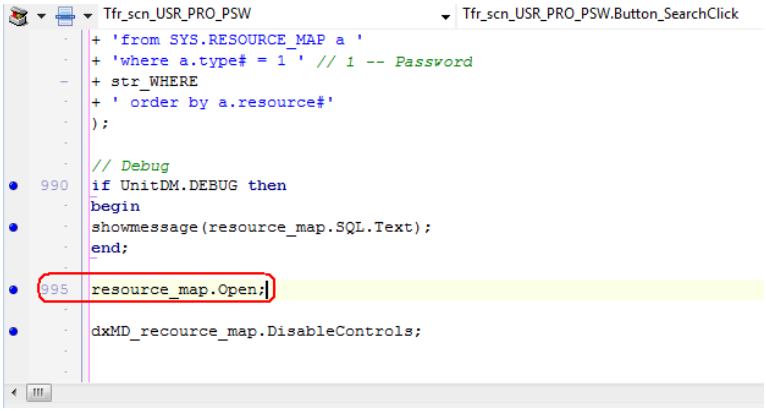
Full Error Stack

The Full Error Stack produces extra debug information on eventual program errors.
The Full Error Stack is controlled by the Application's Debug status!

Its 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

[00CA049A]{OmegaDBSecRep.exe} Oracle.RaiseOracleError$qqrp21Oracle.TOracleSessionip14System.TObject
[0055637E]{OmegaDBSecRep.exe} Vcl.Controls.TWinControl.SetIme$qqrv (Line 10854, "Vcl.Controls.pas")
[00555166]{OmegaDBSecRep.exe} Vcl.Controls.TWinControl.DefaultHandler$qqrpv (Line 10184, "Vcl.Controls.pas")
[00629BC2]{OmegaDBSecRep.exe} Vcl.Forms.TCustomForm.DefaultHandler$qqrpv (Line 5811, "Vcl.Forms.pas")
[00556F0F]{OmegaDBSecRep.exe} Vcl.Controls.TWinControl.WMNCDestroy$qqrr27Winapi.Messages.TWMNoParams (Line 11436, "Vcl.Controls.pas")
[0055050A]{OmegaDBSecRep.exe} Vcl.Controls.TControl.WndProc$qqrr24Winapi.Messages.TMessage (Line 7313, "Vcl.Controls.pas")
[00556F0F]{OmegaDBSecRep.exe} Vcl.Controls.TWinControl.WMNCDestroy$qqrr27Winapi.Messages.TWMNoParams (Line 11436, "Vcl.Controls.pas")
[0055050A]{OmegaDBSecRep.exe} Vcl.Controls.TControl.WndProc$qqrr24Winapi.Messages.TMessage (Line 7313, "Vcl.Controls.pas")
[0040FFFF]{OmegaDBSecRep.exe} System.LocaleCharsFromUnicode$qqruiuipbipcit5pi (Line 38791, "System.pas")
[0040FA65]{OmegaDBSecRep.exe} System.UnicodeToUtf8$qqrpcuipbui (Line 37472, "System.pas")
[0040FFFF]{OmegaDBSecRep.exe} System.LocaleCharsFromUnicode$qqruiuipbipcit5pi (Line 38791, "System.pas")
[0040A468]{OmegaDBSecRep.exe} System.CharFromWChar$qqrpcipxbii (Line 24615, "System.pas")
[00B8C316]{OmegaDBSecRep.exe} Data.DB.Db.TDataSet.DoInternalOpen$qqrv (Line 12527, "Data.DB.pas")
