Netsurion™ | EventTracker

Integration Guide for Oracle Database

EventTracker v 9.x and above

Publication Date: September 13, 2019

Abstract

This guide provides instructions to configure/ retrieve **Oracle database** events using “**Unified Audit Trail**”. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports are configured to monitor the **Oracle database**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Oracle database v12c and above**.

Audience

Administrators who are assigned the task to monitor **Oracle database unified audit trail** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

1. Overview

Oracle Database Service is just one of the Oracle offerings that provide Oracle Database. Users can create databases on DB systems, which are either bare-metal servers or virtual machines with block volumes.

EventTracker, when integrated with the Oracle database, enables users to view critical information related to activities performed in the Oracle database. This information is represented in the form of report, alert and graphical/ pictorial representation(dashboard).

In this integration guide, logging of an audit trail in the Oracle database is set using “**Unified Audit Trail**”.

Unified auditing enables you to capture audit records from the following sources:

- Audit records (including SYS audit records) from unified audit policies and AUDIT settings
- Fine-grained audit records from the DBMS_FGA PL/SQL package
- Oracle Database Real Application Security audit records
- Oracle Recovery Manager audit records
- Oracle Database Vault audit records
- Oracle Label Security audit records
- Oracle Data Mining records
- Oracle Data Pump
- Oracle SQL*Loader Direct Load

2. Prerequisites

- EventTracker agents should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- Users should have administrative privileges on the host system/ server to run PowerShell.
- Read access to the unified audit trail (Login credentials).
- Oracle Wallet, which includes “**tnsnames.ora**” (includes connection string).

3. Integrating Oracle Database with EventTracker

3.1 Setting Unified Audit Trail

Oracle Database provides predefined unified audit policies that cover commonly used security-relevant audit settings. These policies are not enabled for databases that were upgraded from earlier versions, except if the user had created a new database from the previous release and then upgraded it to the current release.

However, for new databases, these policies are enabled by default for both pure unified auditing environments. Default audit policies:

1. ORA_LOGON_FAILURES
2. ORA_SECURECONFIG
3. ORA_DATABASE_PARAMETER
4. ORA_ACCOUNT_MGMT
5. ORA_CIS_RECOMMENDATIONS
6. ORA_RAS_POLICY_MGMT
7. ORA_RAS_SESSION_MGMT
8. ORA_DV_AUDPOL
9. ORA_DV_AUDPOL2

Before setting up a unified audit trail, create a user “**EventTracker**” and grant the “**AUDIT_VIEWER**” role to it.

1. Check if Unified auditing is enabled. If yes, unified auditing is enabled.

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';

PARAMETER          VALUE

----------------  ----------

Unified Auditing  TRUE
```

2. If unified auditing has not been enabled, then the output is `FALSE`. Perform the below steps to enable it:

2.1 Log in to your SQL database. E.g. using SQL*Plus:

```
sqlplus sys as sysdba

Enter password: password
```

2.2 Stop all Oracle processes: databases, listener and Enterprise Manager (if necessary)**:**

a. **Stopping Oracle database:**

```
SQL> shutdown immediate

SQL> exit
```

b. **Stopping listener service:**

```
$ lsnrctl stop
```

c. **Stopping Enterprise Manager (if necessary):**

```
$ cd /u01/app/oracle/product/middleware/oms

$ export OMS_HOME=/u01/app/oracle/product/middleware/oms

$ $OMS_HOME/bin/emctl stop oms
```

2.3 Relink the oracle binaries to turn pure Unified Auditing on:

```
$ cd $ORACLE_HOME/rdbms/lib

$ make -f ins_rdbms.mk uniaud_on ioracle
```

2.4 Restart all Oracle processes: Enterprise Manager, listener, databases**.**

```
$ lsnrctl start

$ sqlplus / as sysoper

SQL> startup
```

2.5 Verify:

```
SQL> select VALUE from V$OPTION where PARAMETER='Unified
Auditing';

VALUE
--------------------
TRUE
```

3. Enable a Unified Audit Policy:

The `AUDIT POLICY` statement can enable a unified audit policy. The following command format is used to enable desired predefined unified audit policy:

```
SQL> AUDIT POLICY { policy_auditing } [WHENEVER [NOT]
SUCCESSFUL]

OR

SQL> AUDIT POLICY { policy_auditing }
```

e.g.

```
SQL> AUDIT POLICY ORA_LOGON_FAILURES WHENEVER NOT SUCCESSFUL;
```

To find all existing policies, query the `AUDIT_UNIFIED_POLICIES` data dictionary view. To find currently enabled policies, query `AUDIT_UNIFIED_ENABLED_POLICIES`.

e.g.

```
SQL> select distinct POLICY_NAME from AUDIT_UNIFIED_POLICIES;

SQL> select distinct POLICY_NAME from AUDIT_UNIFIED_ENABLED_POLICIES;
```

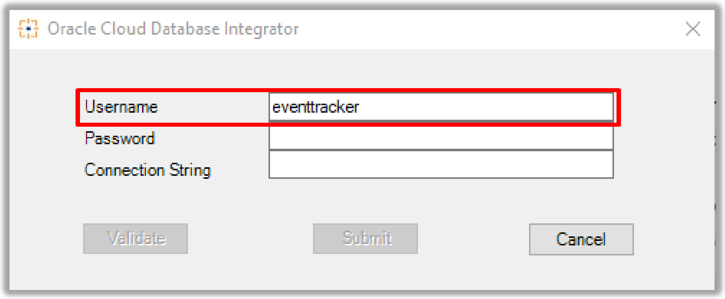
(**NOTE** – Please select the oracle audit policy as desired. The above-mentioned default policies are a point of reference.)

3.2 Forwarding Unified audit Logs to EventTracker

Once Unified auditing is enabled in Oracle database,

1. Request the EventTracker support team for the “**Oracle database Integrator”** executable file.
2. Once the executable application is received, right-click on the file and select “**Run as Administrator**”.
3. Running the Integrator, fill in the given fields.

   3.1 Enter the DB “**username**”:



Oracle Cloud Database Integrator

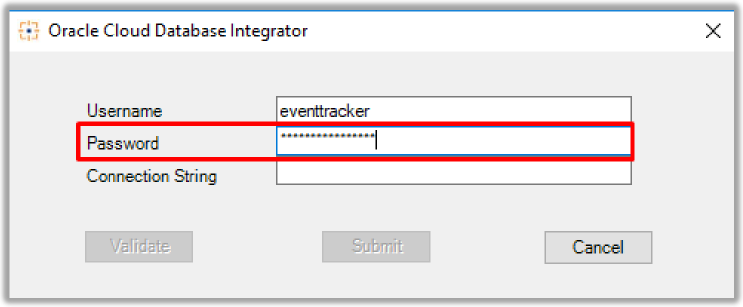
Username: eventtracker

Password:

Connection String:

Figure 1

   3.2 Enter the DB “**password**”:



Oracle Cloud Database Integrator

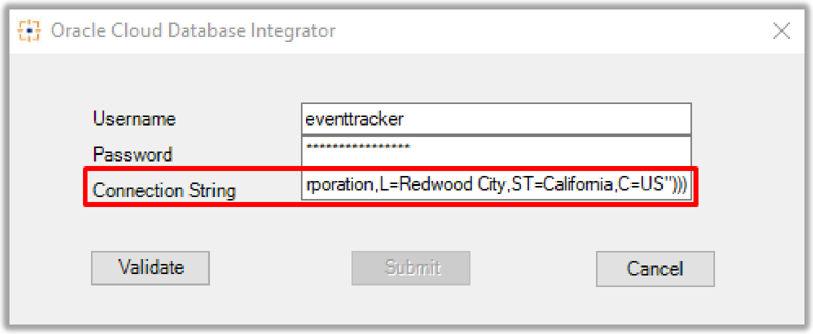
Username: eventtracker

Password: ****************

Connection String:

Figure 2

   3.3 Enter the “**connection string**” as mentioned in “**tnsnames.ora**” file:



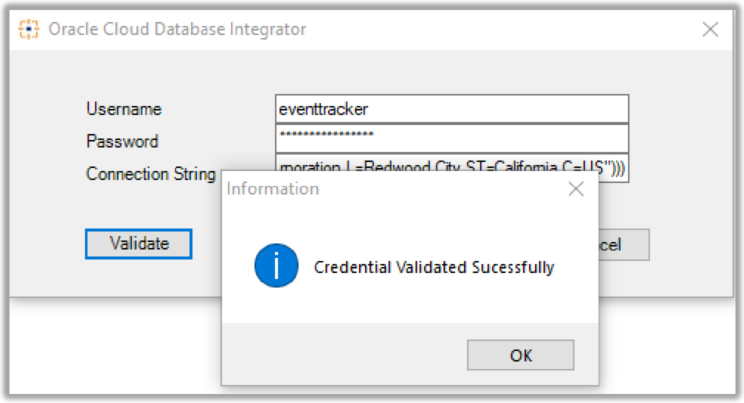
Username: eventtracker
Password: ****************
Connection String: rporation,L=Redwood City,ST=California,C=US")))

Figure 3

e.g.