[00B8C3C6]{OmegaDBSecRep.exe} Data.DB.Db.TDataSet.OpenCursor$qqro (Line 12556, "Data.DB.pas")
[00B8C27D]{OmegaDBSecRep.exe} Data.DB.Db.TDataSet.SetActive$qqro (Line 12508, "Data.DB.pas")
[00B8C0B9]{OmegaDBSecRep.exe} Data.DB.Db.TDataSet.Open$qqrv (Line 12464, "Data.DB.pas")
[013741C2]{OmegaDBSecRep.exe} scn_USR_PRO_PSW.Tfr_scn_USR_PRO_PSW.Button_SearchClick$qqrp14System.TObject (Line 995, "scn_USR_PRO_PSW.pas")
[00550A77]{OmegaDBSecRep.exe} Vcl.Controls.TControl.Click$qqrv (Line 7429, "Vcl.Controls.pas")
[00B59964]{OmegaDBSecRep.exe} JvXPCore.TJvXPCustomControl.Click$qqrv
```

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

Database-Side Debug

This Application is also fully traceable on the Oracle Database side for all activities on it. Other then user session tracing, the following approaches are available too:

1. Monitor of DBA_AUDIT_TRAILS
   with ALL STATEMENTS (or more) Audit on the reporting Oracle account (OMEGADBSECREP)

2. Monitor of V$SQLAREA

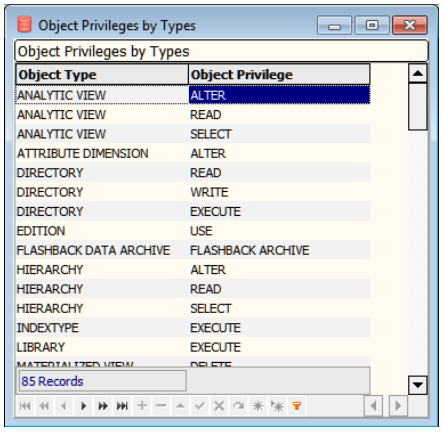
5.4 Application Data

The Application contains data that are necessary for its internal operations and for configurations. They are accessible in the Application's main menu, tab Options, group Application Data, with respective buttons for each.

The buttons will open respectively the following Application forms as below:

Object Privileges by Type

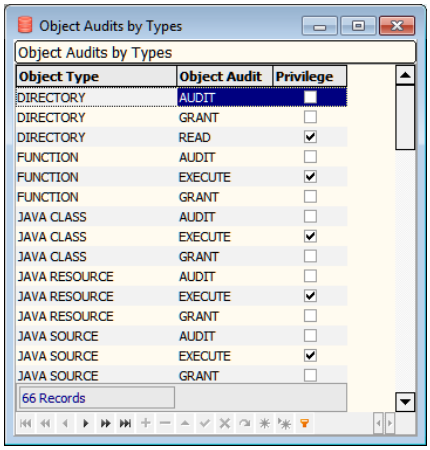
Data used by Object Privileges Report Class.



Persisted in application deployed text file: sys_obj_type_priv.txt

Object Audits by Type

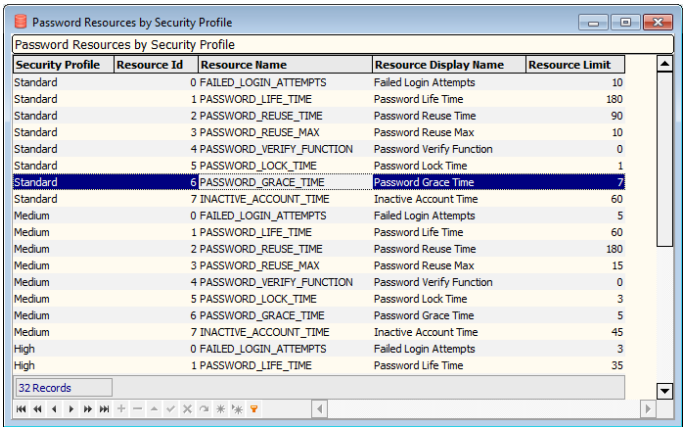
Data used by (Traditional) Object Audit Report Class.



Persisted in application deployed text file: sys_obj_type_aud_td.txt

Password Resources by Security Profile

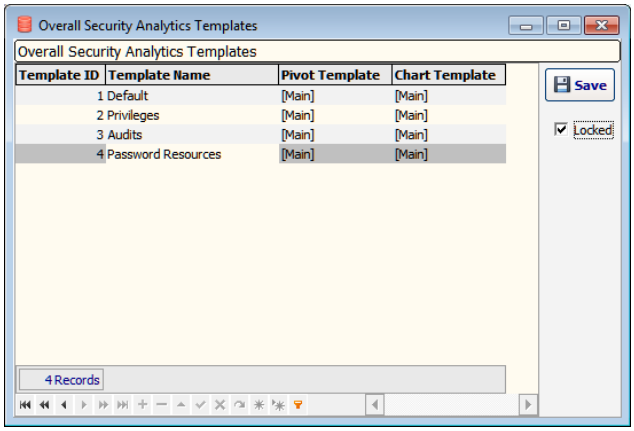
Data used by Password Resources Report Class.



Persisted in application deployed text file: sys_usr_pro_rsc.txt

Overall Security Analytics Templates

Data used for persisting Overall Security Report Analytics Templates.
Persisted in application deployed binary file: sys_osr_anls.db



Locked — un-checking will enable edit of the data.
Use the grid's navigator's buttons to perform necessary actions (see Note below).

Save — saves the data permanently to disk

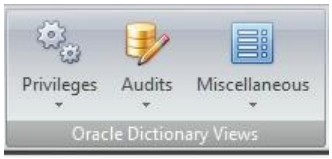
Other than the Default one, the application provides three pre-defined Analytics Templates: Privileges, Audits and Password Resources. As their name implies, they are used for a customized presentation of respective Report Classes. Others can be added, and all edited, from Template management on form Overall Security Report Analytics.

Note:

Application data's are generally available for presentation only. In rare cases, and with DATAPLUS advise and permission, the text files can be edited outside the application - they are presented read-only in it.
Under same conditions, but from within the application, the Overall Security Analytics Templates can be edited in the respective form.

5.5 Oracle Dictionary Views

The Application enables direct search and view on certain important security-related Oracle Dictionary views. The respective application forms are launched from the buttons found under main menu's tab Options, group Oracle Dictionary Views.



The drop-down buttons will open the following Application forms as in the table below. Column on the right shows the Oracle Dictionary views searched/displayed by each form.

Form Name	Oracle Dictionary View
Oracle System Privileges	DBA_SYS_PRIVS
Oracle Object Privileges	DBA_TAB_PRIVS
Oracle Role Privileges	DBA_ROLE_PRIVS
Oracle Statement Audits	DBA_STMT_AUDIT_OPTS
Oracle Object Audits	DBA_OBJ_AUDIT_OPTS
Oracle Fine-Grained Audit Policies	DBA_AUDIT_POLICIES
Oracle Users	DBA_USERS
Oracle Roles	DBA_ROLES
Oracle Objects	DBA_OBJECTS
Oracle Password Resources	DBA_PROFILES

In all forms above focusing on the Oracle "side" the options of exporting data in Xls, Txt and Htm is available.

Press the Export button on the right of each data grid and make the file type of your choice.

6 Appendixes

6.1 Appendix A1 - Oracle Database Account for Reporting

Omega DB Security Reporter is Agent-less and accesses the target database in a read-only mode. Of course an Oracle user account is necessary to access the target database and perform the report. This account is created with the CREATE SESSION only system privilege and with SELECT only privileges in certain Oracle dictionary views, necessary to extract the security information.

Use the SQL commands below in 3 Steps to create the report user account and assign privileges:

-- STEP 1. Create the user account
-- Username OMEGADBSECREP is optional, however recommended. Replace <Password> with your choice.