```
(description=
(address=(protocol=tcps)(port=1522)(host=adb.eu-frankfurt-
1.oracle.com))(connect_data=(service_name=xxxxxxxxxxxxx5o_u
adw_low.adwc.oracle.com))(security=(ssl_server_cert_dn="CN=
adwc.eucom-central-1.oracle.com,OU=Oracle BMCS
FRANKFURT,O=Oracle Corporation,L=Redwood
City,ST=California,C=US")))
```

3.4 Now, click on the **“validate”** button to verify the credentials:

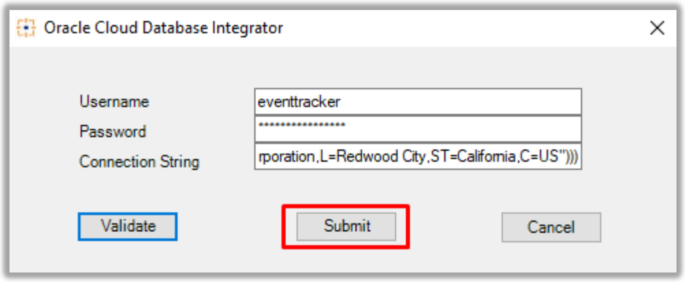


Username: eventtracker
Password: ****************
Connection String: rporation,L=Redwood City,ST=California,C=US")))

Credential Validated Sucessfully

Figure 4

3.5 Click on the **“Ok”** button and then click on the **“submit”** button to complete the integration process.



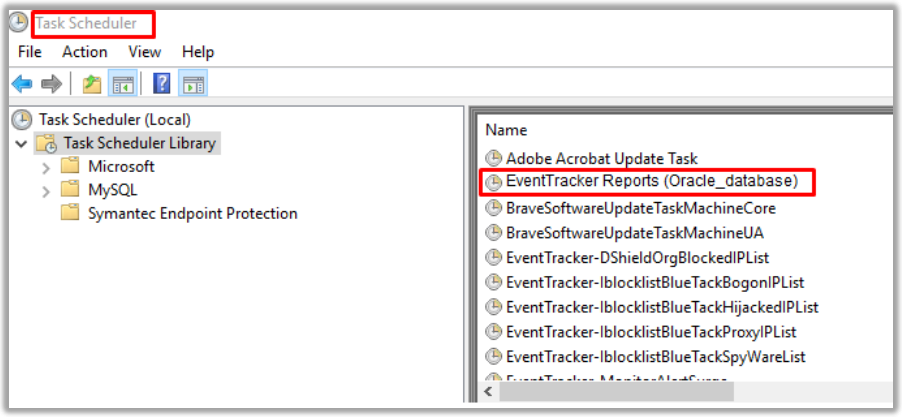
Username: eventtracker
Password: ****************
Connection String: rporation,L=Redwood City,ST=California,C=US")))

Figure 5

3.3 Verification of Oracle database Integration

If the Integration is successful, the action can be verified in two ways:

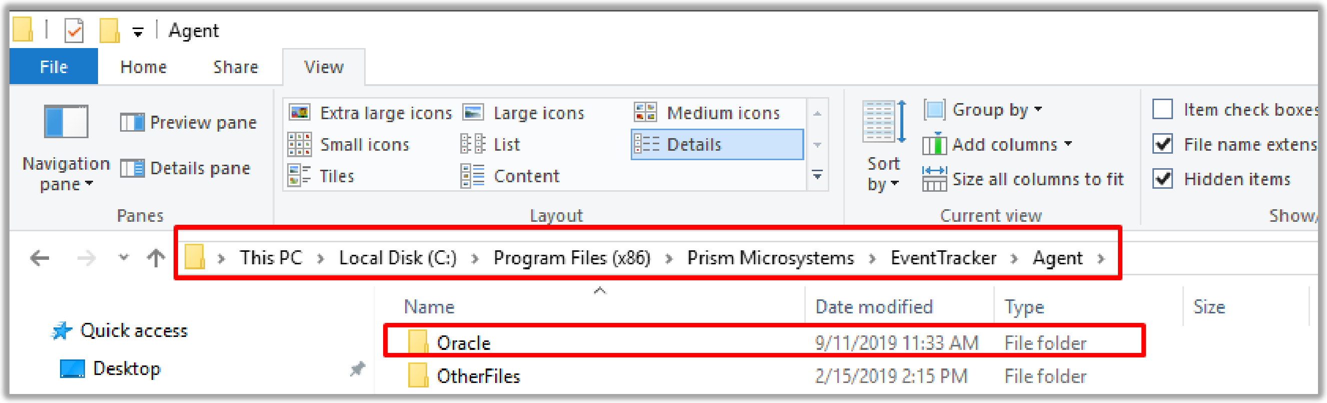
1. A scheduled task, named “**EventTracker Integrator (Oracle_database)**” is created in “**Task Scheduler**”.



- Adobe Acrobat Update Task
- EventTracker Reports (Oracle_database)
- BraveSoftwareUpdateTaskMachineCore
- BraveSoftwareUpdateTaskMachineUA
- EventTracker-DShieldOrgBlockedIPList
- EventTracker-IblocklistBlueTackBogonIPList
- EventTracker-IblocklistBlueTackHijackedIPList
- EventTracker-IblocklistBlueTackProxyIPList
- EventTracker-IblocklistBlueTackSpyWareList

Figure 6

2. A new folder is created in EventTracker agent folder [“C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent”], named “Oracle”.



This PC › Local Disk (C:) › Program Files (x86) › Prism Microsystems › EventTracker › Agent ›

Name	Date modified	Type	Size
Oracle	9/11/2019 11:33 AM	File folder	
OtherFiles	2/15/2019 2:15 PM	File folder	

Figure 7

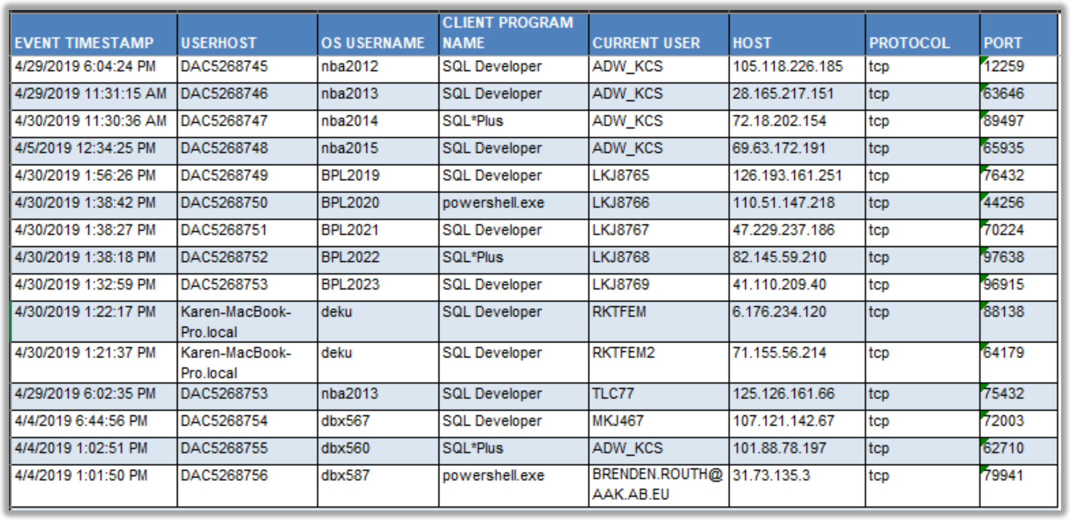
4. EventTracker Knowledge Pack

EventTracker knowledge pack for Oracle database includes:

1. Reports.
2. Alerts.
3. Saved searches.
4. Dashboards.
5. Behavior rules.

4.1 Reports

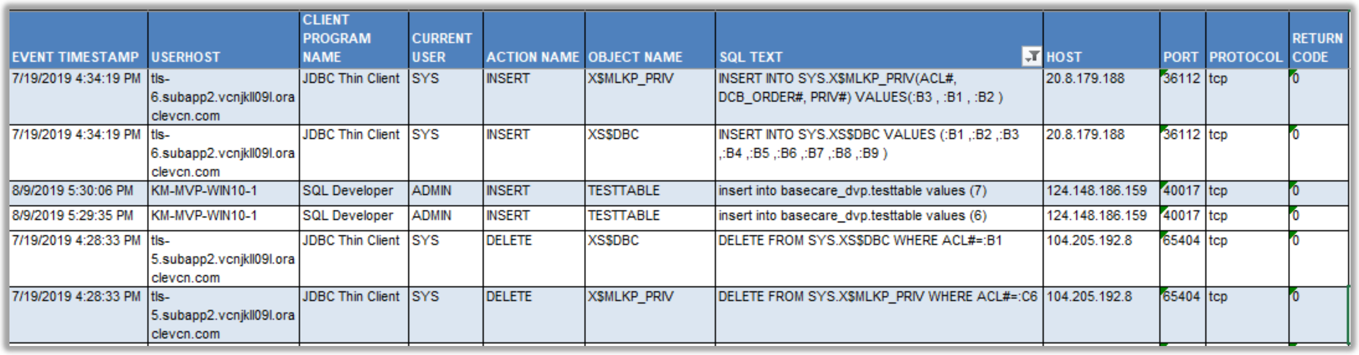
1. **Oracle DB user login success activities** - This report captures all the events related to successful oracle database login. The report includes the login time, username, tool/ software used for login, source Ip address, etc.



EVENT TIMESTAMP	USERHOST	OS USERNAME	CLIENT PROGRAM NAME	CURRENT USER	HOST	PROTOCOL	PORT
4/29/2019 6:04:24 PM	DAC5268745	nba2012	SQL Developer	ADW_KCS	105.118.226.185	tcp	12259
4/29/2019 11:31:15 AM	DAC5268746	nba2013	SQL Developer	ADW_KCS	28.165.217.151	tcp	63646
4/30/2019 11:30:36 AM	DAC5268747	nba2014	SQL*Plus	ADW_KCS	72.18.202.154	tcp	89497
4/5/2019 12:34:25 PM	DAC5268748	nba2015	SQL Developer	ADW_KCS	69.63.172.191	tcp	65935
4/30/2019 1:56:26 PM	DAC5268749	BPL2019	SQL Developer	LKJ8765	126.193.161.251	tcp	76432
4/30/2019 1:38:42 PM	DAC5268750	BPL2020	powershell.exe	LKJ8766	110.51.147.218	tcp	44256