```
create user OMEGADBSECREP identified by <Password>;
```

-- STEP 2. Grant connect privilege

```
grant create session to OMEGADBSECREP;
```

-- STEP 3. Grant object privileges

```
grant select on DBA_AUDIT_POLICIES to OMEGADBSECREP;
grant select on DBA_OBJECTS to OMEGADBSECREP;
grant select on DBA_OBJ_AUDIT_OPTS to OMEGADBSECREP;
grant select on DBA_PROFILES to OMEGADBSECREP;
grant select on DBA_ROLES to OMEGADBSECREP;
grant select on DBA_ROLE_PRIVS to OMEGADBSECREP;
grant select on DBA_STMT_AUDIT_OPTS to OMEGADBSECREP;
grant select on DBA_SYS_PRIVS to OMEGADBSECREP;
grant select on DBA_TAB_PRIVS to OMEGADBSECREP;
grant select on DBA_USERS to OMEGADBSECREP;
grant select on RESOURCE_MAP to OMEGADBSECREP;
grant select on STMT_AUDIT_OPTION_MAP to OMEGADBSECREP;
grant select on SYSTEM_PRIVILEGE_MAP to OMEGADBSECREP;
grant select on TABLE_PRIVILEGE_MAP to OMEGADBSECREP;
grant select on V_$DATABASE to OMEGADBSECREP;
grant select on V_$INSTANCE to OMEGADBSECREP;
grant select on V_$PARAMETER to OMEGADBSECREP;
```

Note:
It is advised to connect as SYS to run the commands above as the normal DBA might not have by default rights in all of them (ex. SYS table RESOURCE_MAP)!

Alternatively last step's (STEP 3) commands can be replaced by:

```
grant SELECT ANY DICTIONARY to OMEGADBSECREP;
```

however this is not advised as it will give read-rights on all Oracle dictionary while needed is only the above!

To drop the report user account, run the following SQL command:

```
drop user OMEGADBSECREP;
```

6.2 Appendix A2 - Oracle Connection Settings

6.2.1 Oracle Client Connectivity

Omega DB Security Reporter uses Oracle Instant Client win-32 libraries for Oracle database connectivity.

This is also a built-in and pre-deployed functionality of the application, thus you don't have to setup or install anything, at least as long as Oracle Client setting is set (default) to Native into the System Settings form; just ensure the Oracle OCI files are in the same folder with the application's .exe.

You can connect also with any 32 Bit Oracle Client, 11gR2 or higher, installed or instant.
In case you have an OS default existing Oracle Client 64 bit, or even a Multiple Oracle Homes (Clients) environment, you can still use the built-in application's Native connectivity (default), or use another Oracle Instant Client 32 bit.

Connectivity Limitations

1. Connectivity from the application is currently supported only on 32 Bit Oracle Clients
2. Change of expired password is valid only when using the operating system's Oracle Client and not for the default native Instant one. In the later the password change will fail with error: "ORA-01017: invalid username/password; logon denied".

6.2.2 Character Set Support

Omega DB Security Reporter uses the NLS_LANG system environment variable to specify locale settings for the Oracle client software used by the application. This variable sets the language and territory and also indicates the client's character set, which corresponds to the character set for data to be entered or displayed by a client program.

The NLS_LANG is an operating system environment variable that relates exclusively to Oracle client software. In case of a clean Windows install will not be present! You can create and manage it as any other Windows environment variable. For example on a Windows 7 machine at Control Panel -> System -> Advanced System Settings - and in the System Properties form that opens, selected tab Advanced, press the "Environment Variables…" button. Form Environment Variables will open, look for System Variables below!

If your Oracle database uses pure Latin/ASCII Western European languages character sets, you don't need to create and set the NLS_LANG at all!

You must create and set this system variable if you need to support:

- Western European Languages in full - with special characters like ë, Ë, ç, Ç, ö, Ö!
- Other single-bytes character sets
- Unicode character sets - for all languages!

The NLS_LANG environment variable has the following format:
NLS_LANG = LANGUAGE_TERRITORY.CHARSET

Example 1
Western European Languages full character support:
NLS_LANG= AMERICAN_AMERICA.WE8MSWIN1252

Example 2

Unicode character support:
NLS_LANG= AMERICAN_AMERICA.AL32UTF8

In general, settings of NLS_LANG are required and set according to Oracle Client Vs Oracle Database technology character sets configurations; the Omega DB Security Reporter uses an relies on the Oracle Client for connectivity like many other Oracle-related software do.

For more, refer to the Oracle Documentation on "Choosing a Locale with the NLS_LANG Environment Variable"!
https://docs.oracle.com/cd/E18283_01/server.112/e10729/ch3globenv.htm#insertedID2

6.3 Appendix A3 - Report Classes and Application Codes

Report Classes

Class Code	Application form *	Object of Assessment	Assessment for:
PRIV_SPR	System Privileges Report	System Privilege	Grantees
PRIV_OBJ	Object Privileges Report	Object Privilege	Grantees
PRIV_ROLE	Role Privileges Report	Role Privilege	Grantees
AUD_SPR_TD	System Privilege Audits Report	System Privilege Audit option	Users
AUD_STM_TD	Statement and Shortcut Audits Report	Statement and Shortcut Audit option	Users
AUD_OBJ_TD	Object Audit Report	Object Audit option	Object
USR_PRO_PSW	User Password Resources Report	User Password Resource	Users

* available also on the form Overall Security Report and on each respective single Report form

Hint:
In the Application the Report Class Codes are visible when used as part of the report file name on save.

Grant Modes

Grant Modes used in privilege-like reports.

Mode Id	Grant Mode Name	Grant Mode Description	SPR	OPR	RPR	AUD Sp.
0	None	Privilege not granted	-	-	-	x
1	Plain	Granted Directly	x	x	x	x
2	Role	Granted through least one role	x	x	x	x
3	Mixed	Granted directly and through least one role	x	x	x	x
4	Public	Granted to PUBLIC	-	-	-	x
-1	N-A	Not Applicable *	-	-	-	x

Grant and Audit Modes Legend:

SPR	System Privilege	AUD Sp.	System Privilege Audit
OPR	Object Privilege	AUD St.	Statement/Shortcut Audit
RPR	Role Privilege	AUD Ob.	Object Audit

* when User Privilege unchecked

Audit Modes

Audit Modes used in audit-like reports.

Mode Id	Audit Mode Name	Audit Mode Description	AUD Sp.	AUD St.	AUD Ob.
0	A0 No Audit	Plain Audit: None Top-SQL Audit: None	x	x	x
1	A1 Partial Audit	Plain Audit: None, Partial Top-SQL Audit: None, Partial, Full	x	x	x
2	A2 Full Audit	Plain Audit: Full Top-SQL Audit: None, Partial, Full	x	x	x

Audit Mode Legend:

Plain Audit	A direct audit on a User Statement or Object, in the first also through a shortcut
Top-SQL Audit	Audited on Top-SQL level (by ALL STATEMENTS)
Partial	Audited by SESSION and/or by one of SUCCESS/FAILURE
Full	Audited directly by ACCESS for both SUCCESS/FAILURE

Control Codes

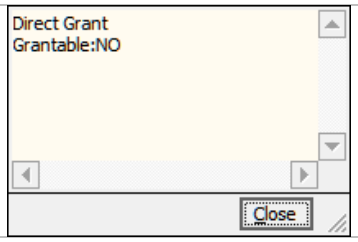
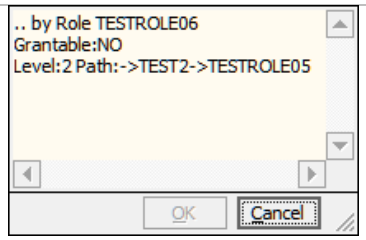
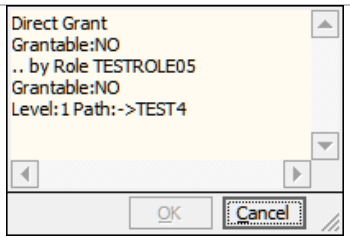
Control codes used for all reports.