4/30/2019 1:38:27 PM	DAC5268751	BPL2021	SQL Developer	LKJ8767	47.229.237.186	tcp	70224
4/30/2019 1:38:18 PM	DAC5268752	BPL2022	SQL*Plus	LKJ8768	82.145.59.210	tcp	97638
4/30/2019 1:32:59 PM	DAC5268753	BPL2023	SQL Developer	LKJ8769	41.110.209.40	tcp	96915
4/30/2019 1:22:17 PM	Karen-MacBook-Pro.local	deku	SQL Developer	RKTFEM	6.176.234.120	tcp	88138
4/30/2019 1:21:37 PM	Karen-MacBook-Pro.local	deku	SQL Developer	RKTFEM2	71.155.56.214	tcp	64179
4/29/2019 6:02:35 PM	DAC5268753	nba2013	SQL Developer	TLC77	125.126.161.66	tcp	75432
4/4/2019 6:44:56 PM	DAC5268754	dbx567	SQL Developer	MKJ467	107.121.142.67	tcp	72003
4/4/2019 1:02:51 PM	DAC5268755	dbx560	SQL*Plus	ADW_KCS	101.88.78.197	tcp	62710
4/4/2019 1:01:50 PM	DAC5268756	dbx587	powershell.exe	BRENDEN.ROUTH@AAK.AB.EU	31.73.135.3	tcp	79941

Figure 8

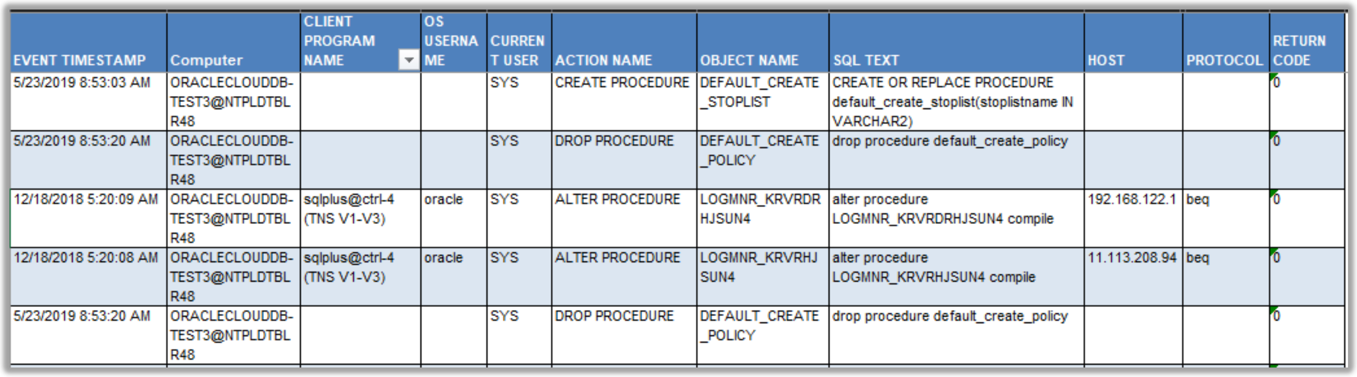
2. **Oracle DB data access activities** - Data access events track audited Data Manipulation Language (DML) activities, for example, all SELECT, INSERT, UPDATE, or DROP SQL statements. This report includes the event timestamp, client program name, object name on which action was performed, etc.



EVENT TIMESTAMP	USERHOST	CLIENT PROGRAM NAME	CURRENT USER	ACTION NAME	OBJECT NAME	SQL TEXT	HOST	PORT	PROTOCOL	RETURN CODE
7/19/2019 4:34:19 PM	tls-6.subapp2.vcnjkll09l.oraclevcn.com	JDBC Thin Client	SYS	INSERT	X$MLKP_PRIV	INSERT INTO SYS.X$MLKP_PRIV(ACL#, DCB_ORDER#, PRIV#) VALUES(:B3 , :B1 , :B2)	20.8.179.188	36112	tcp	0
7/19/2019 4:34:19 PM	tls-6.subapp2.vcnjkll09l.oraclevcn.com	JDBC Thin Client	SYS	INSERT	XS$DBC	INSERT INTO SYS.XS$DBC VALUES (:B1 ,:B2 ,:B3 ,:B4 ,:B5 ,:B6 ,:B7 ,:B8 ,:B9)	20.8.179.188	36112	tcp	0
8/9/2019 5:30:06 PM	KM-MVP-WIN10-1	SQL Developer	ADMIN	INSERT	TESTTABLE	insert into basecare_dvp.testtable values (7)	124.148.186.159	40017	tcp	0
8/9/2019 5:29:35 PM	KM-MVP-WIN10-1	SQL Developer	ADMIN	INSERT	TESTTABLE	insert into basecare_dvp.testtable values (6)	124.148.186.159	40017	tcp	0
7/19/2019 4:28:33 PM	tls-5.subapp2.vcnjkll09l.oraclevcn.com	JDBC Thin Client	SYS	DELETE	XS$DBC	DELETE FROM SYS.XS$DBC WHERE ACL#=:B1	104.205.192.8	65404	tcp	0
7/19/2019 4:28:33 PM	tls-5.subapp2.vcnjkll09l.oraclevcn.com	JDBC Thin Client	SYS	DELETE	X$MLKP_PRIV	DELETE FROM SYS.X$MLKP_PRIV WHERE ACL#=:C6	104.205.192.8	65404	tcp	0

Figure 9

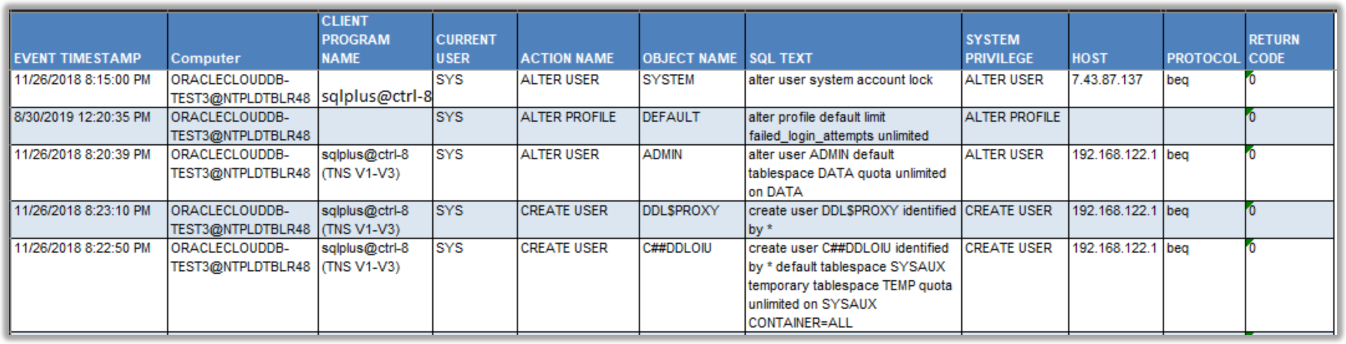
3. **Oracle database procedure management activities –** Procedure management events include activities related to Oracle database 'Procedures'. The action types are ALTER PROCEDURE, CREATE PROCEDURE and DROP PROCEDURE. This report includes event timestamp, action name, Object name on which action was performed, SQL text entered, etc.



EVENT TIMESTAMP	Computer	CLIENT PROGRAM NAME	OS USERNAME	CURRENT USER	ACTION NAME	OBJECT NAME	SQL TEXT	HOST	PROTOCOL	RETURN CODE
5/23/2019 8:53:03 AM	ORACLECLOUDDB-TEST3@NTPLDTBLR48			SYS	CREATE PROCEDURE	DEFAULT_CREATE_STOPLIST	CREATE OR REPLACE PROCEDURE default_create_stoplist(stoplistname IN VARCHAR2)			0