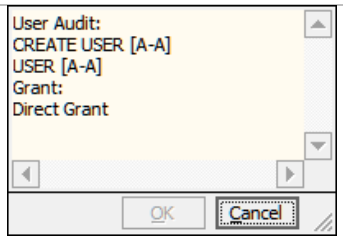
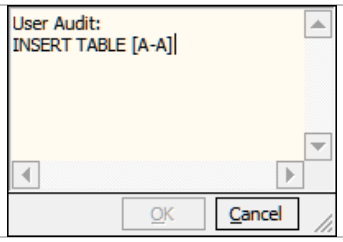
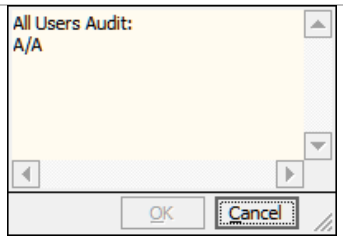
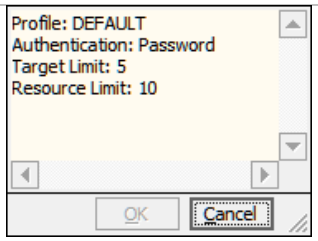
Control Id	Control Name	All Privileges *	Audit Sys. Priv.	Audit Stmt & Short.	Audit Object	User Pass. Resource
0	Generic	x	x	x	x	x
1	Info	x	x	x	x	-
2	Low	x	x	x	x	x
3	Medium	x	x	x	x	-
4	High	x	x	x	x	x
5	Critical	x	x	-	-	-
-1	N-A **					

* All Privileges — System, Object and Role privileges
* N-A — Evaluation not performed - error condition - not supposed to encounter. Report to support! Sole exception is the Control result as N-A for non-Password authenticated user accounts in the "User Password Resources" report class.

Control Details

Control Output – details by Report Classes:

Report Class	Report Output	Description
System Privileges		A System Privilege(ex. ALTER USER)* granted directly on the Grantee (User, or Role). * Security Item itself is not displayed on the Control Output field. No duplication, as a general rule, of information already available in other grid columns.
Object Privileges		An Object Privilege (ex. SELECT on table) initially granted to role TESTROLE06; the later, Grantee TEST2 is granted through another role, TESTROLE05 – Level 2! (SQL) Privilege schema: grant TESTROLE05 to TEST2; grant TESTROLE06 to TESTROLE05; grant SELECT on obj.name to TESTROLE06;
Role Privileges		A Role (ex. TESTROLE06) that Grantee TEST4 is granted directly and also by role TESTROLE05 – Level 1! (SQL) Privilege schema: grant TESTROLE06 to TEST; grant TESTROLE05 to TEST; grant TESTROLE06 to TESTROLE05;

System Privilege Audits		User is audited directly for System Privilege audit option CREATE USER, and for the same although by USER shortcut, both by access on success/failure (SQL) Privilege schema: audit CREATE USER by TEST1 BY ACCESS; audit CREATE USER by TEST1 BY ACCESS;
Statement Audits		User is audited directly for Statement audit option INSERT TABLE, by access on success/failure (SQL) Privilege schema: audit INSERT TABLE by TEST3 BY ACCESS;
Object Audits		All Users (Object Audit Traditional!) are audited on object action (ex. DELETE on table), by access on success/failure (SQL) Privilege schema: audit DELETE on obj.name BY ACCESS;
Password Resources		User's Password Resource Limit (ex. FAILED_LOGIN_ATTEMPTS) is displayed versus the required (Target) Limit objective (SQL) Privilege schema: create profile DEFAULT limit … FAILED_LOGIN_ATTEMPTS = 10 … ; create user TEST5 … profile DEFAULT …;

Compare Codes

Comparison codes used for all reports.

Compare Id	Compare Name	All Privileges	Audit Sys. Priv.	Audit Stmt. & Short.	Audit Object	User Pass. Resource
0	Unchanged	x	x	x	x	x
1	Minor Change	x	x	x	x	x
2	Improve	x	x	x	x	x
3	Public Improve	x	-	-	-	-
5	Decline	x	x	x	x	x
6	Public Decline	x	-	-	-	-
-1	Error *					

* Comparison Error, when one (or both) of Target/Baseline Control[s] is a N-A

6.4 Appendix A4 - Oracle Security Compliance

Common Oracle Security Checklists

Common available Oracle Security checklists contain a wide variety of controls. The Category appears as a specific field in some of them, mostly as a technical categorization by security area/configuration, as it is the case for CIS and SANS, while the field naming the control (usually Item/Index named) indicates categorization information too.

However, a quick look on the controls would also reveal that, purely from a database view – which is the object of the assessment, two main groups of score-able controls are available:

Extra-DB controls score-able by non-SQL commands/tools, outside the database
Intra-DB controls score-able by SQL/PL-SQL commands/tools, within a database session

In the first group, controls categorized as Operating System Settings, Oracle Directory/File Permissions, Installation and Patch, Networking, Encryption, Backup/Availability, General/Custom, and more, are to be found. Although many of them are of top importance, their common quality is that they address security configurations that are exposed to a very limited number of (OS/SYSDBA) users and that are also subject of infrequent changes.

The second group's controls feature categories like Privileges, Audits, User Profiles, Initialization Parameters, and General/Custom. The security configurations addressed by these controls are subject of a much wider base of DB users (DBAs, Developers, Application Owners, batch accounts,…), while also subject to frequent changes. Next, the first group's control scope and results are narrow and limited, while the opposite stands for the second's, and thus it creates a challenge on the process of technical assessment and management of assessed information.

Thus, controls of the first group can be approached periodically by manual assessment, mostly by OS/DB tools, but require not to be frequent. The controls of the second group are of the kind that Omega DB Security Reporter *does* perform, and the later should be use to assess them frequently.

The table below displays control types from different Oracle Security Checklists supported by Omega DB Security Reporter, categorized by latter's Report Classes.

Omega DB Security Reporter	CIS Controls	STIG-DISA Controls	SANS Controls
System Privileges	9 named privileges (1) 74 CREATE% privileges (2) 157 %ANY% privileges Granted to Roles only Admin grants	Granted to Roles only Admin grants PUBLIC grants	10 named privileges 157 %ANY% privileges Granted to Roles only Admin grants PUBLIC grants
Object Privileges	26 named Oracle objects All ALL_% public views All DBA_% views All X$% tables All V$% views Grantable grants PUBLIC grants	11 named Oracle objects Granted to Roles only Grantable grants PUBLIC grants	17 named Oracle objects All DBA_% views Granted to Roles only Grantable grants PUBLIC grants EXECUTE on all SYS packages
Role Privileges	2 named Oracle roles 3 %CATALOG% roles PUBLIC grants	1 named Oracle role Grantable grants PUBLIC grants	3 named Oracle roles 3 %CATALOG% roles PUBLIC grants
Statement Audits (3)	13 specific audit options 77 CREATE% statements 44 DROP% statements	29 Oracle (doc) advised. Unsuccessful login attempts All Failures	3 specific audit options 47 ALTER% statements 77 CREATE% statements 44 DROP% statements
Object Audits	All on SYS.AUD$ Insert Failures	All Failures	All on SYS.AUD$ Failures on critical objects
Password Resources	7 resources	4 resources	4 resources

1. named specifically and dedicated controls, ex.: CREATE USER for System Privileges, DBA for Roles, CREATE ROLE for System Privilege Audit, and so on for all Report Classes…

2. counted (for all %...% uses) on an Oracle 12c R2 environment
3. System Privileges and Statements/Shortcuts Report Classes

Notes:

1. Table above represents only explicit references to assessed items. Others supported exist in rest of controls on all checklists! For its Report Classes, Omega DB Security Reporter supports any security item available – ex. all system privileges.