5/23/2019 8:53:20 AM	ORACLECLOUDDB-TEST3@NTPLDTBLR48			SYS	DROP PROCEDURE	DEFAULT_CREATE_POLICY	drop procedure default_create_policy			0
12/18/2018 5:20:09 AM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	sqlplus@ctrl-4 (TNS V1-V3)	oracle	SYS	ALTER PROCEDURE	LOGMNR_KRVRDRHJSUN4	alter procedure LOGMNR_KRVRDRHJSUN4 compile	192.168.122.1	beq	0
12/18/2018 5:20:08 AM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	sqlplus@ctrl-4 (TNS V1-V3)	oracle	SYS	ALTER PROCEDURE	LOGMNR_KRVRHJSUN4	alter procedure LOGMNR_KRVRHJSUN4 compile	11.113.208.94	beq	0
5/23/2019 8:53:20 AM	ORACLECLOUDDB-TEST3@NTPLDTBLR48			SYS	DROP PROCEDURE	DEFAULT_CREATE_POLICY	drop procedure default_create_policy			0

Figure 10

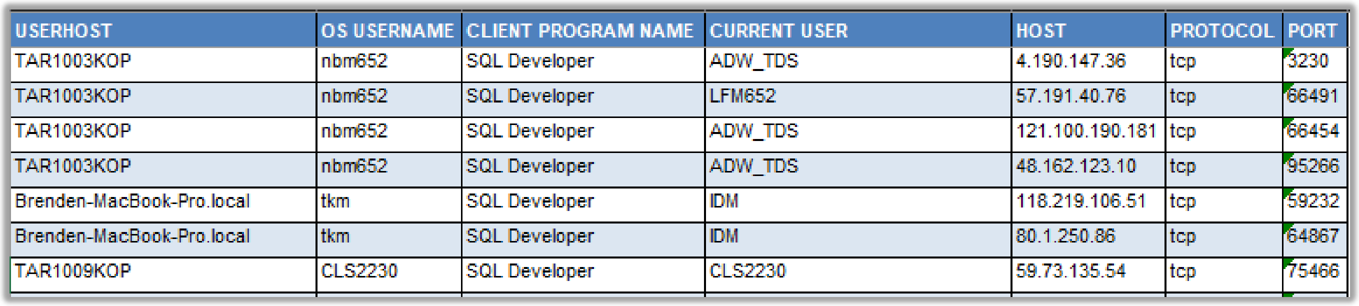
4. **Oracle database user account management activities** – User account management includes Oracle database user account creation, deletion, modification, etc. This report includes event timestamp, Client program name, an action performed, SQL text entered, etc.



EVENT TIMESTAMP	Computer	CLIENT PROGRAM NAME	CURRENT USER	ACTION NAME	OBJECT NAME	SQL TEXT	SYSTEM PRIVILEGE	HOST	PROTOCOL	RETURN CODE
11/26/2018 8:15:00 PM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	sqlplus@ctrl-8	SYS	ALTER USER	SYSTEM	alter user system account lock	ALTER USER	7.43.87.137	beq	0
8/30/2019 12:20:35 PM	ORACLECLOUDDB-TEST3@NTPLDTBLR48		SYS	ALTER PROFILE	DEFAULT	alter profile default limit failed_login_attempts unlimited	ALTER PROFILE			0
11/26/2018 8:20:39 PM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	sqlplus@ctrl-8 (TNS V1-V3)	SYS	ALTER USER	ADMIN	alter user ADMIN default tablespace DATA quota unlimited on DATA	ALTER USER	192.168.122.1	beq	0
11/26/2018 8:23:10 PM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	sqlplus@ctrl-8 (TNS V1-V3)	SYS	CREATE USER	DDL$PROXY	create user DDL$PROXY identified by *	CREATE USER	192.168.122.1	beq	0
11/26/2018 8:22:50 PM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	sqlplus@ctrl-8 (TNS V1-V3)	SYS	CREATE USER	C##DDLOIU	create user C##DDLOIU identified by * default tablespace SYSAUX temporary tablespace TEMP quota unlimited on SYSAUX CONTAINER=ALL	CREATE USER	192.168.122.1	beq	0

Figure 11

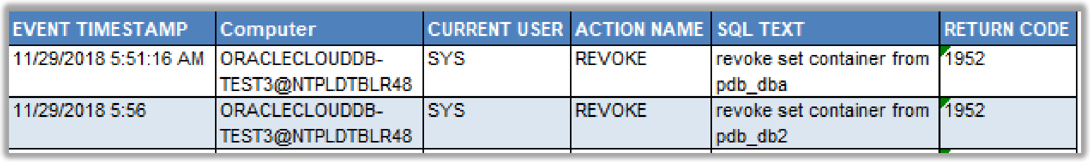
5. **Oracle DB user login failed activities –** This report captures all the failed oracle database login attempts. It includes event timestamp, client login name, client program name, client IP address, etc.



USERHOST	OS USERNAME	CLIENT PROGRAM NAME	CURRENT USER	HOST	PROTOCOL	PORT
TAR1003KOP	nbm652	SQL Developer	ADW_TDS	4.190.147.36	tcp	3230
TAR1003KOP	nbm652	SQL Developer	LFM652	57.191.40.76	tcp	66491
TAR1003KOP	nbm652	SQL Developer	ADW_TDS	121.100.190.181	tcp	66454
TAR1003KOP	nbm652	SQL Developer	ADW_TDS	48.162.123.10	tcp	95266
Brenden-MacBook-Pro.local	tkm	SQL Developer	IDM	118.219.106.51	tcp	59232
Brenden-MacBook-Pro.local	tkm	SQL Developer	IDM	80.1.250.86	tcp	64867
TAR1009KOP	CLS2230	SQL Developer	CLS2230	59.73.135.54	tcp	75466

Figure 12

6. **Oracle database syntax error and access rule violation detection –** This report includes invalid SQL syntax or SQL access rule violation related events. The report includes event timestamp, User name, SQL error code, SQL text, etc.



EVENT TIMESTAMP	Computer	CURRENT USER	ACTION NAME	SQL TEXT	RETURN CODE
11/29/2018 5:51:16 AM	ORACLECLOUDDB-TEST3@NTPLDTBLR48	SYS	REVOKE	revoke set container from pdb_dba	1952
11/29/2018 5:56	ORACLECLOUDDB-TEST3@NTPLDTBLR48	SYS	REVOKE	revoke set container from pdb_db2	1952

Figure 13

4.2 Alerts

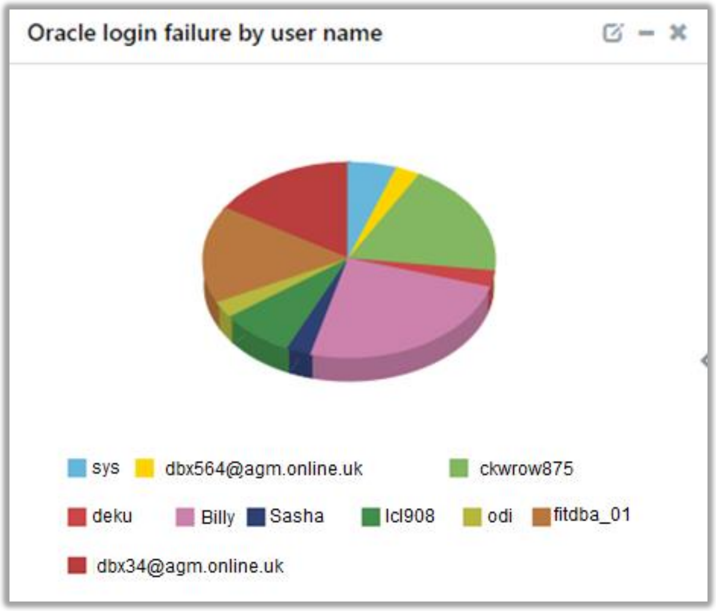
- **Oracle database failed logon has been detected**.
- **Oracle database syntax error and access rule violation have been detected**.
- **Oracle Database user login from a new IP address has been detected**.
- **Oracle Database user login from a new system has been detected**.

4.3 Saved searches

- **Oracle login failures**.
- **Oracle login success**.
- **Oracle database SQL syntax error and access rule violation**.
- **Oracle database user account management**.
- **Oracle database data access management**.

4.4 Dashboards

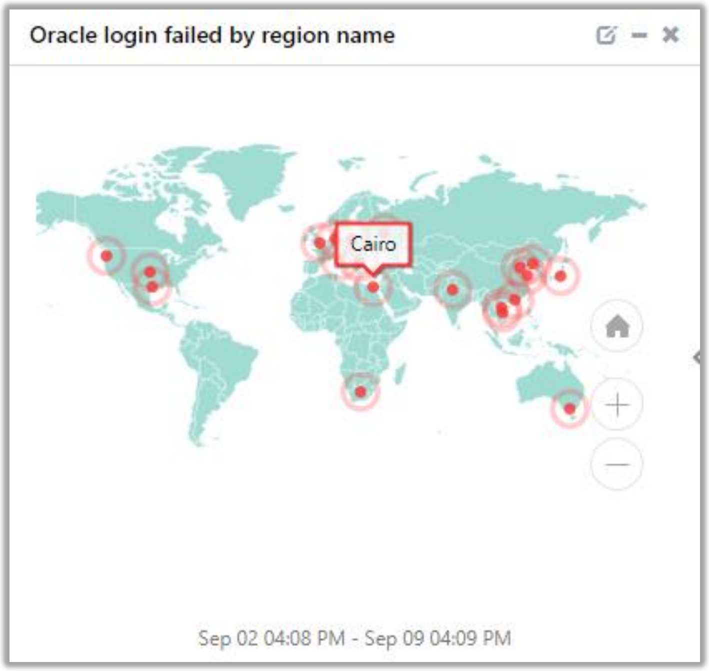
- **Oracle login failure by user name**



Oracle login failure by user name

Figure 14

- **Oracle login failed by region name**



Oracle login failed by region name

Sep 02 04:08 PM - Sep 09 04:09 PM

Figure 15

- **Oracle login activity by Process**

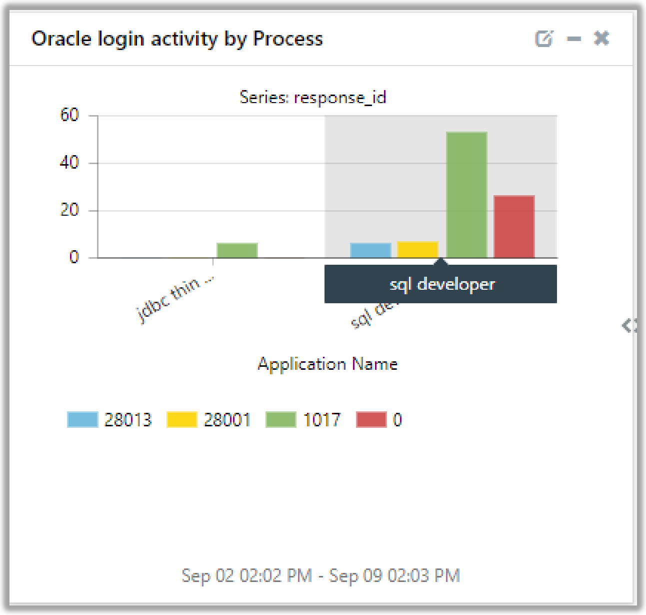


Figure 16

- **Top 10 Oracle database actions**

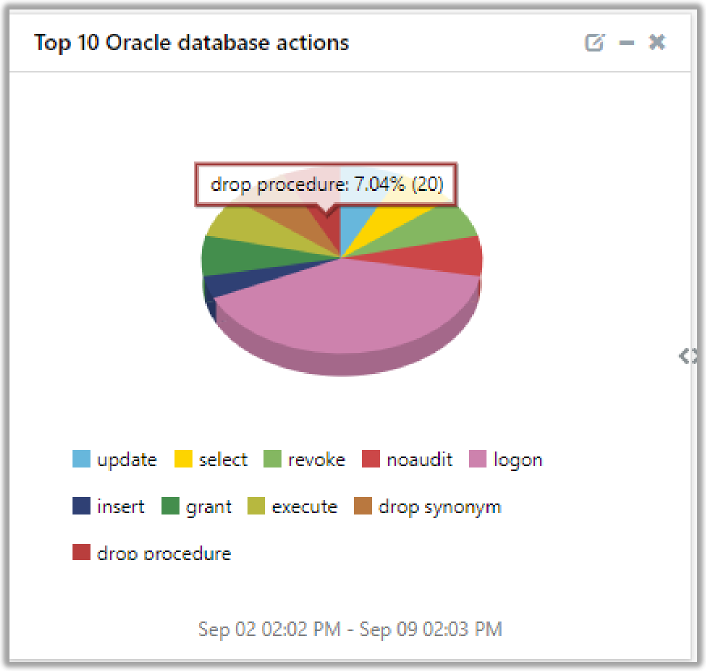

Top 10 Oracle database actions
drop procedure: 7.04% (20)
update
select
revoke
noaudit
logon
insert
grant
execute
drop synonym
drop procedure
Sep 02 02:02 PM - Sep 09 02:03 PM

Figure 17

- **Oracle database actions by user**

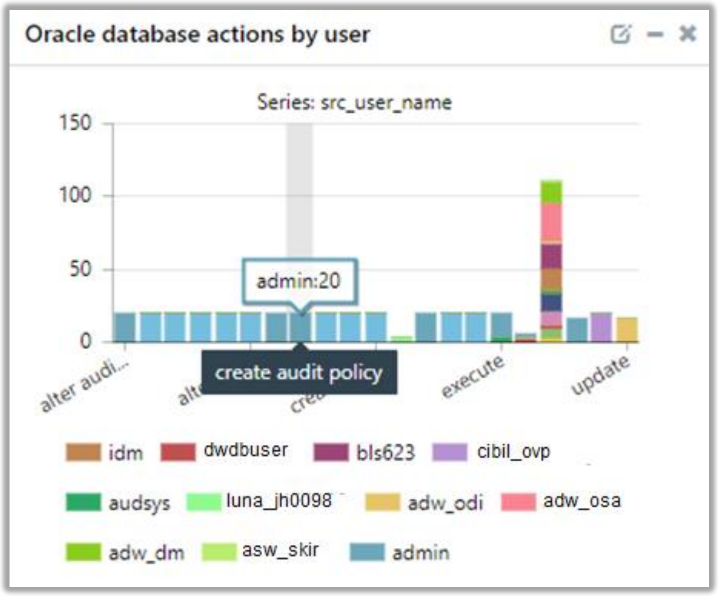


Figure 18

- **Oracle database new users created**

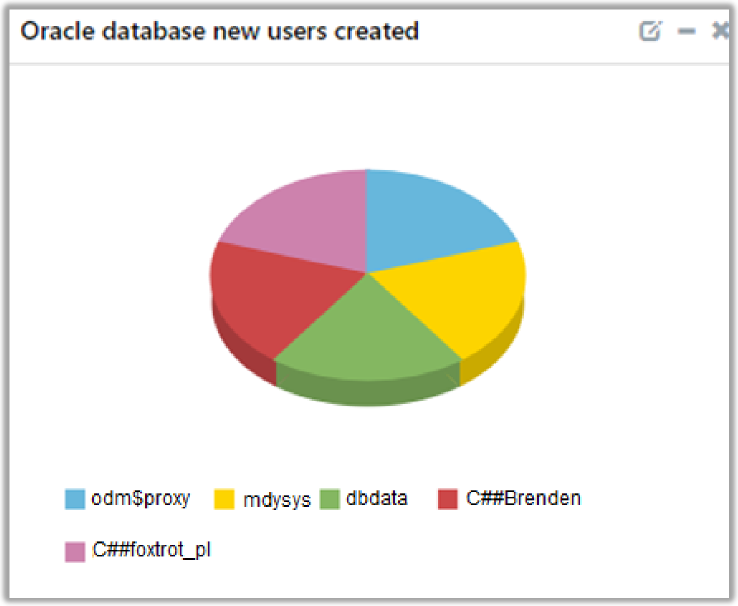


Figure 19

- **Oracle database action by permission granted**

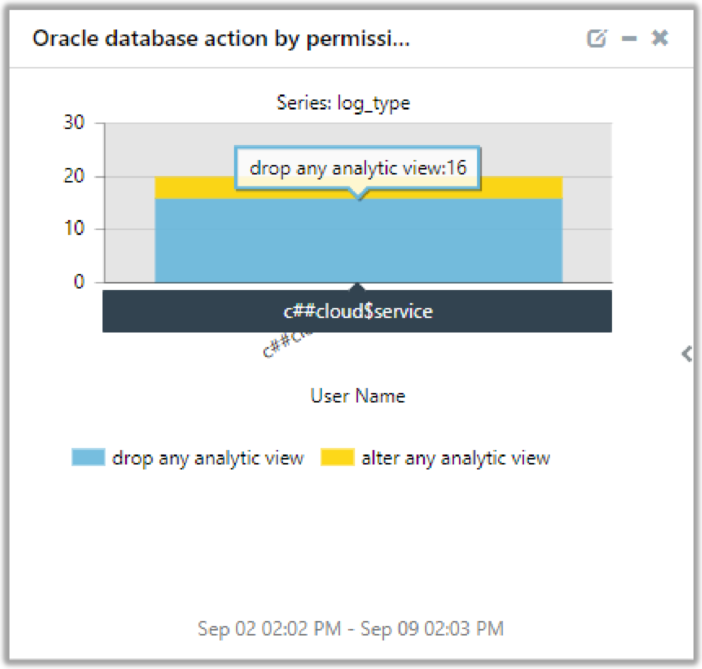


Figure 20

- **Oracle database changes by user**

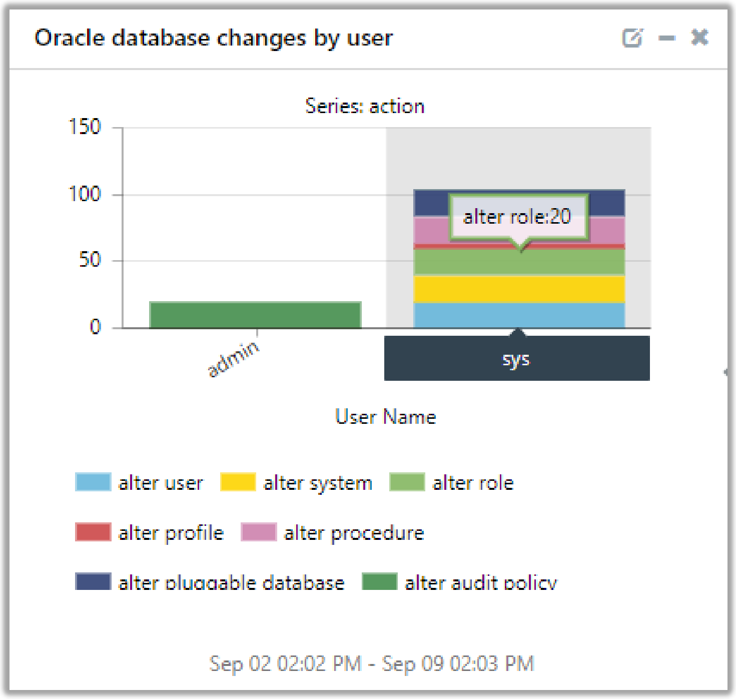


Figure 21

- **Oracle database changes in audit policy by user**

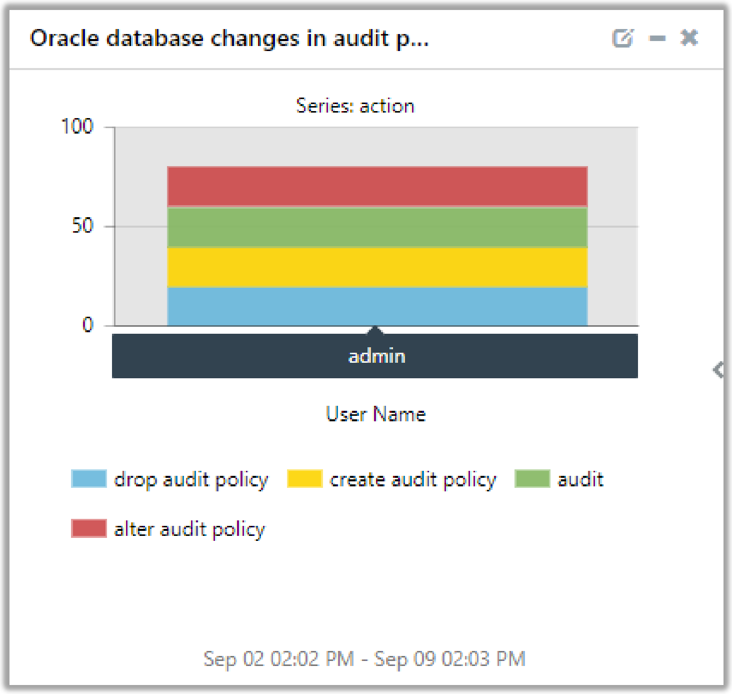


Figure 22

- **Oracle database changes in audit policy**

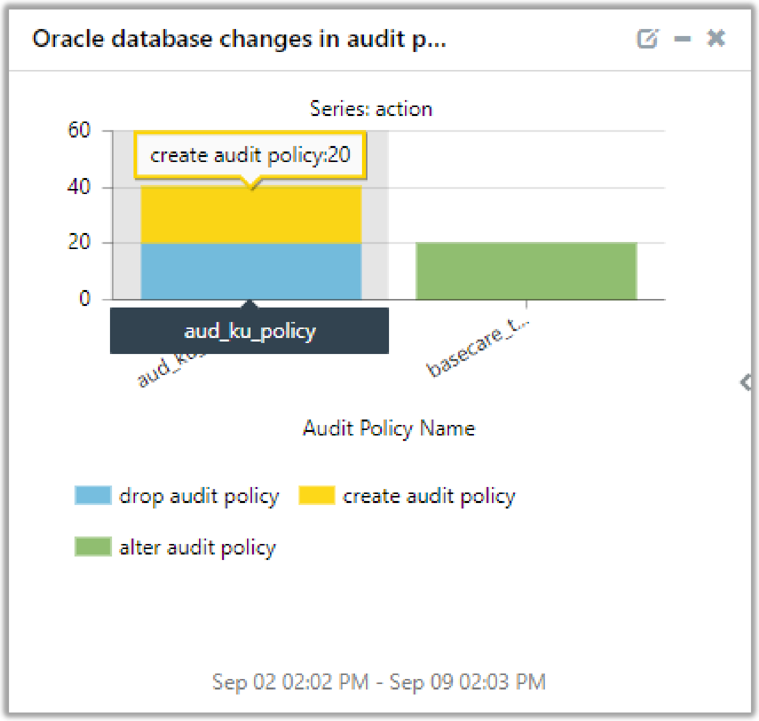


Figure 23

- **Oracle login success by user name**

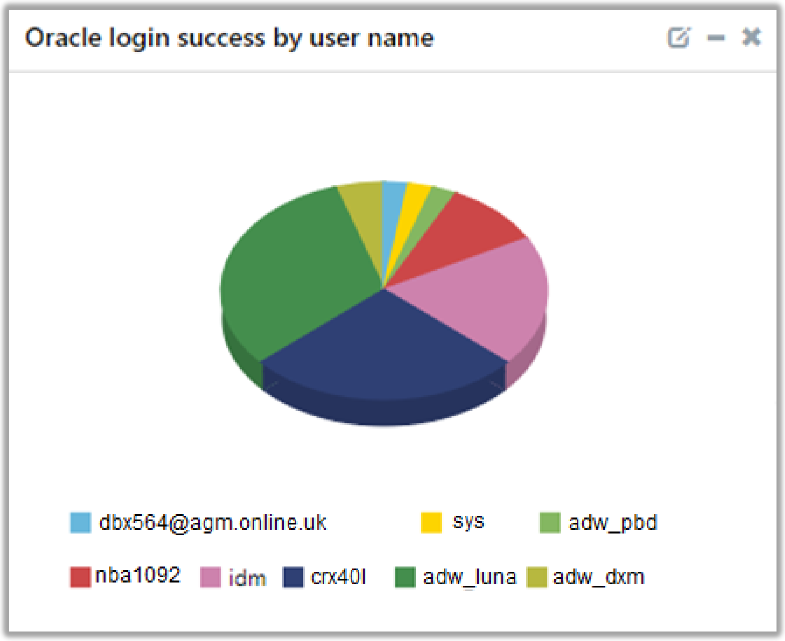


Figure 24

- **Oracle login success by region name**

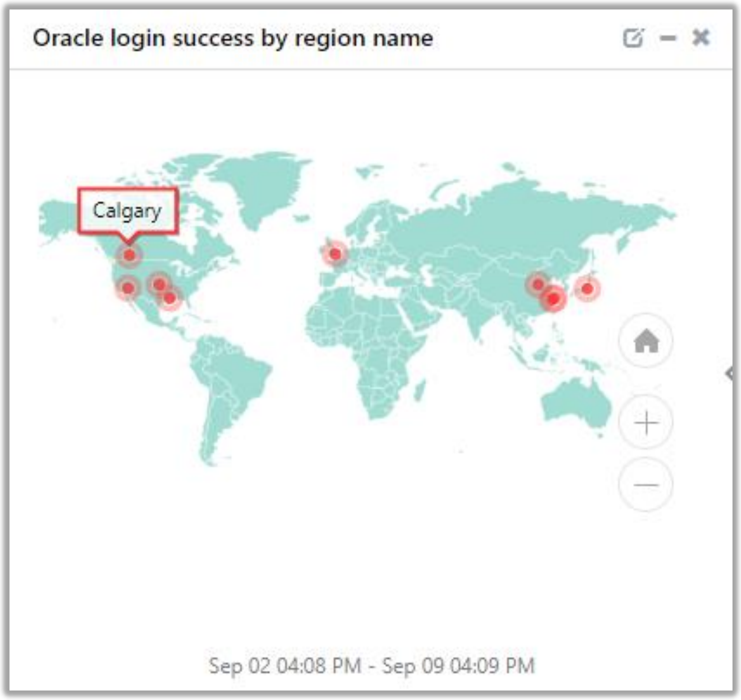

Oracle login success by region name
Calgary
Sep 02 04:08 PM - Sep 09 04:09 PM

Figure 25

4.5 Behavior rules

- **Oracle Database User login from new IP address**.
- **Oracle Database User login from new system**.

5. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.

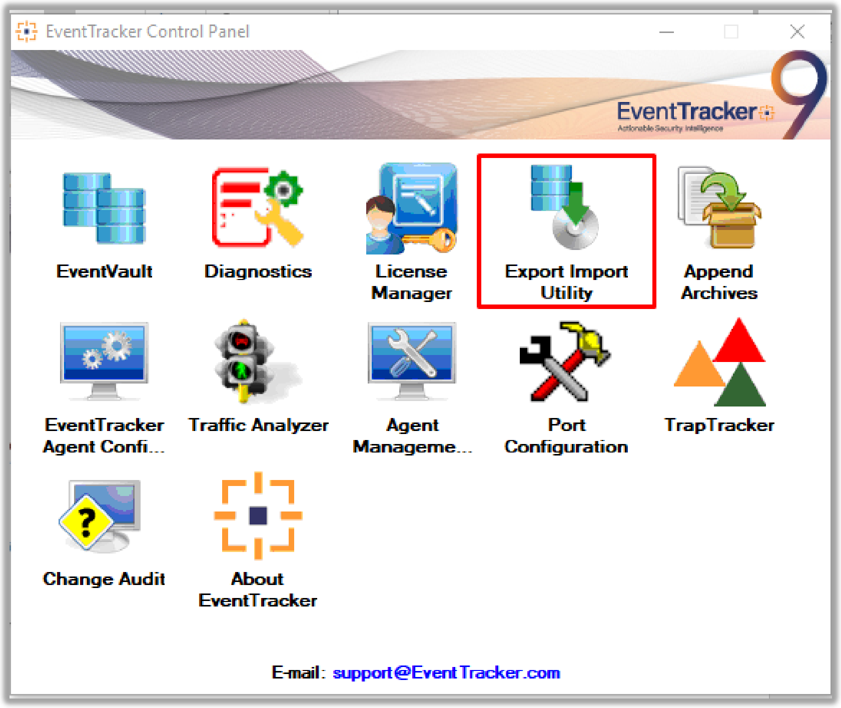
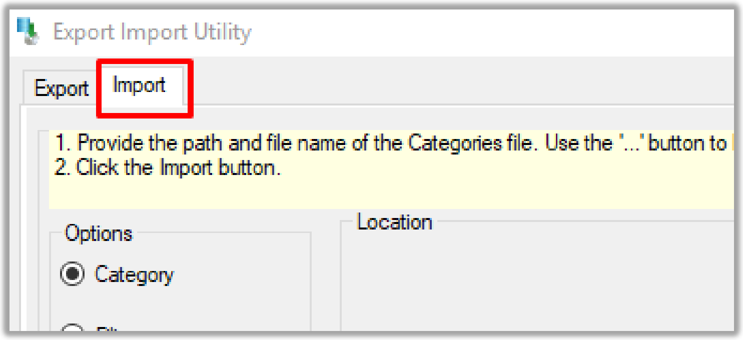


Figure 26



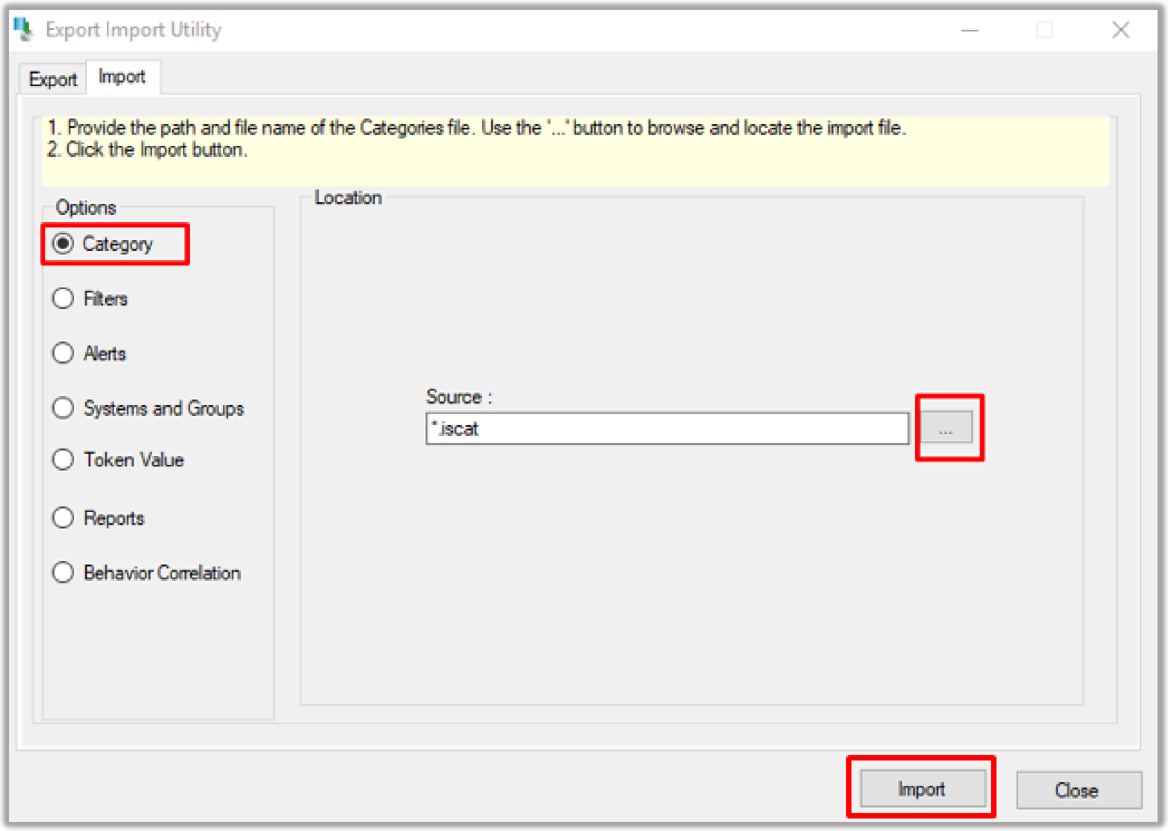
1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

Figure 27

3. Click the **Import** tab.

5.1 Categories

1. Once you have opened "**Export-Import Utility**" via "**EventTracker Control Panel**", click the **Category** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension **".iscat", e.g. "Categories_Oracle database.iscat"** and then click on the "**Import**" button:

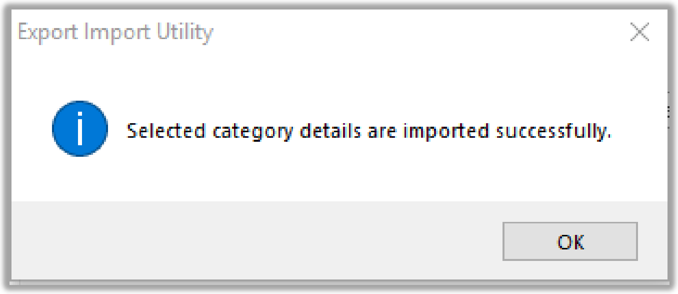


1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Source : *.iscat

Figure 28

EventTracker displays a success message:



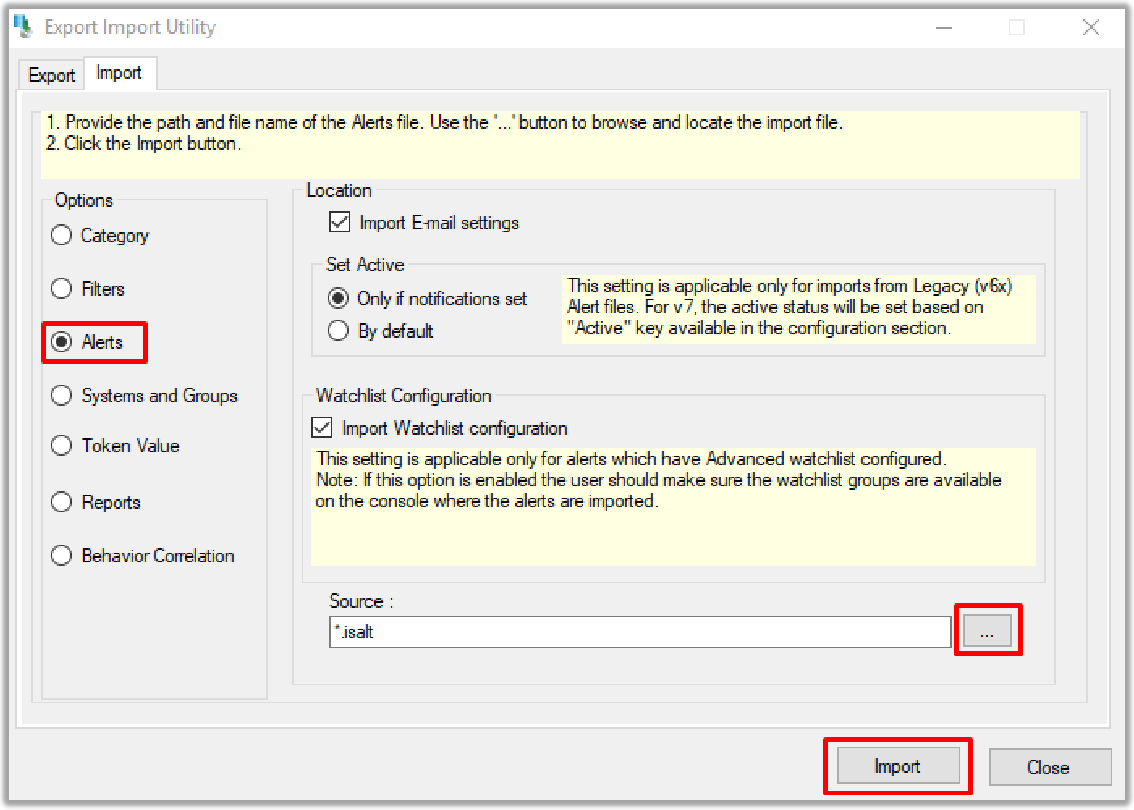
Export Import Utility

Selected category details are imported successfully.

Figure 29

5.2 Alerts

1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click **Alert** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension **“.isalt**”, **e.g**. “**Alerts_Oracle database.isalt**” and then click on the “**Import**” button:



Export Import Utility

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration

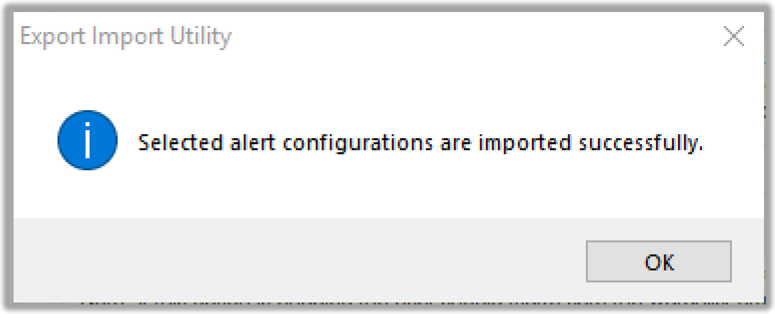
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt

Figure 30

EventTracker displays a success message:



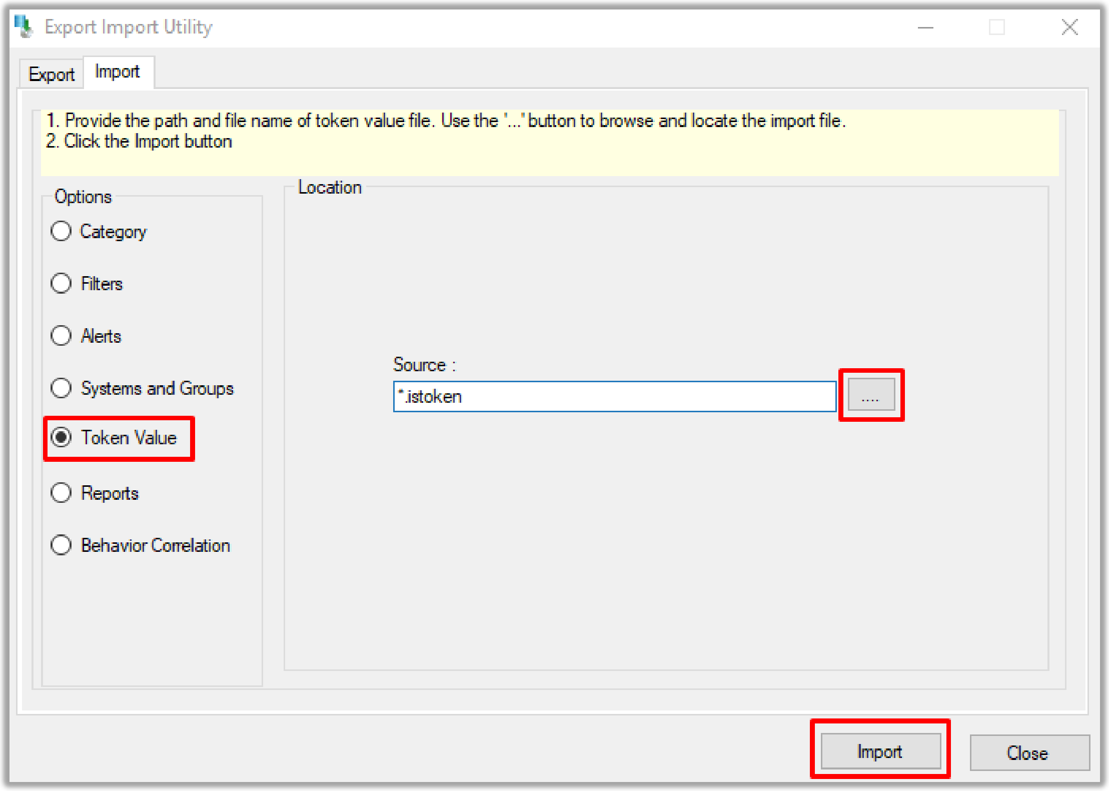
Export Import Utility

Selected alert configurations are imported successfully.

Figure 31

5.3 Parsing Rules

1. Once you have opened "**Export-Import Utility**" via "**EventTracker Control Panel**", click the **"Token Value"** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension **".istoken", e.g. "Parsing Rules_Oracle database.istoken"** and then click on the "**Import**" button:



Export Import Utility

1. Provide the path and file name of token value file. Use the '...' button to browse and locate the import file.
2. Click the Import button

Options

○ Category

○ Filters

○ Alerts

○ Systems and Groups

● Token Value

○ Reports

○ Behavior Correlation

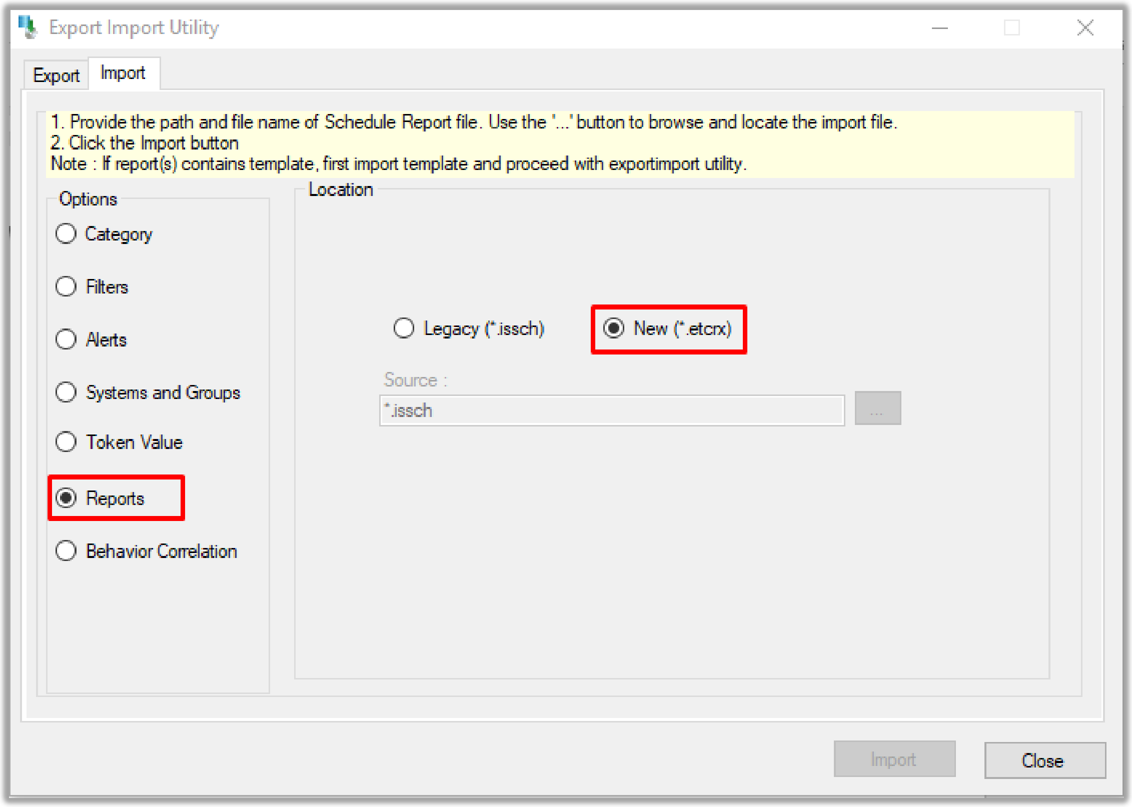
Location

Source : *.istoken

Figure 32

5.4 Flex Reports

1. In the EventTracker control panel, select "**Export/ Import utility**" and select the "**Import tab**". Then, click **Reports** option, and choose "**New (*.etcrx)**":



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

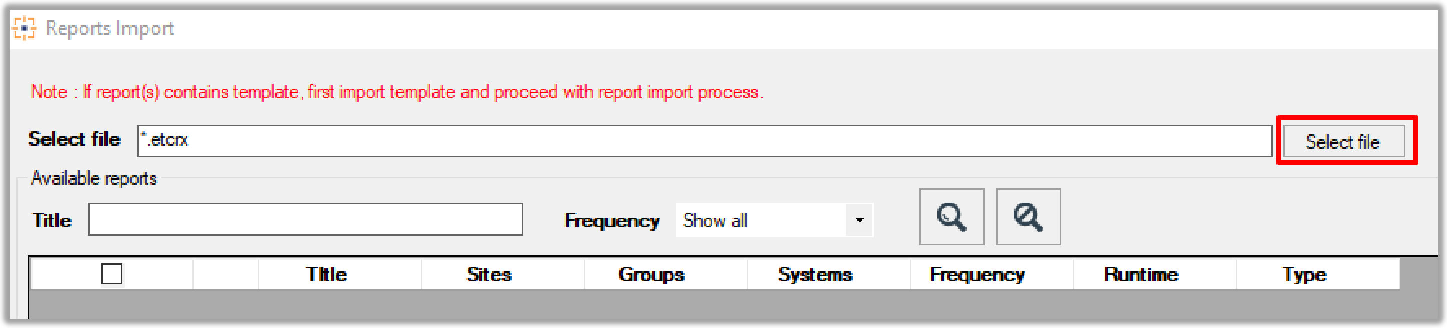
Options: ○ Category ○ Filters ○ Alerts ○ Systems and Groups ○ Token Value ● Reports ○ Behavior Correlation

Location: ○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 33

2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click the "**Select File**" button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g. "Reports_Oracle database.etcrx".**



Note : If report(s) contains template, first import template and proceed with report import process.

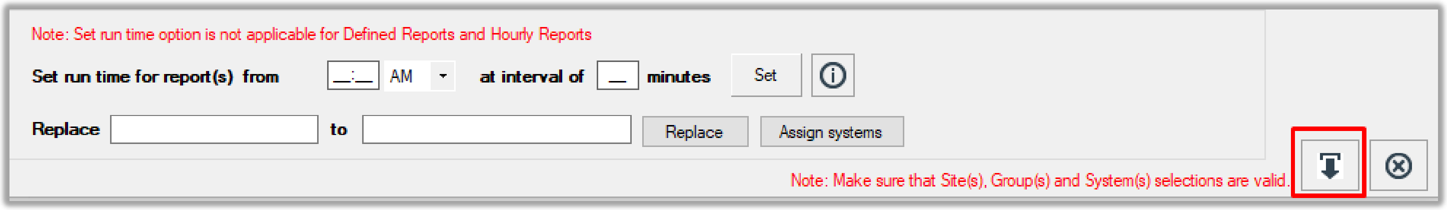
Select file: *.etcrx

Frequency: Show all

□		Title	Sites	Groups	Systems	Frequency	Runtime	Type

Figure 34

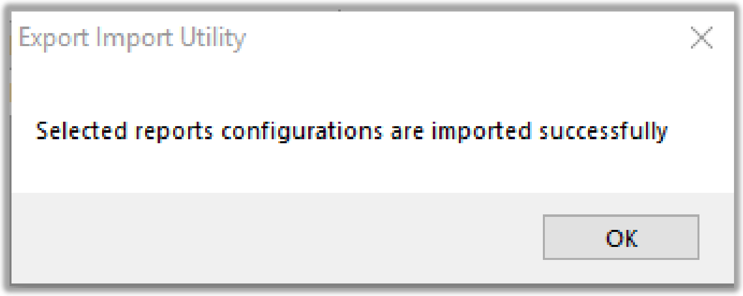
3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the **Import** button.


Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 35

EventTracker displays a success message:


Export Import Utility

Selected reports configurations are imported successfully

Figure 36

5.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager web interface.

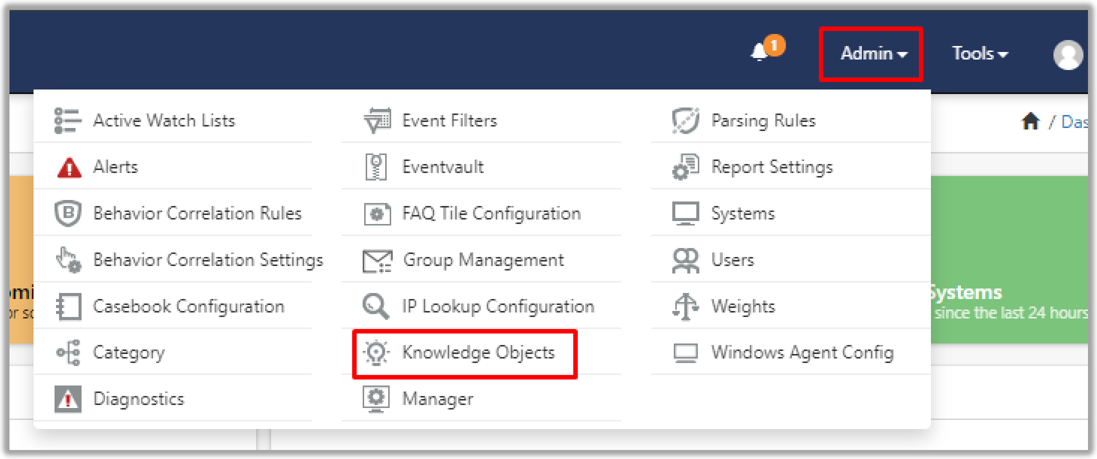


Figure 37

2. Next, click the **“import object”** icon:

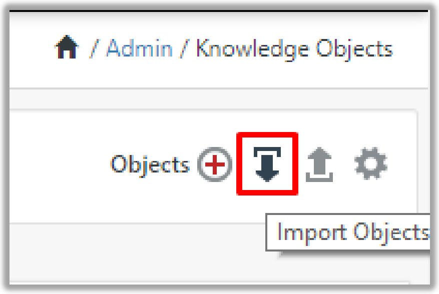


Figure 38

3. A pop-up box will appear, click "**Browse**" in that and navigate to knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g. "KO_Oracle database .etko"** and then click "**Upload**" button.

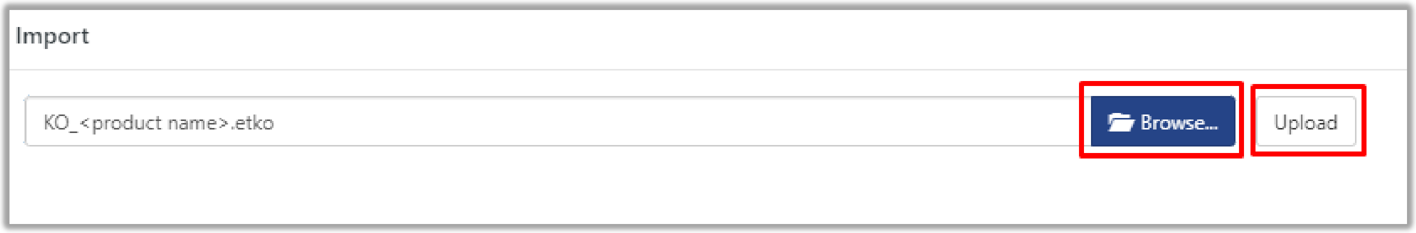


Figure 39

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the "**Import**" button:

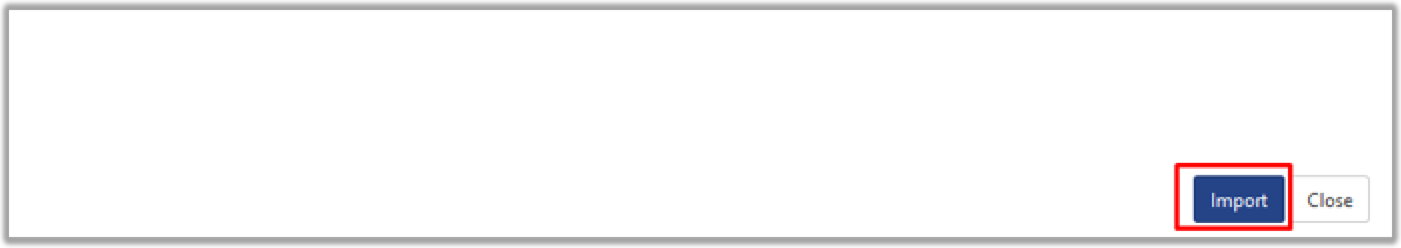


Figure 40

5.6 Dashboards

1. Login to the **EventTracker manager web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", Click **Import Button**:

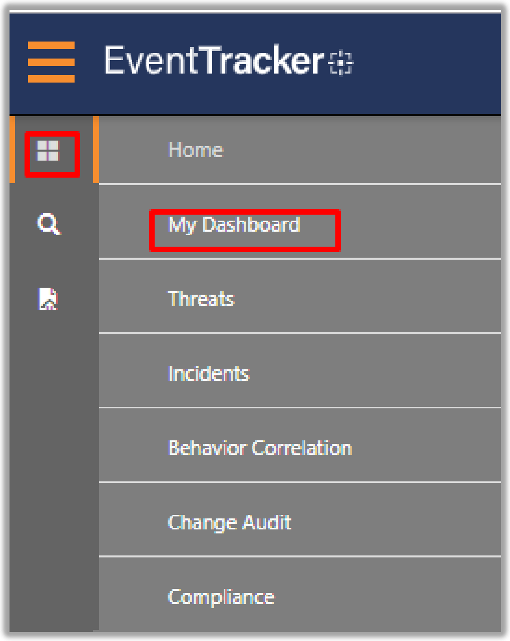


Figure 41

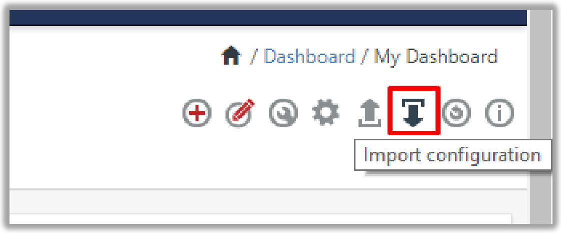
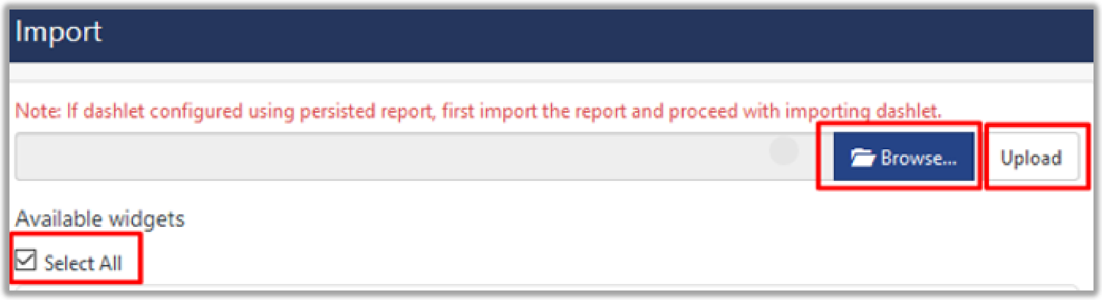


Figure 42

4. Select the **browse** button and navigate to the knowledge pack folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) where "**.etwd**", **e.g.** "**Dashboard_AWS.etwd**" is saved and click on "**Upload**" button.

5. Wait while EventTracker populates all the available dashboards. Now, choose "**Select All**" and click on **"Import"** Button.


Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Figure 43

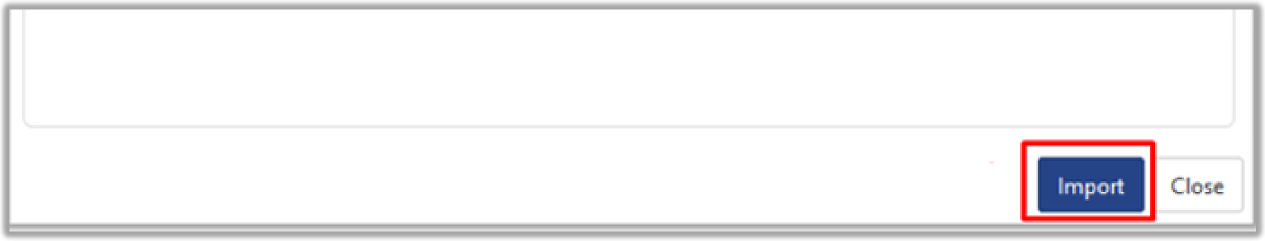
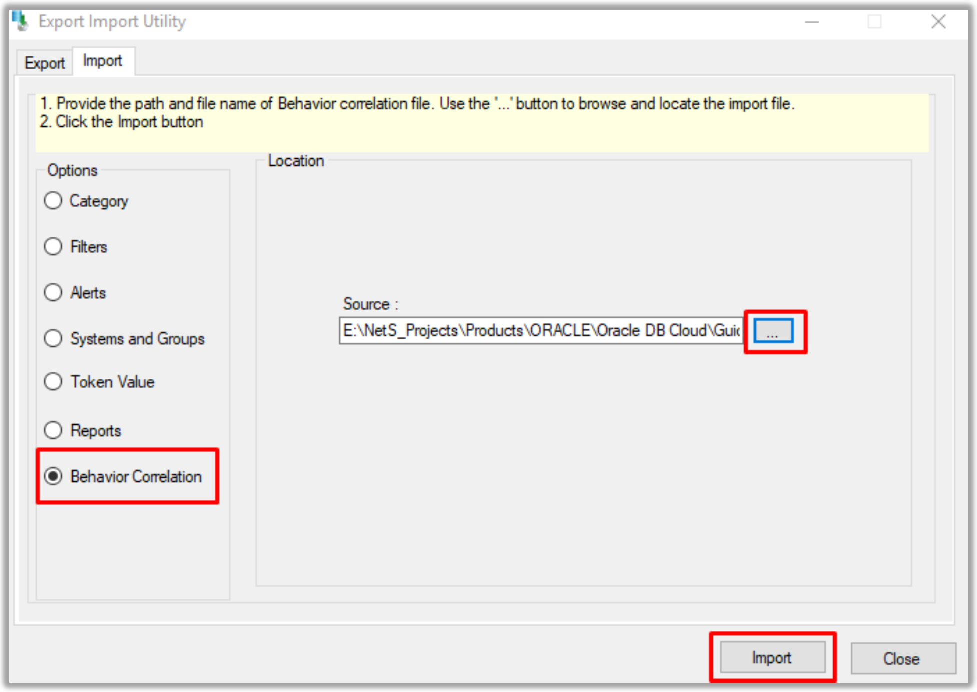


Figure 44

5.7 Behavior rules

1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click the **“Behavior Correlation”** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension **“.isrule”, e.g. “Behavior rule_Oracle database.isrule”** and then click on the “**Import**” button:



1. Provide the path and file name of Behavior correlation file. Use the '...' button to browse and locate the import file.
2. Click the Import button

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
● Behavior Correlation

Source : E:\NetS_Projects\Products\ORACLE\Oracle DB Cloud\Guic ...

Figure 45

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to the **EventTracker manager web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **“ORACLE”** group folder to view the imported categories:

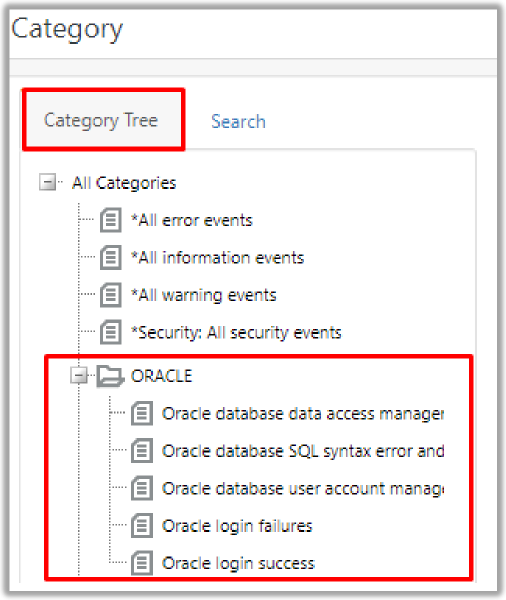
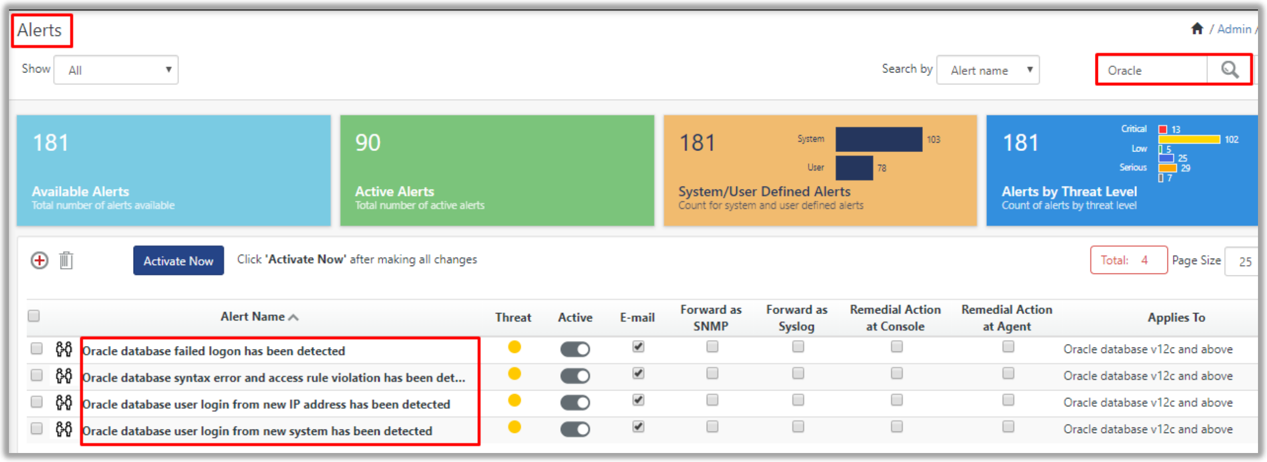


Figure 46

6.2 Alerts

1. In the **EventTracker manager** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **“Oracle”** and then click the **Search** button.
   EventTracker displays an alert related to the Oracle database**:**


Alerts
/ Admin /
Show All
Search by Alert name
Oracle
181
Available Alerts
Total number of alerts available
90
Active Alerts
Total number of active alerts
181
System 103
User 78
System/User Defined Alerts
Count for system and user defined alerts
181
Critical 13
102
Low 5
25
Serious 29
7
Alerts by Threat Level
Count of alerts by threat level
Activate Now
Click 'Activate Now' after making all changes
Total: 4
Page Size 25

□	Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	Oracle database failed logon has been detected	●	●	☑	□	□	□	□	Oracle database v12c and above
□	Oracle database syntax error and access rule violation has been det...	●	●	☑	□	□	□	□	Oracle database v12c and above
□	Oracle database user login from new IP address has been detected	●	●	☑	□	□	□	□	Oracle database v12c and above
□	Oracle database user login from new system has been detected	●	●	☑	□	□	□	□	Oracle database v12c and above

Figure 47

6.3 Parsing Rules

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rule.**
2. In the **Parsing Rule** tab, click on the **"ORACLE"** group folder to view the imported Token Values.

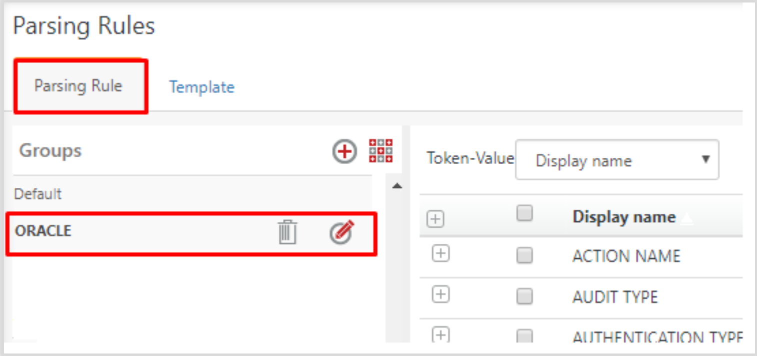


Figure 48

6.4 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.

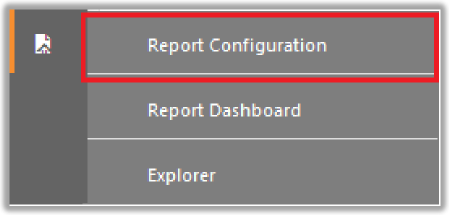
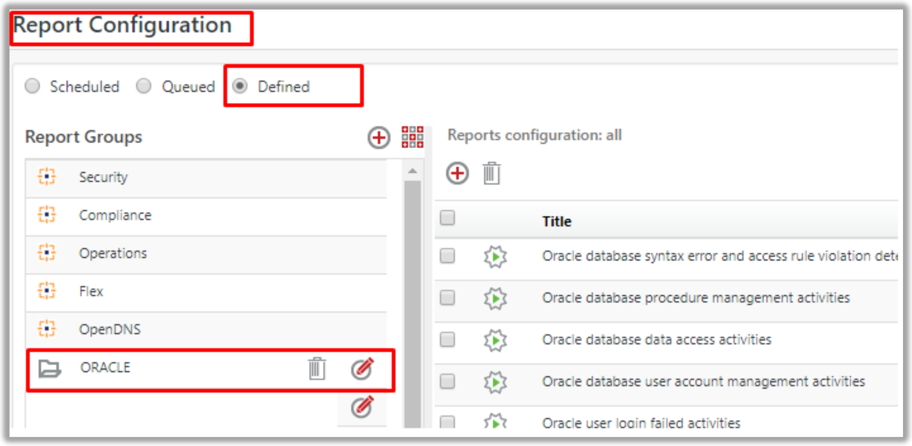


Figure 49

2. In **Reports Configuration** pane, select the **Defined** option.

3. Click on the **“ORACLE”** group folder to view the imported reports.



Report Configuration

○ Scheduled ○ Queued ● Defined

Report Groups

- Security
- Compliance
- Operations
- Flex
- OpenDNS
- ORACLE

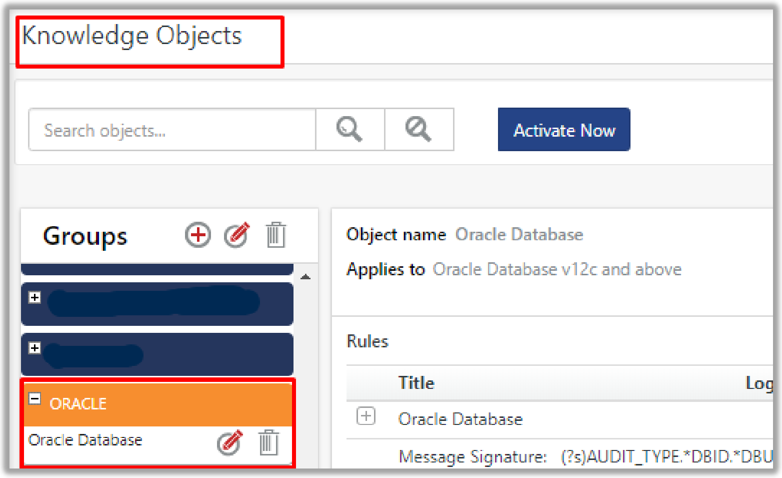
Reports configuration: all

□	Title
□	Oracle database syntax error and access rule violation dete
□	Oracle database procedure management activities
□	Oracle database data access activities
□	Oracle database user account management activities
□	Oracle user login failed activities

Figure 50

6.5 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **“ORACLE”** group folder to view the imported Knowledge objects.



Knowledge Objects

Search objects...

Activate Now

Groups

[redacted]

[redacted]

⊟ ORACLE

Oracle Database

Object name Oracle Database

Applies to Oracle Database v12c and above

Rules

	Title	Log
⊞	Oracle Database	
	Message Signature: (?s)AUDIT_TYPE.*DBID.*DBU	

Figure 51

6.6 Dashboards

1. In the EventTracker web interface, Click on Home Button and select “**My Dashboard**”.

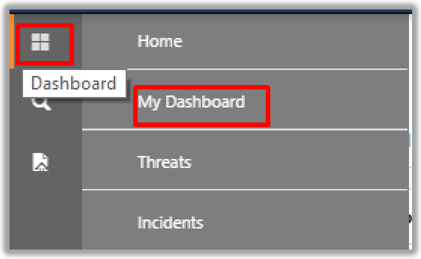


Figure 52

2. In “**Oracle database”** dashboard you should be able to see something like this:

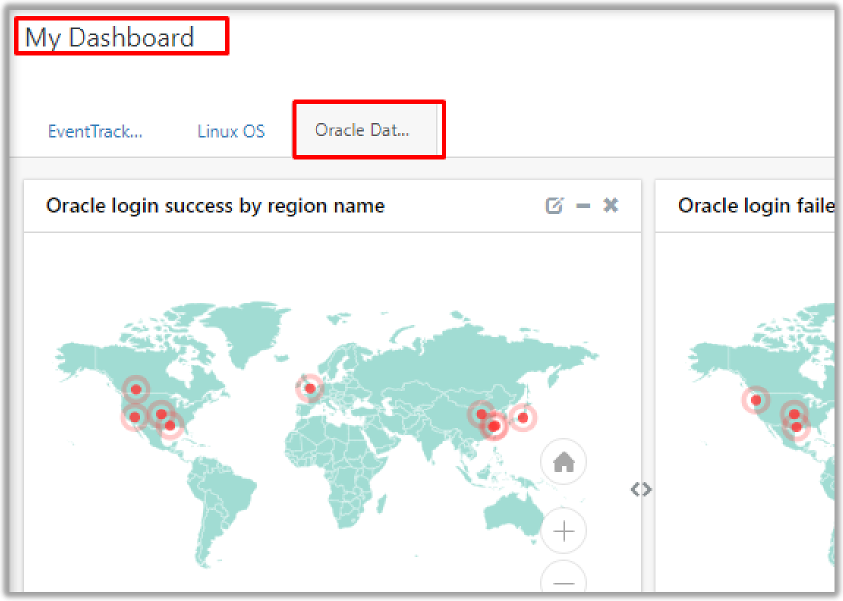
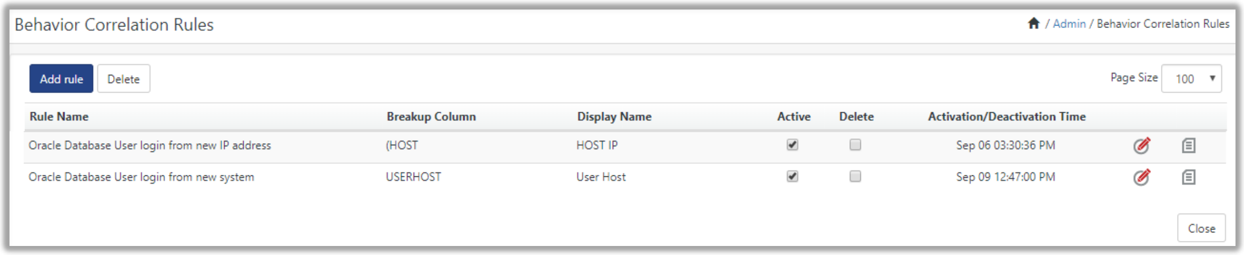


Figure 53

6.7 Behavior rules

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Behavior Correlation Rules.**
2. Increase the Page size to ‘50’ or ‘100’ and scroll down, you will find the recently imported **Behavior Correlation Rules:**


Behavior Correlation Rules

Rule Name	Breakup Column	Display Name	Active	Delete	Activation/Deactivation Time		
Oracle Database User login from new IP address	(HOST	HOST IP	☑	□	Sep 06 03:30:36 PM		
Oracle Database User login from new system	USERHOST	User Host	☑	□	Sep 09 12:47:00 PM		

Figure 54