2. The three checklists above, CIS, STIG-DISA and SANS contain respectively 302, 215 and 328 controls. However, these controls are indented for manual operation and evaluation of results. Some of them, and especially those supported by Omega DB Security Reporter, actually contain multiple controls when it comes to the real "security item" assessed, ex. a System/Object Privilege, or an Audit of the same, thus increasing greatly the real number of controls, to tens and hundred for even one of this application's Report Classes.

Common IT Security Frameworks and Standards

Table below displays examples of requirements from different IT Security Frameworks/Standards addressed by the Omega DB Security Reporter.

Framework/Standard	Topic
ISO 27001/2	Doc: ISO 27002 2013, Security Techniques/Code of Practice 9.2.3 Management of privileged access rights 9.4.3 Password management system 12.1.2 Change management 12.4.1 Event logging 12.4.2 Protection of log information 12.4.3 Administrator and operator logs 12.7.1 Information systems audit controls
ISACA (Cobit)	Doc: Oracle Database Security Checklist, Whitepaper, 2008 Enforce Password Management Manage Access to SYSDBA and SYSOPER Roles Enable Oracle Data Dictionary Protection Follow the Principle of Least Privilege Public Privileges
PCI-DSS	Doc: PCI DSS Quick Reference Guide, version 3, 2019 PCI DATA SECURITY Requirement 6. Develop and maintain secure systems and applications Requirement 7. Restrict access to cardholder data by business need-to-know Requirement 8. Identify and authenticate access to system components
HIPAA	Doc: The HIPAA Security Rule, 2003 Ensure the confidentiality, integrity, and availability of all electronic health information Detect and safeguard against anticipated threats to the security of the information Protect against anticipated impermissible uses or disclosures

Some of the Frameworks/Standards listed above have published their own Oracle Security checklists, like ISACA. Others either suggest usage of any of the Oracle Security Checklists in the previous topic, or remain limited to general guide-lining only.

6.5 Appendix A5 - Use Case

The following provides a simplified use case and demonstration of the solution's features and operations.

Prerequisites:

1. Setup Omega DB Security Reporter on a new clean environment.

2. Install a new test Oracle Database*, OS independent and with the most default settings, whenever presented by the setup routine. This will be used as the target database to report on.

3. Omega DB Security Reporter is set up for the target Oracle database and ready to report.

* Oracle 11g and above is supported

Use Case Steps

Initially: load an Oracle General template on the Overall Security Report form.

STEP 1: Run a new Overall Security Report on the Database.
Save the first report.

STEP 2: Create a new user account in the Database; grant the DBA role to it.
Run the second report and save it.
Compare the second report with the first one. *
Note the Declines related to the new DBA.

STEP 3: Lock the newly created user account in the Database.
Run the third report and save it.
Compare the third report with the second one.
Note the Improve related to the locked DBA.

* Comparison is a Professional-only feature, available only during the 30 day Trial period!

Conclusions:

The use case presented so far was a simplified simulation to demonstrate the skills and features Omega DB Security Reporter. Simplification is done for the sake of the easiness of the tester; however the later is encouraged to go further in testing and simulate real-live situations, as of course the use case above is just a start on the subject.

6.6 Appendix B - Support and Licensing

6.6.1 Support

Omega DB Security Reporter users of the free *Standard* edition are entitled to:

- new (Standard) versions
- upgrades and fixes
- new security controls
- online/offline documentations

Commercial annual support is available to the users of the *Professional* edition and also, cumulatively, features:

- discounts for new (Professional) versions
- online support

Professional edition 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-db-security-reporter

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
Peerlyst	https://www.peerlyst.com/companies/dataplus/dashboard

6.6.2 Licensing

Omega DB Security Reporter license is perpetual. It allows the customer to use the licensed software indefinitely and not being tied to the product version. Neither there is any vendor online service/website or OS/machine-specific dependence for its setup and use.

License Types:

User	installed on one computer, for use by a single individual
Enterprise	multiple individuals/computers within the organization
Consultant	external auditor (consultant) services

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

Copyright: