

# Voltage Database Activity Monitoring

Software Version 24.3.0

User Guide

**opentext™**

Document Release Date: July 2024  
Software Release Date: July 2024

## Legal notices

Copyright 2023 - 2024 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Except as specifically indicated otherwise, this document contains confidential information and a valid license is required for possession, use or copying. If this work is provided to the U.S. Government, consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

## Support

Visit the [MySupport portal](#) to access contact information and details about the products, services, and support that OpenText offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

# Contents

Introduction .....	6
Abbreviations .....	6
Voltage DAM Users and Roles .....	7
Voltage DAM Architecture .....	7
Logging in to Voltage DAM .....	9
Voltage DAM Usage .....	11
Menu and Controls .....	11
Home .....	13
Cluster Status .....	14
Health and Disk .....	15
Index Size .....	15
Database Info .....	16
Top Activity .....	16
Events .....	17
Ongoing Alerts .....	17
Search .....	18
Search Panel .....	18
Date Range Section .....	19
Range .....	20
Export and Save Actions .....	21
Field Chooser .....	21
Historical Alert Processor .....	25
Breakdowns .....	25
Existing Assets .....	26
Queries .....	26
Reports .....	27
Schedule Properties .....	28
Voltage DAM Query Examples .....	30
String Queries .....	30
Specific Field-Based Queries .....	30
Regular Expression Queries .....	31
Regex String Queries .....	31
Regex Queries on Specific Fields .....	32

Alerts .....	33
Dashboard .....	34
Edit Dashboard .....	37
Actions .....	40
Creating a New Dashboard .....	40
Agents .....	42
Agents Tab .....	48
Policies .....	49
Options .....	50
Alert Rules .....	52
Adding New Alert Rule .....	53
Generic Rule .....	54
Missed Rule .....	56
Multi-hit Rule .....	57
Mappings .....	59
Add New Mappings .....	60
Lookup Lists .....	62
Settings .....	63
User Settings .....	64
Adding New User .....	65
User Activities Settings .....	66
Roles Settings .....	67
Adding a New Role .....	68
API Users Settings .....	71
Adding a New API User Guide .....	72
Security Settings .....	72
Notification Group Settings .....	73
Adding a New Notification Group .....	74
Storage Settings .....	74
Main Storage Settings .....	74
Storage Security Settings .....	75
Import Archive Settings .....	75
Restore from Backup .....	75
Storage Curator Settings .....	76
System Notification Settings .....	77
SMTP Server Settings .....	78
LDAP Server Settings .....	79
Action Account Settings .....	80
Alert Forwarding Settings .....	81
Distributed Search Settings .....	82

Multi-Tenant Mapping Settings .....	83
VDAM Mapping .....	83
OpenVAS Account Settings .....	83
File Server Settings .....	84
All Settings .....	85

# Introduction

OpenText™ Voltage Database Activity Monitoring provides privileged user and application access monitoring that is independent of native database logging and audit functions. It can function as a compensating control for privileged user separation-of- duties issues by monitoring administrator activity.

Voltage DAM monitors database activity without audit subsystem of the respective database server being turned on. It classifies and correlates the audit logs and store them outside the database to comply with seperation-of-duties principle. Voltage DAM also ensures that a service account only accesses a database from a defined source, and only runs a narrow group of authorized queries. This can be used to detect compromises of a service account either from the system that normally uses it, or if the account credentials show up in a connection from an unexpected system.

Voltage DAM Agents can record all SQL transactions (DML, DDL, DCL, and TCL) without relying on local database logs, thus reducing performance degradation. Voltage DAM lets you:

**Monitor Logins** - Monitor successful and failed logons and ensure they are from predefined and valid sources.

**Monitor Changes** - Audit SELECT, UPDATE, DELETE, EXEC, and other SQL statements.

**Monitor Access to Sensitive Information** - Monitor who is accessing sensitive information. When the unexpected happens generate alerts.

**Monitor Privileged Users** - Audit DBA/Developer activity and configuration changes to the database system.

**Generate Reports** - Pre-defined policies and reports for PCI, SOX, and other generic compliance requirements.

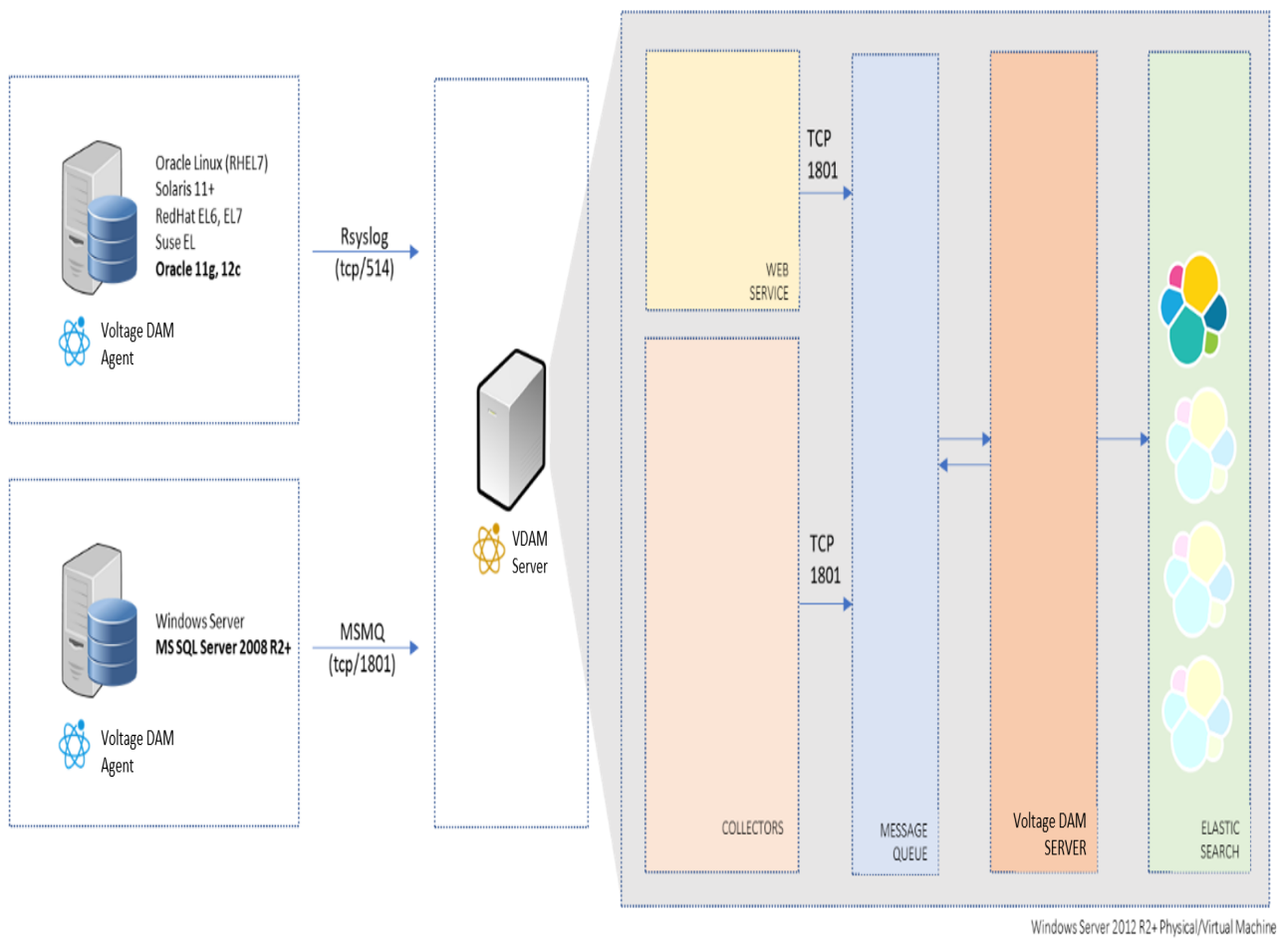
## Abbreviations

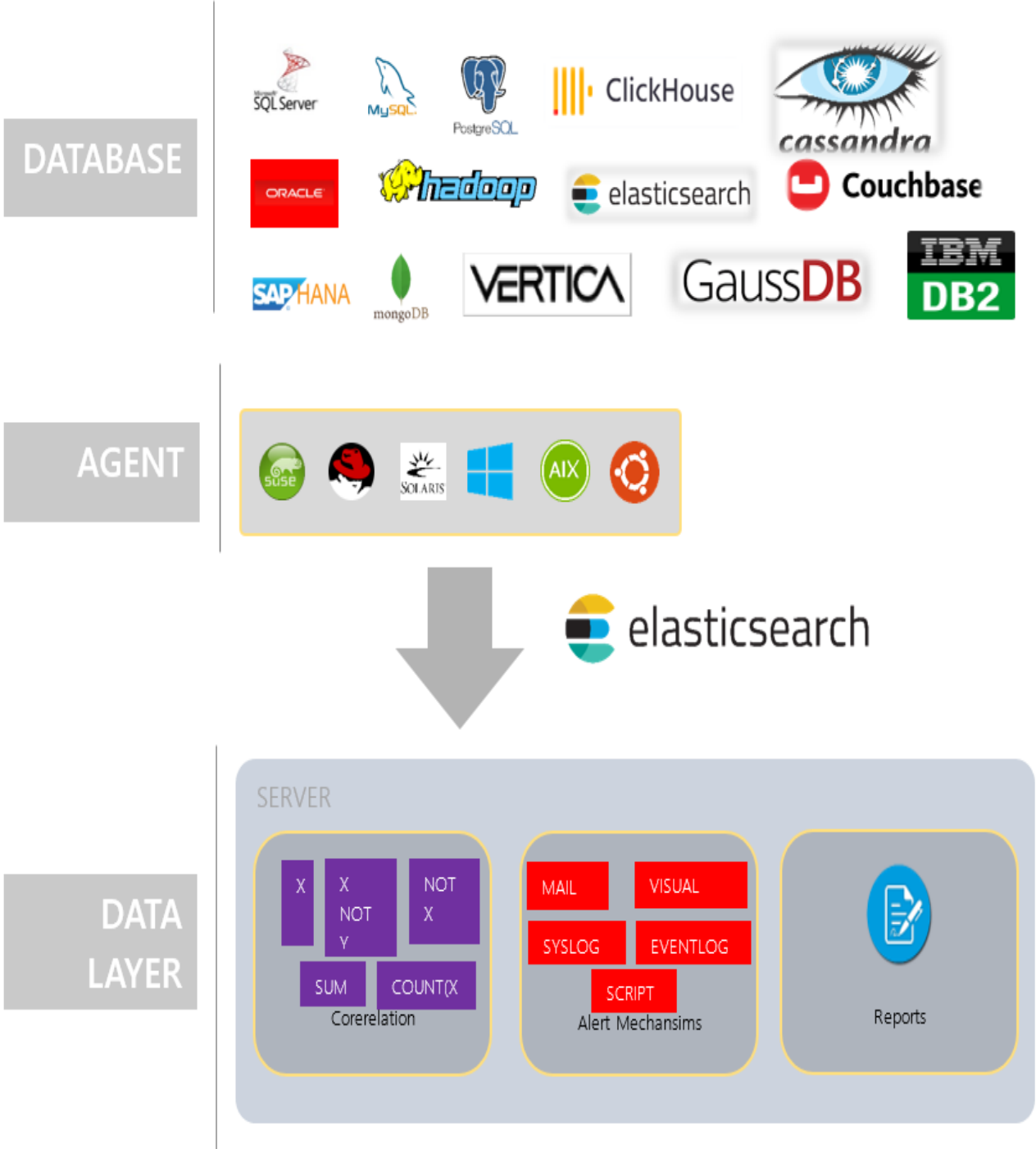
Abbreviations	Definition
DAM	Database Activity Monitoring
DSIM	Voltage DAM Installation Manager
DSPL	Voltage DAM Socket TAP Module
DSTAP	Voltage DAM TAP Module
LDAP	Lightweight Directory Access Protocol
OpenVAS	Open Vulnerability Assessment Scanner
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol

## Voltage DAM Users and Roles

Voltage DAM has flexible user role management support that makes Voltage DAM available to create its roles depending on the privileges defined before. These roles are like groups in Voltage DAM. New roles can be created by admin, and users can be assigned to these roles. For more details, see [All Settings](#).

## Voltage DAM Architecture







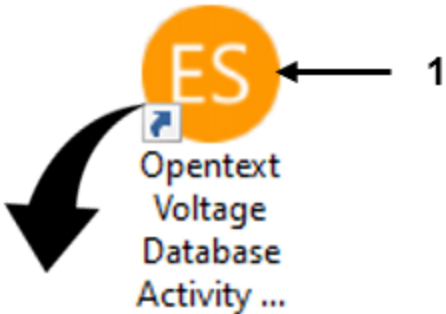
## Logging in to Voltage DAM

The user should log in to OpenText Voltage Database Activity Monitoring application.

1. Double click on OpenText Voltage Database Activity Monitoring (1) application.
2. Enter **Server Name** (2) **Username** (3) and **Password** (4) on the OpenText Voltage DAM application
3. Click **Sign In** (5) button.

**NOTE:** The Server Name field can be filled in 3 ways: localhost, Server IP, or Server hostname.

- If logging in through the server, the user writes localhost.
- If accessing the server from user's environment, the user writes the Server IP or Server hostname.



**opentext™** | Voltage  
Database Activity Monitoring

Server Name  ← 2

User Name  ← 3

Password  ← 4

Remember me

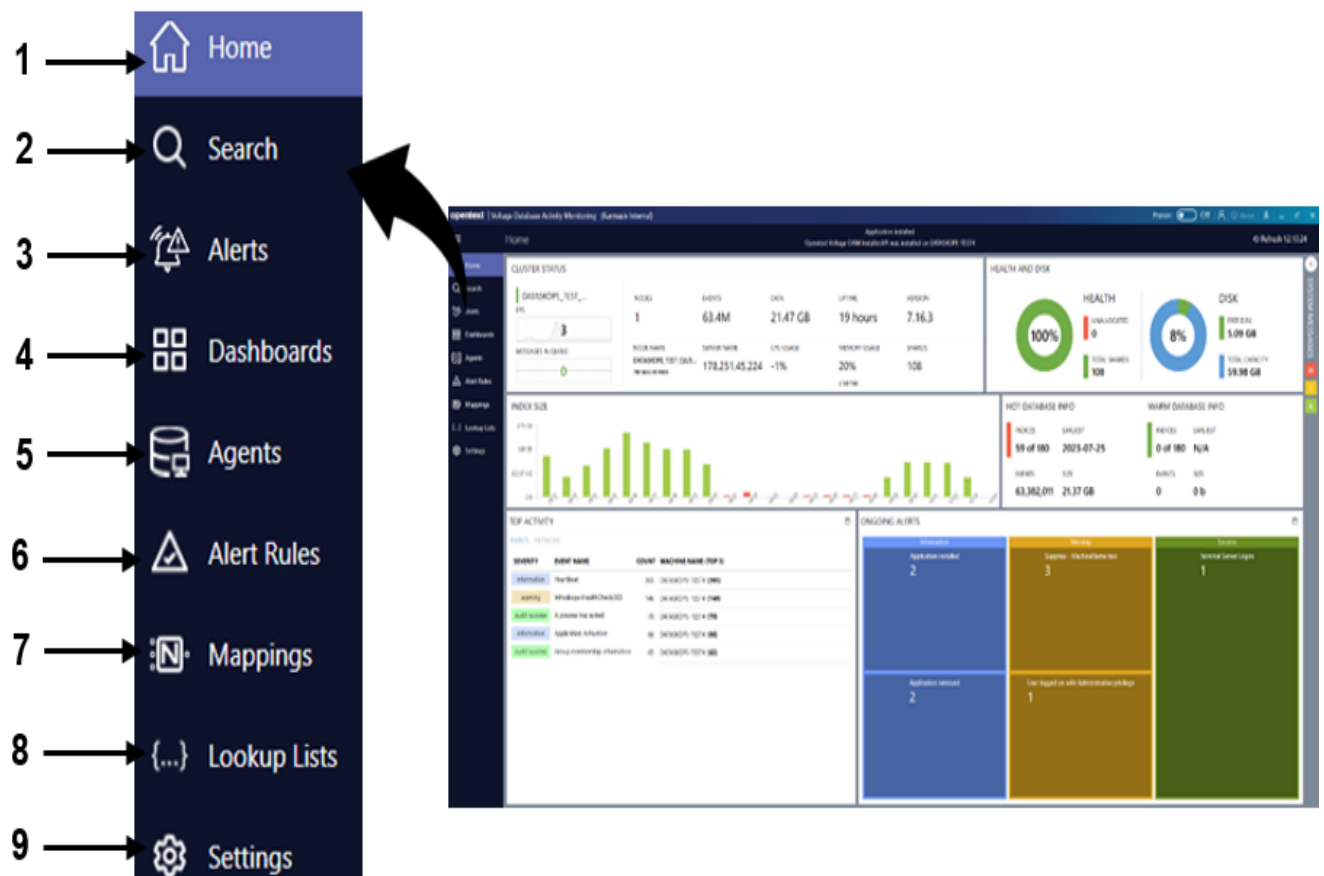
Sign in ← 5

Copyright 2023 Open Text. All Rights Reserved. Trademarks owned by Open Text.

# Voltage DAM Usage

## Menu and Controls



Voltage DAM has nine menu items and some control buttons. These are listed in the table below


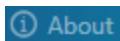

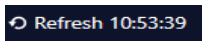




Ref.	Menus	Function
1	Home	Used to display the home screen of Voltage DAM.
2	Search	Used to search events and export search results as xls or pdf.
3	Alerts	Used to view alerts in detail.
4	Dashboards	Used to view and edit dashboards.
5	Agents	Used to show Agents, Policies and Options tabs, and Refresh, New Agent, Edit, Delete, Actions (Export, Send as E-mail) and Open Terminal

		tasks.
6	Alert Rules	Used to show alert and correlation rules.
7	Mappings	Used to view, edit and manage mappings in detail.
8	Lookup List	Used to show Lookup Lists.
9	Settings	Used to reach Settings as Users, User Activities, Roles, API Users etc.

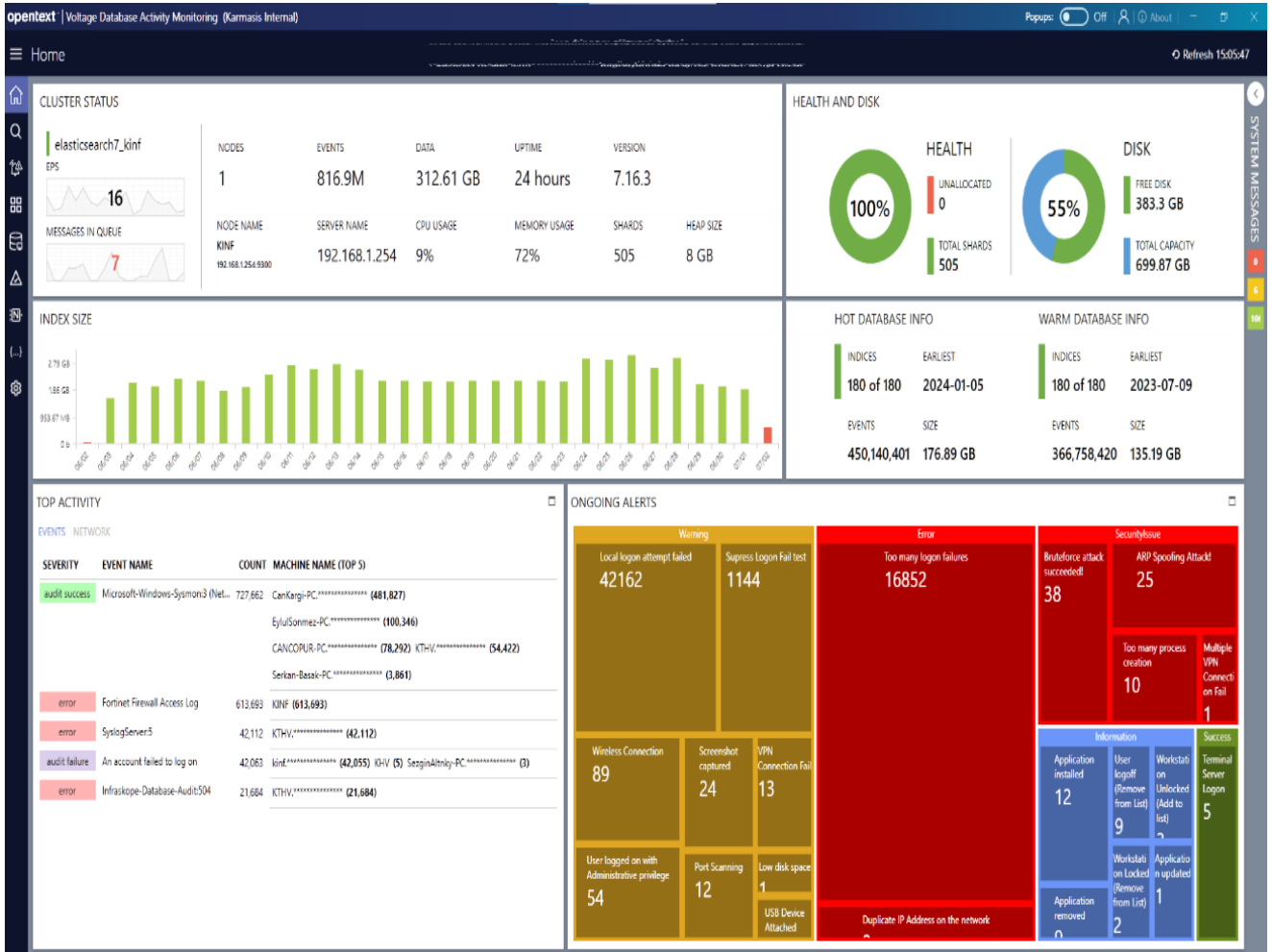


Ref.	Menus	Function
1		Used to close and open the menu on the left. The menu part can be closed for a wider graphic view.
2		Used to turn pop-up contents on or off.

3		Used to reach user details. Includes <b>Logged On Users</b> , <b>My Profile</b> and <b>Logout</b> submenus.
4		Used to show Copyright, Version, Disclaimer and License information
5		Used to check updates
6		Used to refresh.
7		Used to show System Errors (red), Warnings (yellow) and Messages (green). Details and content can be viewed with the (  ) icon. The numbers in the colored boxes indicate the number of errors, warnings, and messages.

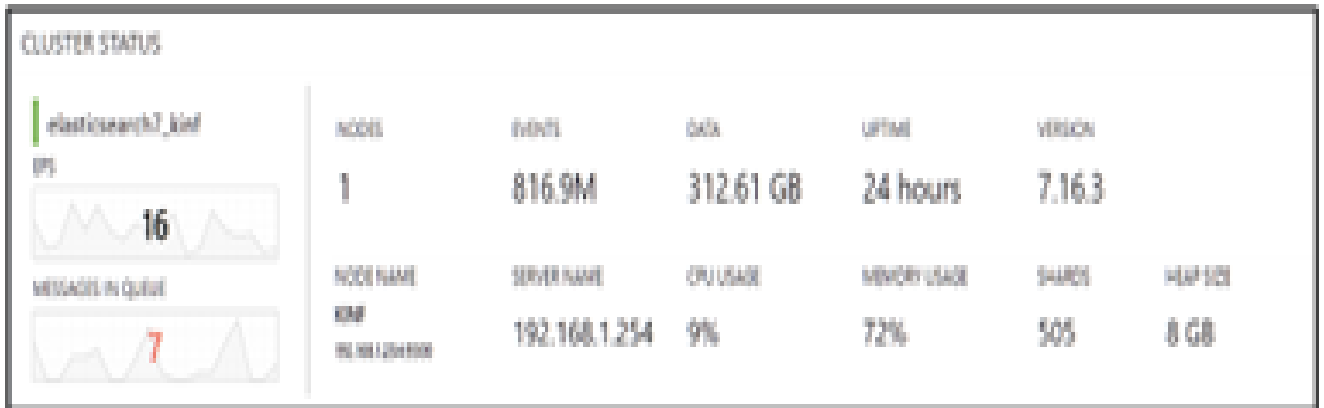
## Home

Performing an analysis of the current situation using a single screen facilitates efficient work management by enabling prompt actions to be executed. Accordingly, **Home** screen presents **Cluster Status**, **Health** and **Disk**, **Index Size**, **Database Info**, **Top Activity** and **Ongoing Alerts** analysis to the user.



## Cluster Status

The panel containing information about ElasticSearch provides insights into the status of your system. The most important feature on this screen is the ability to monitor the performance of the machine where the SIEM product is currently installed in real-time.

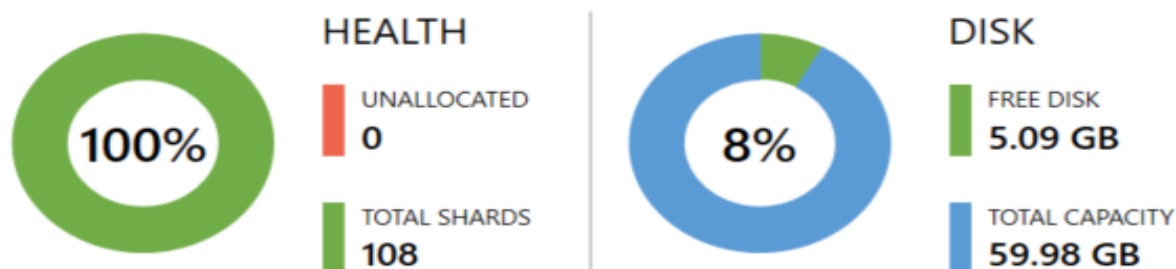


- **Nodes** shows the number of shards in the database (determined based on the system size).
- **Events** shows the number of events in the database.
- **Data** shows the record size.
- **Uptime** shows the active time period of the system.
- **Version** shows database version number.
- **Node Name** shows the node name.
- **Server Name** shows the server's name.
- **CPU Usage** shows the CPU usage percentage.
- **Memory Usage** shows the memory usage percentage. The max value, is also given with the Memory Usage, shows the amount of memory allocated for ElasticSearch. In Figure 5, the max value for ElasticSearch is given as 3 GB max.
- **Shards** shows the number of the small unit where records are stored.
- **Heap Size** shows the amount of allocated RAM to the Elasticsearch mode.
- **EPS** shows the events per second.
- **Messages in Queue** shows the real-time incoming log count.

## Health and Disk

This panel shows the information about cluster health and disk capacities.

### HEALTH AND DISK



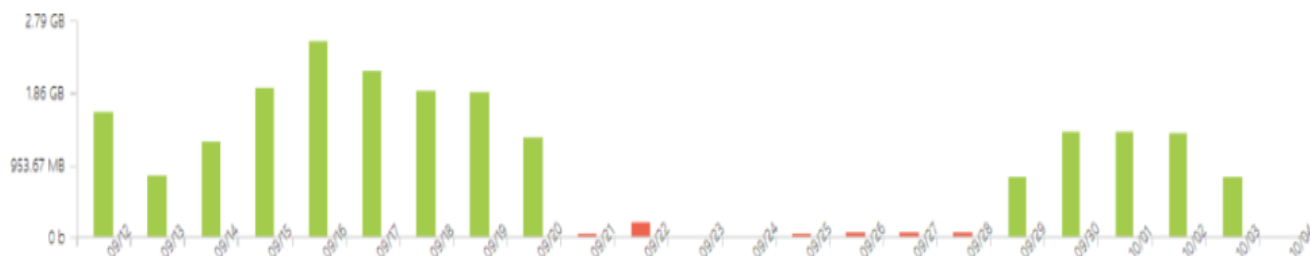
- **Unallocated** shows the available unit count.
- **Total Shards** shows the number of the small unit where records are stored.
- **Free Disk** shows the remaining free space on the disk.
- **Total Capacity** shows the total disk capacity.

## Index Size

This panel shows how many computers are sending logs, how many computers have Voltage DAM agent installed in Active Directory, and how many computers have not connected to the system for a

long time. Index Size is the database index, it graphically shows the amount of logs written to the database. If the log amount is the expected (average) number, the bar is shown green, if it is more than or lower than expected, the bar is shown red.

### INDEX SIZE



## Database Info

This panel shows the number of records and the amount of space they occupy in two separate databases categorized as HOT and WARM. Hot database keeps records for the specified number of days. In default, the number of days is given as 180 and it keeps records of the last 180 days. Warm database keeps a record of 180 days before hot database records.

### HOT DATABASE INFO

INDICES EARLIEST  
**59 of 180** **2023-07-25**

EVENTS SIZE  
**63,382,054** **21.37 GB**

### WARM DATABASE INFO

INDICES EARLIEST  
**0 of 180** **N/A**

EVENTS SIZE  
**0** **0 b**

- Indices shows the number of days for real-time log retention.
- Earliest shows the start date of log collection.
- Events shows the number of events.
- Size shows the total size of the events.

## Top Activity

This panel shows the events and network activities based on their importance level, with the ability to determine the number of top items to display.

Top Activity panel, which operates in sync with INDEX SIZE, potentially provides you with the most important information. It presents records sorted by the importance level, name, and quantity of the generated events. Additionally, it also provides information about which machine the respective events occurred on and how many instances occurred.



TOP ACTIVITY ☐

EVENTS NETWORK

SEVERITY	EVENT NAME	COUNT	MACHINE NAME (TOP 5)
information	Heartbeat	388	DATASKOPE-TEST4 (388)
warning	Infraskope-HealthCheck:503	155	DATASKOPE-TEST4 (155)
audit success	Group membership information	73	DATASKOPE-TEST4 (73)
audit success	A process has exited	71	DATASKOPE-TEST4 (71)
information	Application Activation	66	DATASKOPE-TEST4 (66)

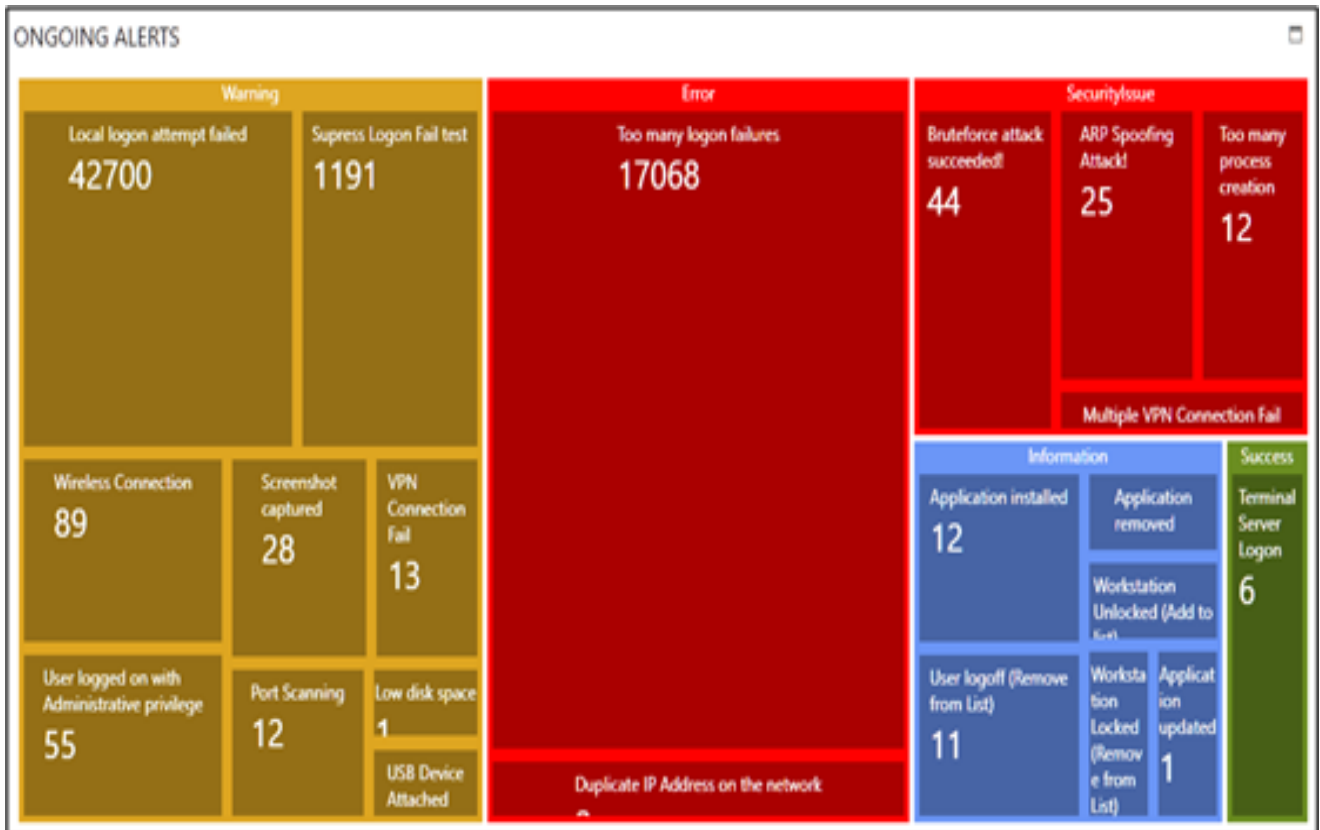
### Events

- **Severity** shows the event type.
- **Event Name** shows the event description.
- **Count** shows the number of occurrences of the event.
- **Machine Name** shows the machine name where the event occurred.

### Ongoing Alerts

This panel shows critical events occurring during the day. It also provides alarm rules that have been predefined or created according to the organization's needs on the monitor screen. Relevant alarms are color-coded based on the criteria of the events.

When clicked on the relevant alarm, user can view the details of the events that occurred in a new tab.



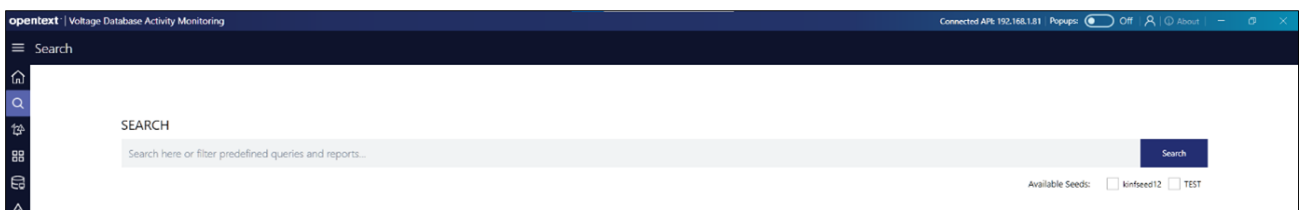
- **Warning** shows the warnings on clients.
- **Error** shows the unsuccessful attempts on clients.
- **Security Issue** shows the security breaches and vulnerabilities.
- **Information** shows the information of actions on clients.
- **Success** shows the successful actions.

## Search

Search panel provides a search engine where user can examine event records in detail.

### Search Panel

In this screen, user can run automatically generated queries by the system or create new queries to capture specific records. Users can select and search for different SearchDB clusters/seeds from Available Seeds options through a single Search UI.



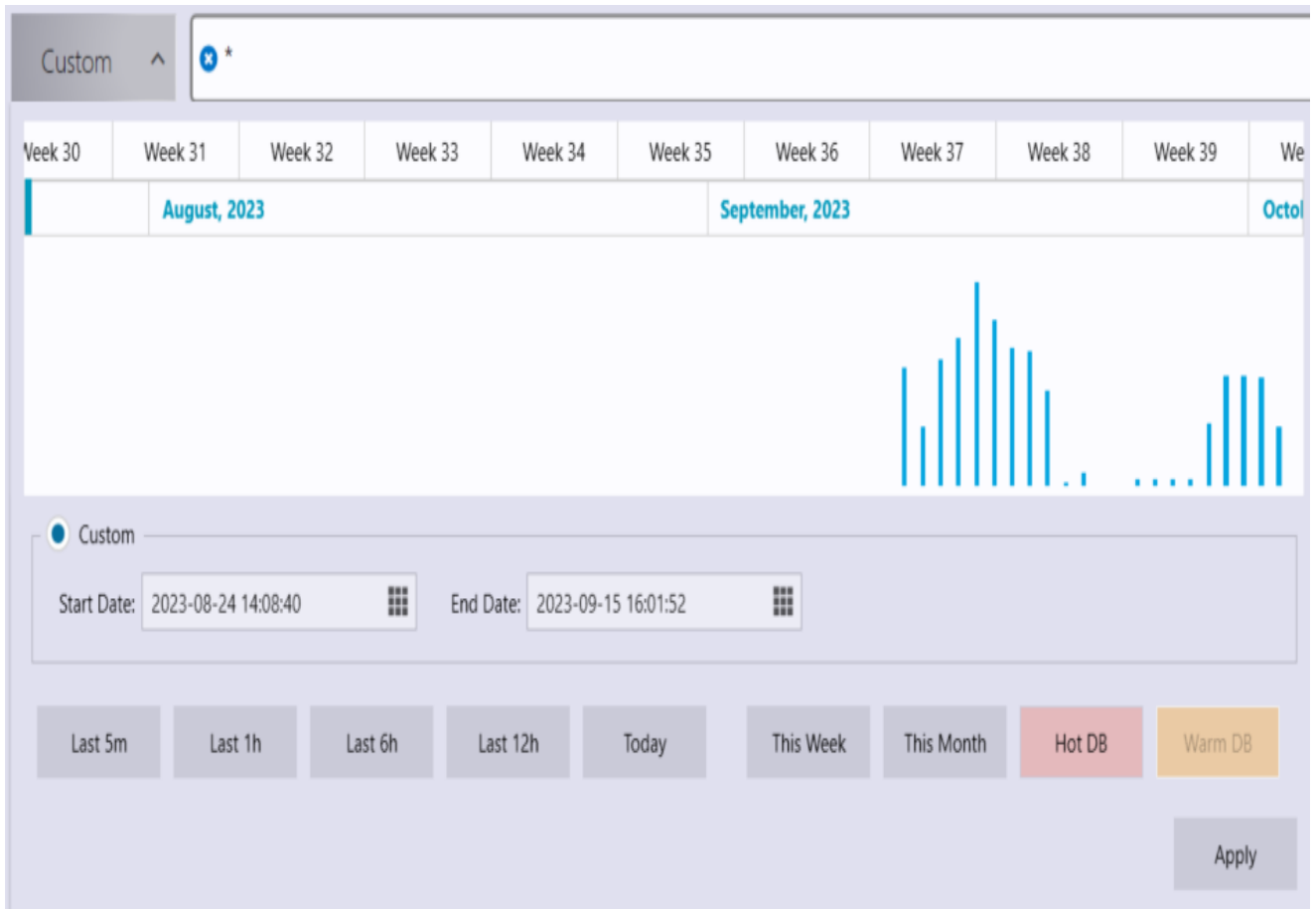
Accordingly, the Search screen presents Breakdowns, Search Results, Event Details and Field Chooser to the user.

The screenshot shows the Voltage Database Activity Monitoring (VDAM) Search screen. At the top, it displays the search criteria: 'Hot DB' and 'EventSource:SqlServer-Audit'. The search results are summarized as 296,310,527 events in 29,236 records. The interface is divided into four main sections:

- BREAKDOWNS:** A list of event categories with their respective counts. For example, 'rpc\_completed' has 143,391,731 events, 'sql\_login' has 70,000,899, and 'sql\_text\_completed' has 9,919,881.
- SEARCH RESULTS:** A table showing search results with columns: Keywords, TimeCreated, MachineName, Name, and Summary. The results are sorted by TimeCreated in descending order.
- EVENT DETAILS:** A detailed view of a selected event, showing its JSON structure and various fields. The event is 'rpc\_completed' with a summary of 'sa - 138 -> AuditDB -> exec sp\_who2top'. The JSON includes fields like 'Log Name', 'Source', 'Event ID', 'Level', 'User Name', and 'Machine Name'.
- FIELD CHOOSER:** A section for selecting fields to display in the search results. It includes a list of 'Standard Fields' and 'Dynamic Fields' with checkboxes for selection.

### Date Range Section

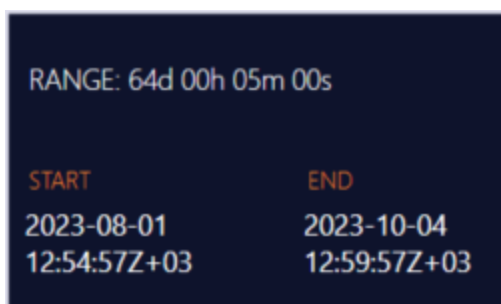
The date range section is automatically set to scan events that occurred within the last 5 minutes. Additionally, users can click on the relevant section to customize the date range according to their preferences.




Users can finalize their search by using the mouse to select the preferred time period on the chart. This empowers individuals to clearly define the precise time span they require. In the date range section, aside from the regular time intervals, there are choices labeled as Hot DB and Warm DB. Hot DB pertains to the initial 180 days, while Warm DB relates to the subsequent 180-day period. These choices enable individuals to conduct searches within both the currently active data and the archived data, all within the specific time spans they've chosen to search within the active and archived data for the specified time periods.

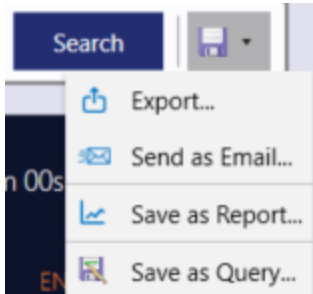
### Range

Range Panel provides information about the time range for which the report was generated.

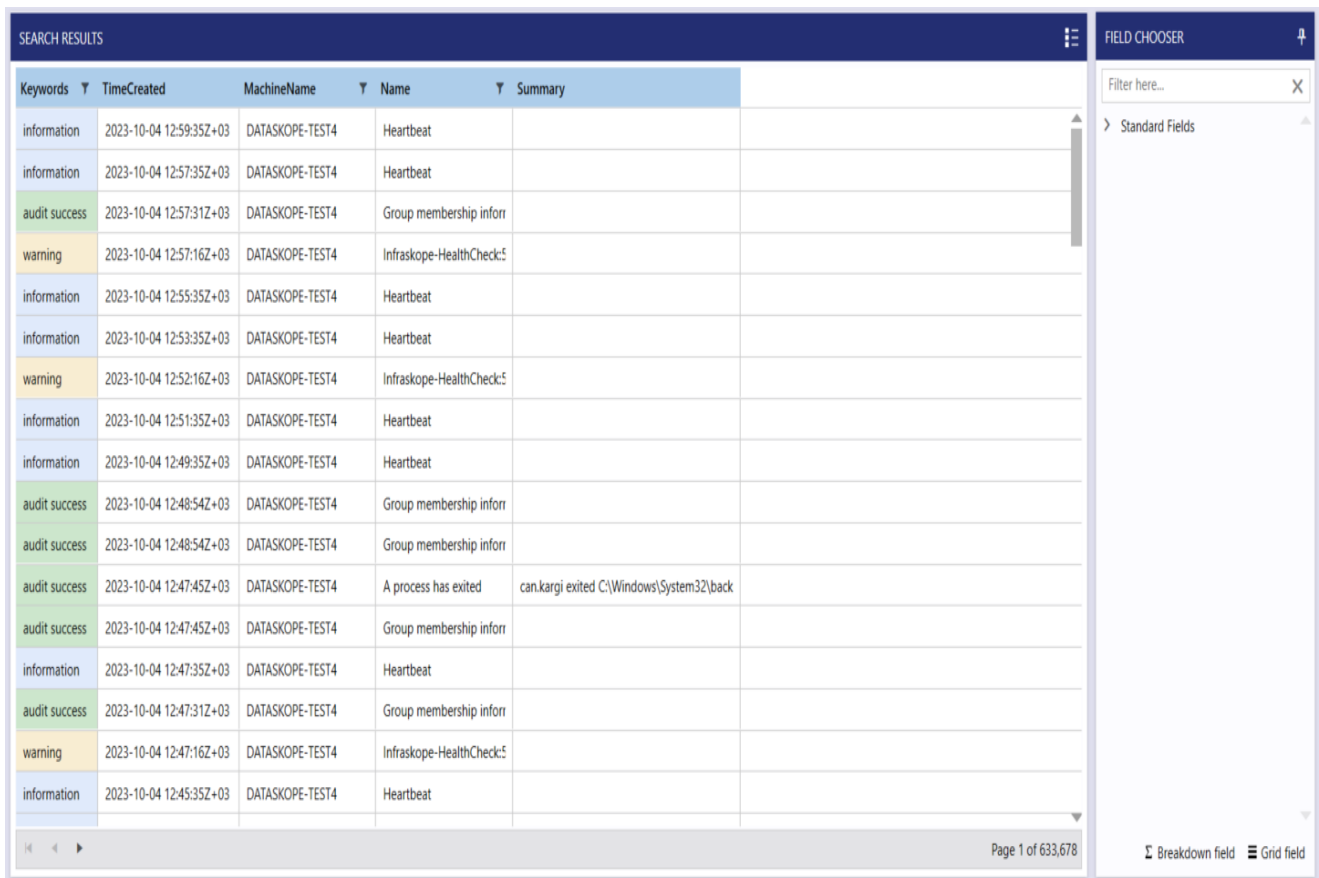


### Export and Save Actions

After completing the search, users can save the results as report or query, export them in Excel or PDF format, or send it via email by using the Save  button.

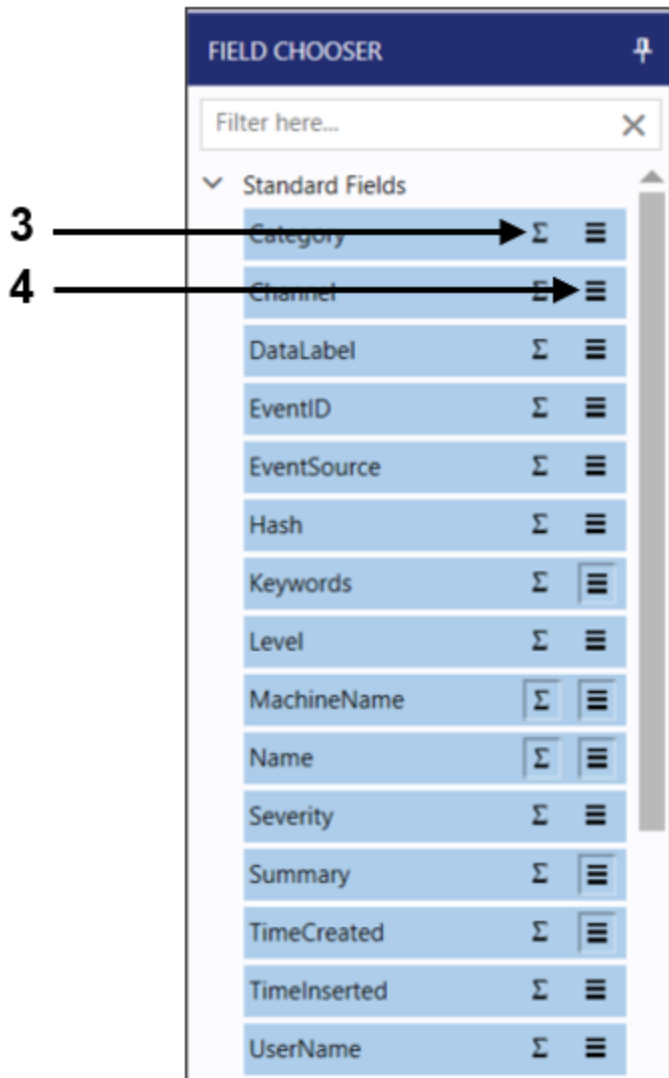


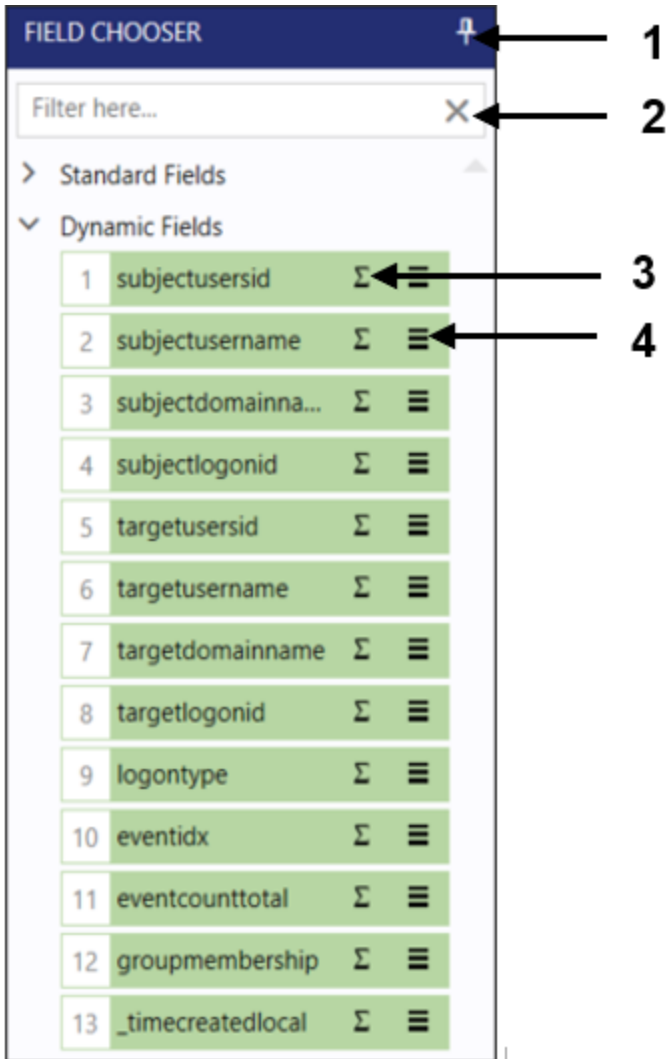
### Field Chooser



Keywords	TimeCreated	MachineName	Name	Summary
information	2023-10-04 12:59:35Z+03	DATASKOPE-TEST4	Heartbeat	
information	2023-10-04 12:57:35Z+03	DATASKOPE-TEST4	Heartbeat	
audit success	2023-10-04 12:57:31Z+03	DATASKOPE-TEST4	Group membership inform	
warning	2023-10-04 12:57:16Z+03	DATASKOPE-TEST4	Infraskope-HealthCheck:5	
information	2023-10-04 12:55:35Z+03	DATASKOPE-TEST4	Heartbeat	
information	2023-10-04 12:53:35Z+03	DATASKOPE-TEST4	Heartbeat	
warning	2023-10-04 12:52:16Z+03	DATASKOPE-TEST4	Infraskope-HealthCheck:5	
information	2023-10-04 12:51:35Z+03	DATASKOPE-TEST4	Heartbeat	
information	2023-10-04 12:49:35Z+03	DATASKOPE-TEST4	Heartbeat	
audit success	2023-10-04 12:48:54Z+03	DATASKOPE-TEST4	Group membership inform	
audit success	2023-10-04 12:48:54Z+03	DATASKOPE-TEST4	Group membership inform	
audit success	2023-10-04 12:47:45Z+03	DATASKOPE-TEST4	A process has exited	can.kargi exited C:\Windows\System32\back
audit success	2023-10-04 12:47:45Z+03	DATASKOPE-TEST4	Group membership inform	
information	2023-10-04 12:47:35Z+03	DATASKOPE-TEST4	Heartbeat	
audit success	2023-10-04 12:47:31Z+03	DATASKOPE-TEST4	Group membership inform	
warning	2023-10-04 12:47:16Z+03	DATASKOPE-TEST4	Infraskope-HealthCheck:5	
information	2023-10-04 12:45:35Z+03	DATASKOPE-TEST4	Heartbeat	

When you right-click on the unwanted columns in the query report and select "Remove" the respective column will be removed from the report area.







Field Chooser panel provides two different field structures:

**Standard Fields:** It lists the columns that exist in the standard event records and are automatically displayed in the report screen.

**Dynamic Fields:** It lists the columns that have been defined based on the user's specific needs, beyond the standard columns for event records. The button on the right side of the column is used for hiding unwanted or re-adding desired columns.

Ref.	Controls	Function
1		Used to hide the Field Chooser panel.
2		Used to filter the fields.

3		Used to add the filter to the Breakdowns list.
4		Used to add the filter to the search results table as a column.

SEARCH RESULTS				
Keywords	TimeCreated	MachineName	Name	Summary
information	2023-10-04 12:59:35Z+03	DATASKOPE-TEST4	Heartbeat	
information	2023-10-04 12:57:35Z+03	DATASKOPE-TEST4	Heartbeat	
audit success	2023-10-04 12:57:31Z+03	DATASKOPE-TEST4	Group membership inform	
warning	2023-10-04 12:57:16Z+03	DATASKOPE-TEST4	Infraskope-HealthCheck:5	
information	2023-10-04 12:55:35Z+03	DATASKOPE-TEST4	Heartbeat	
information	2023-10-04 12:53:35Z+03	DATASKOPE-TEST4	Heartbeat	
warning	2023-10-04 12:52:16Z+03	DATASKOPE-TEST4	Infraskope-HealthCheck:5	
information	2023-10-04 12:51:35Z+03	DATASKOPE-TEST4	Heartbeat	
information	2023-10-04 12:49:35Z+03	DATASKOPE-TEST4	Heartbeat	
audit success	2023-10-04 12:48:54Z+03	DATASKOPE-TEST4	Group membership inform	
audit success	2023-10-04 12:48:54Z+03	DATASKOPE-TEST4	Group membership inform	
audit success	2023-10-04 12:47:45Z+03	DATASKOPE-TEST4	A process has exited	can.kargi exited C:\Windows\System32\back
audit success	2023-10-04 12:47:45Z+03	DATASKOPE-TEST4	Group membership inform	
information	2023-10-04 12:47:35Z+03	DATASKOPE-TEST4	Heartbeat	
audit success	2023-10-04 12:47:31Z+03	DATASKOPE-TEST4	Group membership inform	
warning	2023-10-04 12:47:16Z+03	DATASKOPE-TEST4	Infraskope-HealthCheck:5	
information	2023-10-04 12:45:35Z+03	DATASKOPE-TEST4	Heartbeat	

Page 1 of 633,678

When the user right-clicks on any row in the Search Results table, the user can reach the actions given below.

- **Edit Summary:** Used to edit the summary.
- **Check Integrity [For All Events, For Selected Events]:** Used to check integrity for all events or selected events.
- **Add Drop Rule:** Used to add a drop rule.
- **Create Alert Rule:** Used to create an alert rule.
- **Find Related:** Used to find related query.



### Historical Alert Processor

Users can select historical logs to correlate/create alerts with newly added rules. This feature provides the ability to re-process certain database activities based on newly added rules.

Keywords	TimeCreated	MachineName	Name	Summary
information	2024-07-01 14:48:40Z+03	KNF	sa_logout	sa logged out from client 192.168.1.254
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 619 -> AuditDB -> exec sp_executesql
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 361 -> AuditDB -> exec sp_executesql
information	2024-07-01 14:48:40Z+03	KNF	sa_logout	sa logged out from client 192.168.1.254
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 47 -> AuditDB -> exec sp_reset_connection
information	2024-07-01 14:48:40Z+03	KNF	sa_login	sa user logged on to KNF
information	2024-07-01 14:48:40Z+03	KNF	sa_login	sa user logged on to KNF
information	2024-07-01 14:48:40Z+03	KNF	sa_login	sa -> 232 -> AuditDB -> exec sp_executesql
information	2024-07-01 14:48:40Z+03	KNF	sa_logout	sa logged out from client 192.168.1.254
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 14 -> AuditDB -> exec sp_reset_connection
information	2024-07-01 14:48:40Z+03	KNF	sa_login	sa user logged on to KNF
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 286 -> AuditDB -> exec sp_executesql
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 182 -> AuditDB -> exec sp_executesql
information	2024-07-01 14:48:40Z+03	KNF	sa_logout	sa logged out from client 192.168.1.254
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 16 -> AuditDB -> exec sp_reset_connection
information	2024-07-01 14:48:40Z+03	KNF	sa_login	sa user logged on to KNF
information	2024-07-01 14:48:40Z+03	KNF	rpt_completed	sa -> 167 -> AuditDB -> exec sp_executesql

### Breakdowns

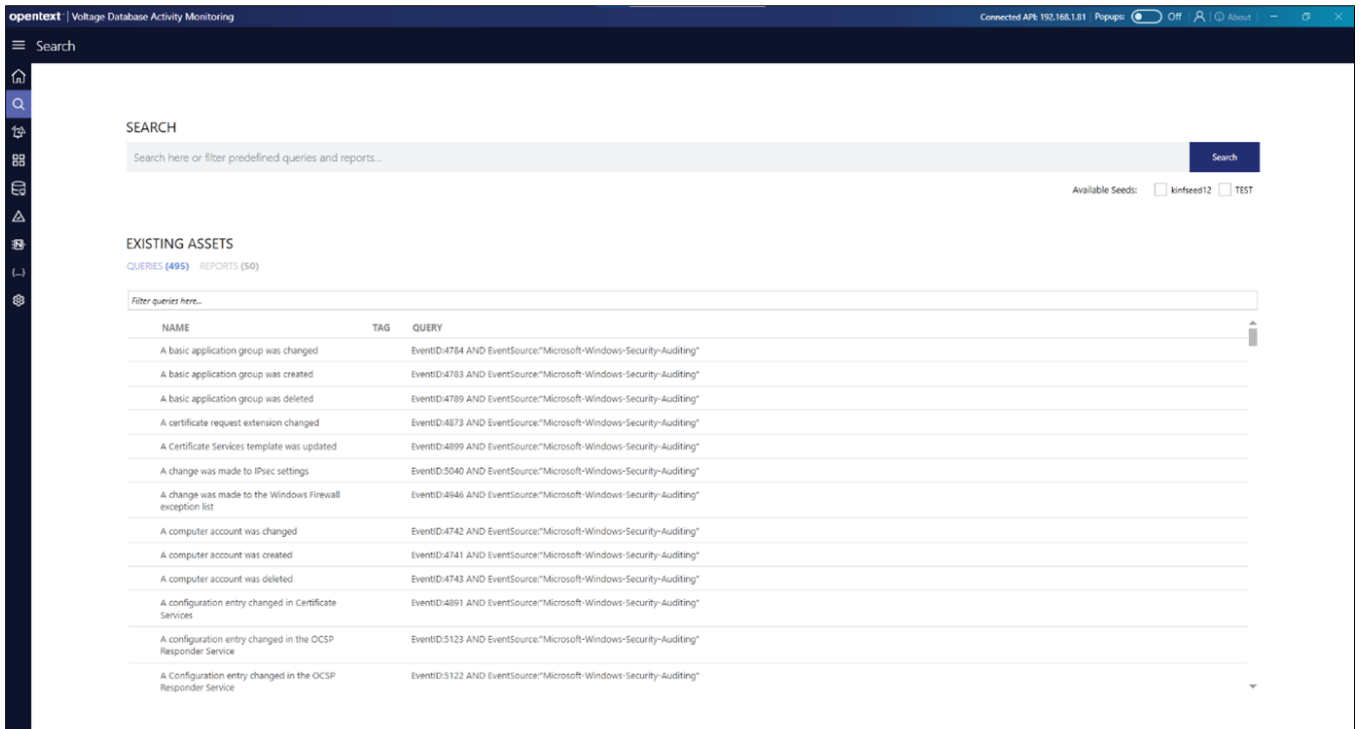
Breakdowns panel is used to access breakdown event easily on a categorized list.

BREAKDOWNS	
Filter here... X	
MachineName (5)	
<a href="#">DATASKOPE-TEST4</a>	60,799,477
<a href="#">192.168.1.111</a>	2,518,616
<a href="#">oracle19</a>	26,553
<a href="#">WIN-F84RHN67HRR</a>	22,918
<a href="#">ubuntutest</a>	176
Name (6)	
<a href="#">rpc_completed</a>	26,473,416
<a href="#">sql_logout</a>	12,846,396
<a href="#">sql_login</a>	12,846,374
<a href="#">error_reported</a>	2,861,636
<a href="#">Dataskope-JSONFiles-Audit:9500</a>	2,518,616
<a href="#">Other</a>	5,821,296

## Existing Assets

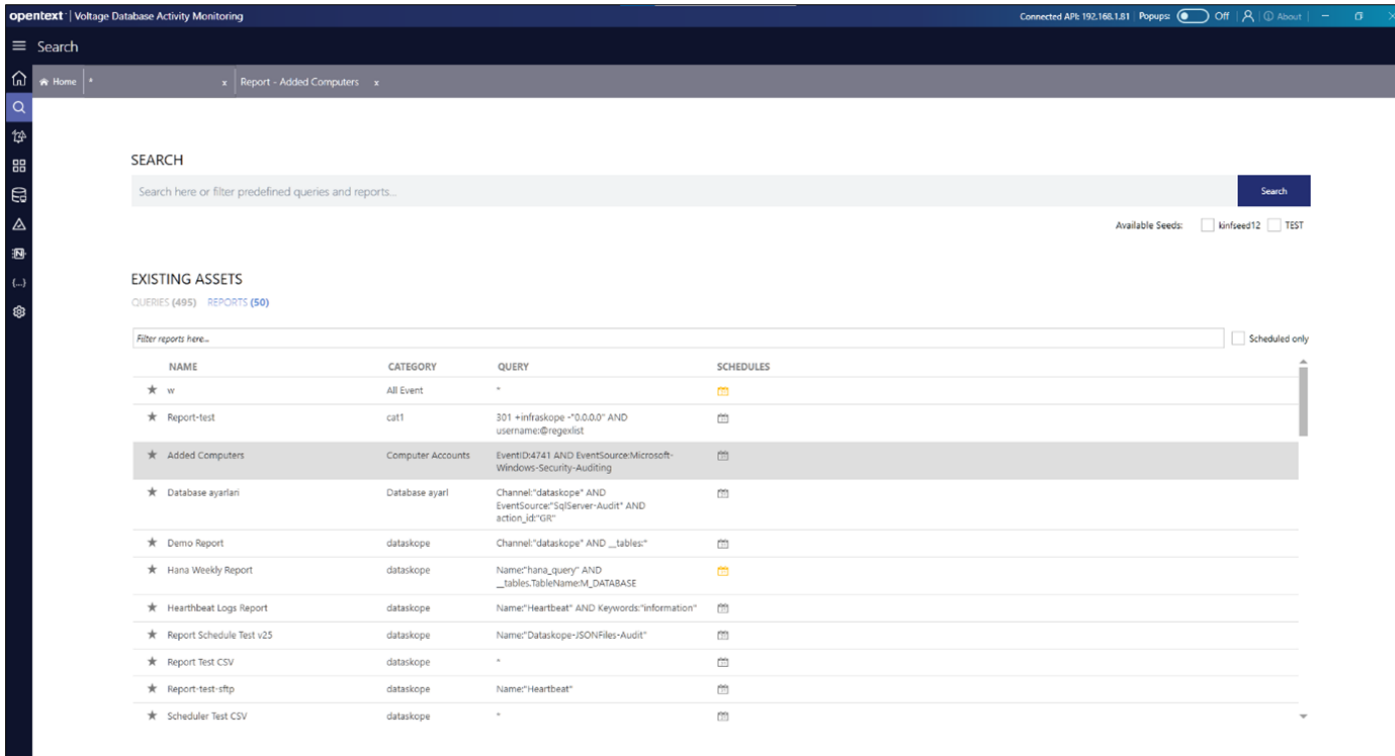
### Queries

The queries used for the search criteria are listed here. When desired, query results can be accessed by clicking on the relevant query.



## Reports

The available query results are reported. It is possible to schedule to receive these reports regularly.



## Schedule Properties

Export criteria of scheduled reports are selected.

**Schedule Properties**

Enable Schedule

GENERAL TRIGGER

Content:  Data  Summary

File Name: File Name

Format: Csv

Page Size: A4

Page Orientation: Portrait

CSV Options:  Convert time to local  Show column headers  
 Enclose value in double quotes  Clear double quotes inside value

Delimiter:  Tab  Semicolon  Comma  Space  Other

Email File Share FTP Share

Enable

Subject: Auto generated alert

Subscribers:   Notification groups only

Apply classification rules for subscribers

SAVE CANCEL

**Schedule Properties**

Enable Schedule

GENERAL TRIGGER

Content:  Data  Summary

File Name: File Name

Format: Excel

Page Size: A4

Page Orientation: Portrait

CSV Options:  Convert time to local  Show column headers  
 Enclose value in double quotes  Clear double quotes inside value

Delimiter:  Tab  Semicolon  Comma  Space  Other

Email File Share FTP Share

Enable

Share Path:  BROWSE

Domain Name:  User Name:

Password:

TEST CONNECTION

SAVE CANCEL

Schedule Properties

Enable Schedule

GENERAL TRIGGER

Content:  Data  Summary

File Name: File Name

Format: Excel

Page Size: A4

Page Orientation: Portrait

CSV Options:  Convert time to local  Show column headers  
 Enclose value in double quotes  Clear double quotes inside value

Delimiter:  Tab  Semicolon  Comma  Space  Other

Email File Share FTP Share

File sending with FTP enabled  File sending with SFTP enabled

Select file server Select file server

SAVE CANCEL

Schedule Properties

Enable Schedule

GENERAL TRIGGER

Daily  Weekly  Monthly

Start: 00:00:00

Between Specific Time 00:00:00 00:00:00

Runs at 00:00 every day. Generates report for the previous day.

SAVE CANCEL

## Voltage DAM Query Examples

### String Queries

PURPOSE	QUERY
To search log entries starts with given character or word:	a* companyname*
To search log entries ends with given character or word:	*a *companyname
To search log entries that contain the given keyword:	Companyname
To search for log entries using a wildcard character to represent a portion of the keyword:	companyn?me
To search for a keyword with corrected spelling by allowing up to 2 characters of error:	cmpnyname~
To search for log entries that contain the keyword "companyname" and either "productname" or "applicationname":	companyname AND (productname OR applicationname) Alternatively, you can use the OR operator directly without parentheses: companyname productname OR companyname applicationname
These queries will retrieve log entries that meet the specified conditions. The "AND" operator ensures that the keyword "companyname" must be present in the log entries, while the "OR" operator provides flexibility by allowing either "productname" or "applicationname" to be present.	

### Specific Field-Based Queries

PURPOSE	QUERY
To search a full text:	MachineName: "Companyname-PC" MachineName: 'Companyname-PC' MachineName: Companyname-PC
To search log entries starts with given character or word:	MachineName: Companyname* MachineName: a* c.
To search log entries ends with given character or word:	MachineName: *companyname b. MachineName: *a
To search for words with missing initial character(s), you can use the following examples:	MachineName: *companyname

<p>To perform searches with restrictions on different fields, you can use the following syntax:</p>	<p>Keywords: (critical OR error) AND EventSource: 'productname' EventSource: 'productname' AND (Keywords: 'critical' OR Keywords: 'error')</p>
<p>To search for a word with potential spelling mistakes and allow for a certain degree of error tolerance, you can use fuzzy search or approximate matching. In Voltage DAM, user can utilize the tilde (~) operator to perform fuzzy searches.</p>	<p>EventSource: producme~ (Correct spelling is productname) EventSource: productme~ EventSource: proutname~ EventSource: proutnae~</p>
<p>To perform searches with restrictions on a single field:</p>	<p>EventSource: 'productname OR OSname' EventSource: 'productname OSname' (Works in the same way with OR)</p>
<p>To perform a search using a specified range:</p>	<p>TimeCreated: '[Date to Date]' TimeCreated: '[* TO 2017-12-01]' (Returns all dates before the specified date)</p>
<p>Search with sorting</p>	<p>EventID: &gt;10 EventID: &gt;=10 EventID: &gt;= 500 AND EventID: &lt;=1000 EventID: [500 TO 1000]</p>

## Regular Expression Queries

### Regex String Queries

PURPOSE	QUERY
<p>To search for a constraint between two characters or words within a keyword, you can use regular expressions. Regular expressions allow for pattern matching and can help you specify constraints in your search query. Here are the examples you provided:</p>	<p><code>/(P p)ro(ductname file)/</code>                      This regular expression pattern will match the word "Pro" followed by either "ductname" or "file". The "(P p)" part allows for variations in the capitalization of the letter "P"</p> <p><code>/(p P)ro./</code>                      This regular expression pattern will match any word that starts with "pro" or "Pro" followed by any characters. The "(p P)" part allows for variations in the capitalization of the letter "P",</p>

	and the "." represents any number of characters after "pro" or "Pro"
To search log entries start with a given character or word:	/a.*/ /companyname.*/
To search log entries ends with a given character or word:	/.*a/ /.*companyname /
To search for a keyword using wildcard characters, you can use the following symbols:	/compa.../
To search for numerical ranges, you can use the following syntax:	/companyname/ /192.168.1./
To search for minimum or maximum repeating words	/a{2,4}/ /a{3}a{2}/ /companyname{3}/
To search for minimum or maximum occurrences of a keyword, you can use the following examples:	/c~e/ Words starting with 'c' and ending with 'e' /co~e/ Words starting with 'c', followed by 'o', and ending with 'e'

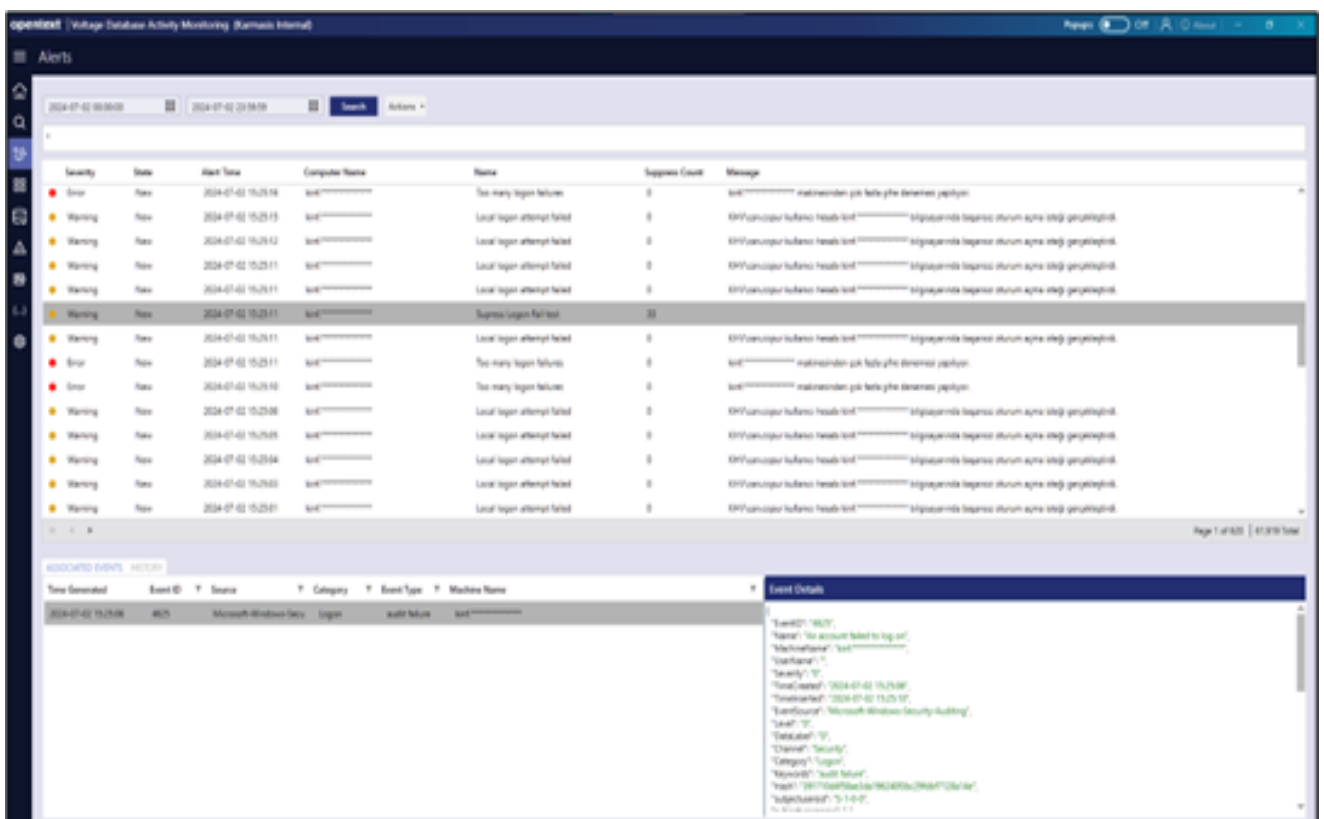
### Regexp Queries on Specific Fields

PURPOSE	QUERY
To search for a keyword with a limitation between two letters or words, you can use the following example:	EventSource: /(P p)ro(ductname file)/ /(p P)ro.*/
To search for records that start with a specific character or word, you can use the following examples:	MachineName: /a.*/ MachineName: /companyname.*/
To search for records that start with a specific character or word, you can use the following examples:	MachineName: /.*a/ MachineName: /.*companyname/
To search for any character occurring within a word, you can use wildcard characters. The most commonly used wildcard characters are:	EventSource: /Produ../
To search for numerical ranges, you can query for numbers within a specific range. You can use the following examples to specify a range:	EventID: // MachineName: /companyname/ (MachineName: /.*companyname/ - The reason for this is the ability to perform term-



	based searches without requiring any specific word or character except for the one following the asterisk.
To search for a specific number of characters within a word, you can use the following wildcard characters:	MachineName: /[a-z]{2,4}/
To search for a range of values within a specific field:	MachineName: /p~e/ Words starting with 'p' and ending with 'e' MachineName: /pr~e/ Words starting with 'p', followed by 'r', and ending with 'e'

## Alerts

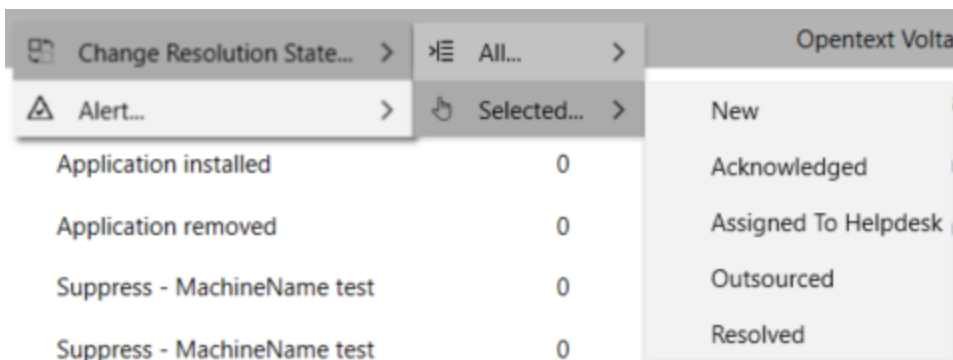


- **Severity** shows the event type.
- **State** shows the action status of the event.
- **Alert Time** shows the date and time of the event occurrence.
- **Computer Name** shows the machine name where the event occurred.

- **Name** shows the event description.
- **Suppress Count** shows the number of suppressed events.
- **Message** shows the description.

**NOTE:** Users can specify a time frame that blocks thousands of alerts and actions by suppressing them, improving system manageability.

When users right-click on the listed alarm records, users see following menus:

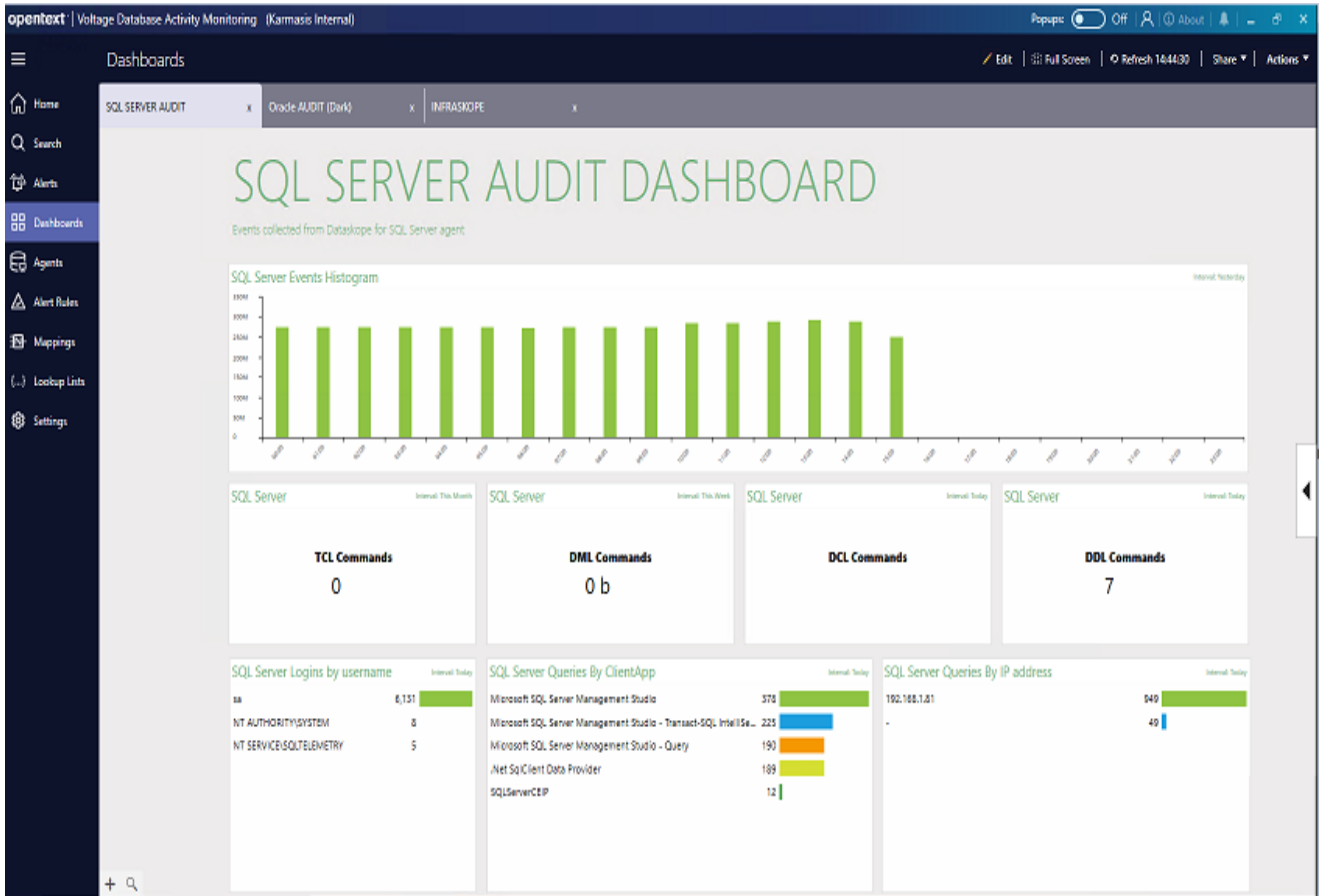


#### Change Resolution State Menu:

- **All:** Allows you to change the resolution state for all records.
  - **New:** Indicates a newly received alarm.
  - **Acknowledged:** Indicates that the alarm has been reviewed and acknowledged by the authorized person.
  - **Assigned to Helpdesk:** Indicates the assignment of the alarm to the helpdesk team.
  - **Outsourced:** Indicates the outsourcing of the alarm to external service providers.
  - **Resolved:** Indicates that action has been taken regarding the alarm and it has been resolved.
- **Alert:**
  - **Selected:** Allows you to change the alert state only for the selected records.
  - **Go to Related Alert:** Provides information about the alarm rule under which the record was generated.
  - **Disable:** Allows you to disable the alarm rule according to your preference.

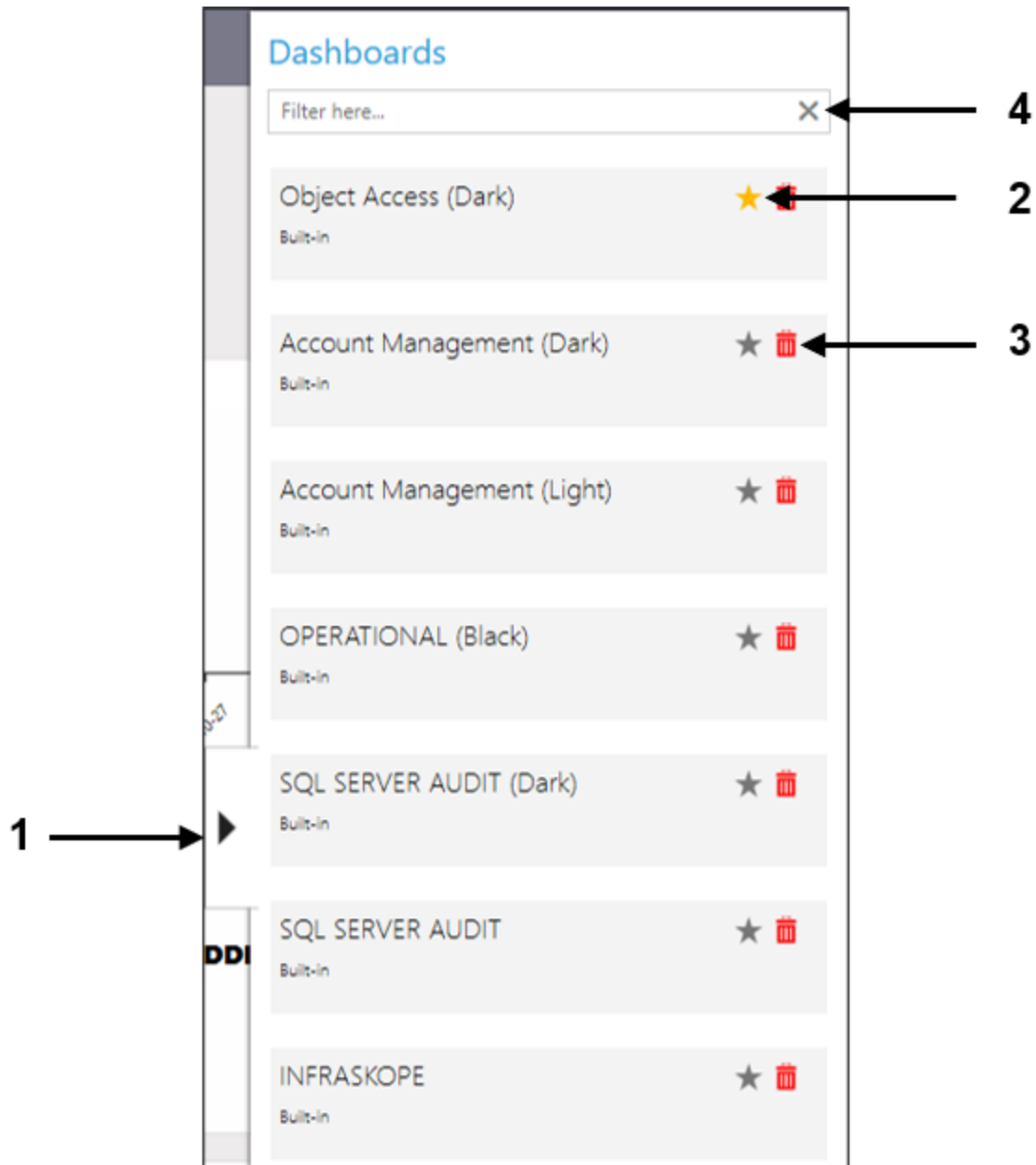
## Dashboard

Dashboard menu is used to visually monitor critical events that are important for organization without the need for any specific reports. It allows users to create a customized dashboard with graphical representations of the events.



### Sliding Dashboard Panel

To open the sliding panel and view all dashboard designs, click on arrow (1).



In the sliding panel, users can select their favourite dashboard designs and take them to the top by clicking **star** (2) icon.

When users want to delete one of the dashboard designs, they can click on the trash bin (3) icon.

If users want to find the dashboard design they want by typing its name instead of scrolling, they can use the **Filter here** (4) section.



Ref.	Controls	Function
1	Edit	Used to edit the dashboard.
2	Full Screen	Used to display the dashboard full screen.
3	Refresh	Used to refresh the dashboard.
4	Share	Used to share the dashboard with internal users.
5	Actions	Used to reach various actions related to the dashboard. Includes <b>Edit</b> , <b>Delete</b> , <b>Bookmark</b> , <b>Rename</b> , <b>New Dashboard [Blank Dashboard, Copy From Existing]</b> , <b>Import</b> and <b>Export</b> .

## Edit Dashboard

When the **Edit** mode is enabled, 4 new tabs appear at the top as **File**, **Design**, **Themes** and **Options**.

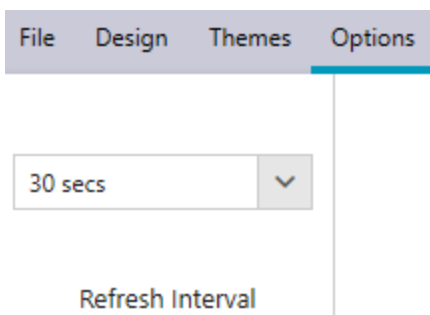
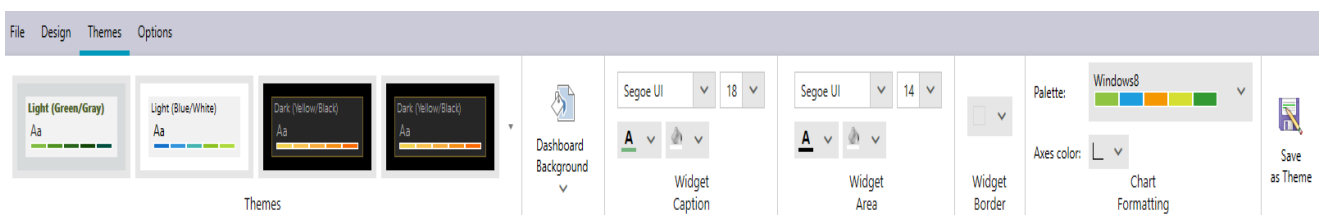
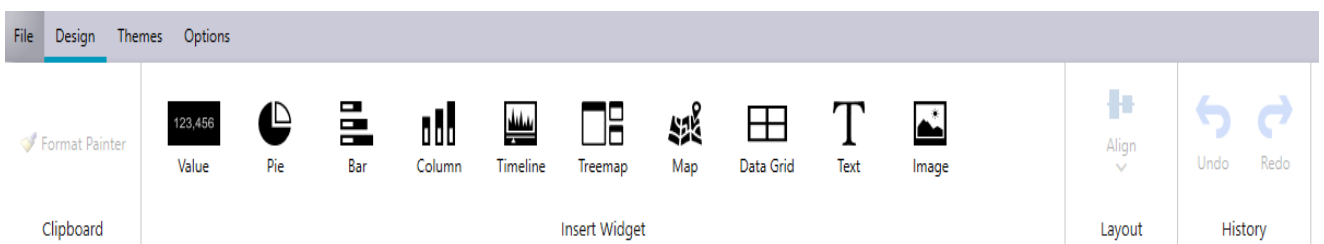
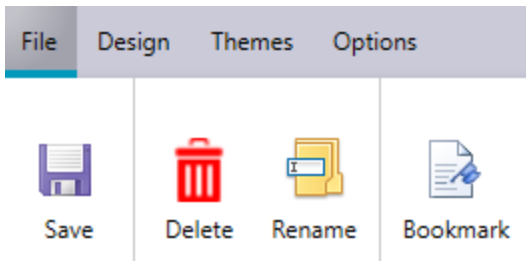
The **File** tab is used for **Save**, **Delete**, **Rename** and **Bookmark** operations.

The **Design** tab is used for **Format Painter**, **Insert Widgets (Value, Pie, Bar, Column, Timeline, Treemap, Map, Data Grid, Text, Image)**, **Align**, **Undo** and **Redo** operations.

The **Themes** tab offers various **Theme Designs**. It also provides separate customization opportunities for **Background, Widget Caption, Widget Area, Widget Border** and **Chart Formatting**.

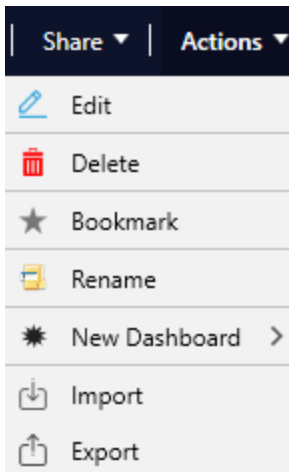
The **Options** tab allows user to change the **Refresh Interval** value.

After the editing process is completed, the user saves the changes using the **Save** button on the top left. If users want to close the changes without saving, they use the **Cancel** button.





## Actions



- **Edit:** Used to edit the dashboard.
- **Delete:** Used to delete the dashboard.
- **Bookmark:** Used to take the dashboard to the top in the sliding dashboard panel. Its function is the same as to star in a sliding dashboard panel.
- **Rename:** Used to rename the dashboard.
- **New Dashboard [Blank Dashboard, Copy From Existing]:** Used to add new dashboard from blank one or copy from existing.
- **Import:** Used to import a design template that previously exported from another machine using the saved file.
- **Export:** Used to export the dashboard design.

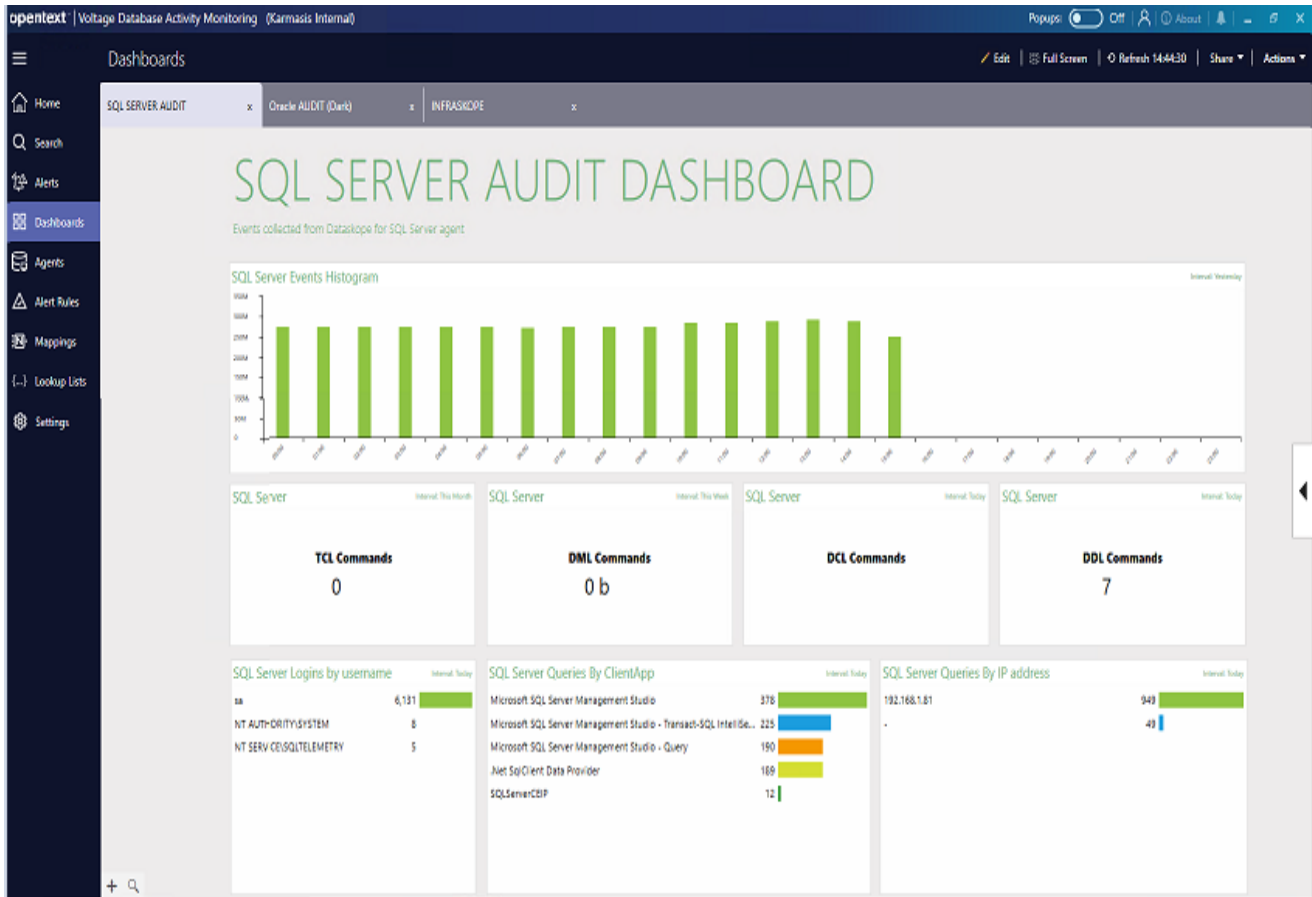
## Creating a New Dashboard

Users can create a new dashboard according to their needs and track all activities through charts in real time.

To create a new dashboard, click **Actions > New Dashboard > Blank Dashboard**.

1. In the New Dashboard window, enter the Dashboard name and description.
2. Choose a theme for the new dashboard and press the OK button.





New Dashboard ✕

Please provide a new name for the new dashboard:

Description for the new dashboard:

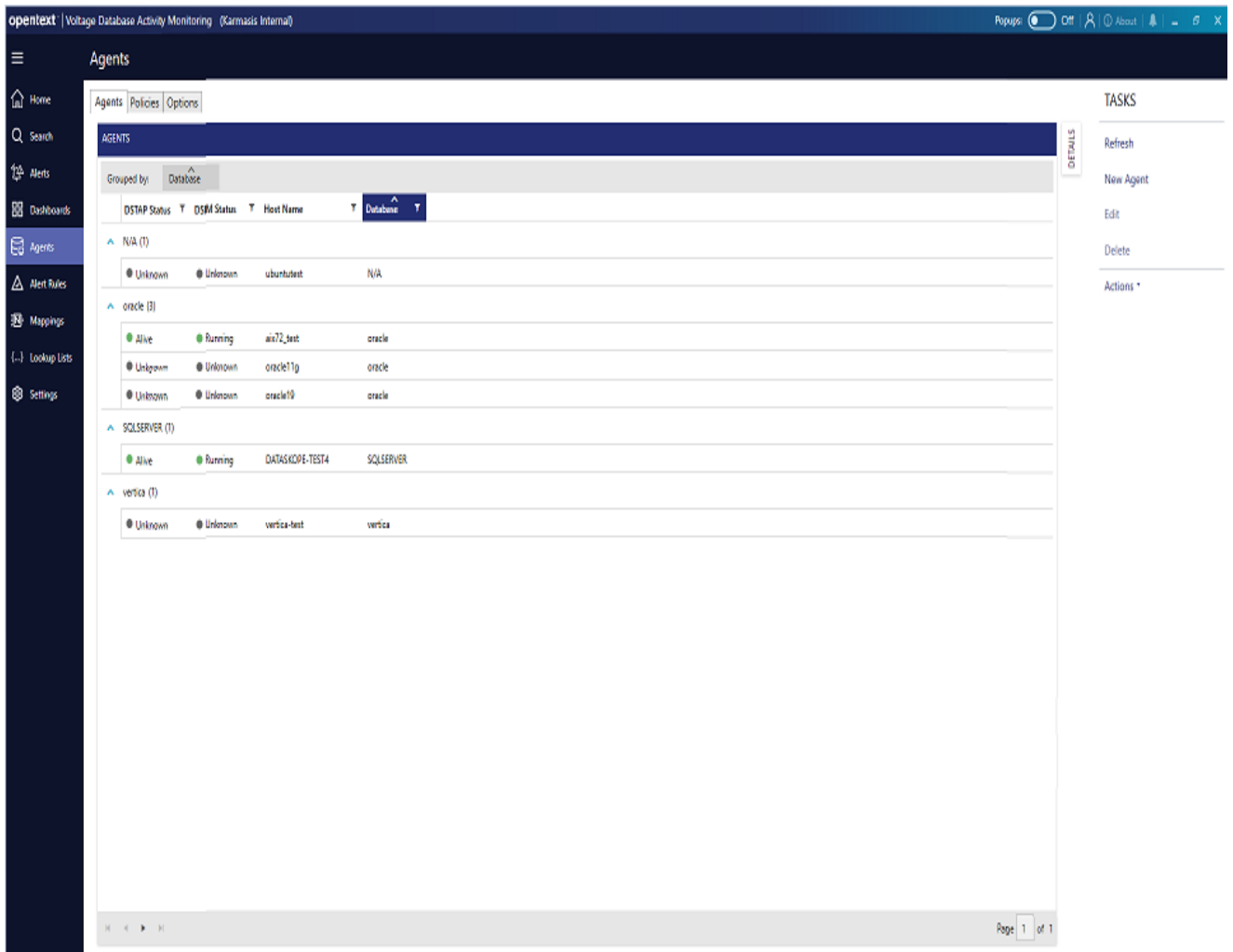
Select a theme for the new dashboard:

<b>Light (Green/Gray)</b> Aa 	<b>Light (Blue/White)</b> Aa 	<b>Dark (Yellow/Black)</b> Aa 	<b>Dark (Yellow/Black)</b> Aa 
<b>Dark (Khaki/Gray)</b> Aa 	<b>Dark (Khaki/Gray)</b> Aa 	<b>Dark (Green/Black)</b> Aa 	<b>Dark (Green/Black)</b> Aa 

## Agents

Agents Menu allows you to manage, monitor, and configure your agents. It consists of panels where users can define and modify settings for the agents installed on client machines With **Agents**, **Policies**, and **Options** tabs.

- Add, delete, and edit agents through this interface.
- Modify agent policies and update certificates.
- Oversee a detailed monitoring process and read agent metrics with the Real-time Diagnostics tool.
- Instantly intervene when the status of online agents changes.
- Observe agent updates and access information about machines.
- Group your agents for monitoring purposes with the categorization feature.



### Adding a New Agent

1. To add a new agent, click on **New Agent** button.
2. In the opened **New Agents Wizard** window, enter the **IP Address** of the machine where the agent is installed, and choose the appropriate **Protocol**. If necessary, you can use the sub-panel to upload certificates.
3. Click **Next**.

The screenshot shows the 'New Agent Wizard' window with the 'Connection' step active. The window title is 'New Agent Wizard' with a close button. The main heading is 'Connection'. Below the heading, there is a prompt: 'Enter the connection information to connect to the agent'. The 'IP Address' field contains '192.168.1.74' and the port field contains '8765'. The 'Protocol' dropdown menu is set to 'TLS 1.2'. Below this is a 'Certificate' sub-panel with three radio button options: 'Use old default certificate', 'Use new default certificate' (which is selected), and 'Upload certificate'. Under 'Upload certificate', there are two more radio button options: 'Use old certificate' and 'Use new certificate'. Below these are two input fields: 'Client Certificate:' with a 'Browse' button, and 'Password:'. At the bottom right of the wizard, there are 'CANCEL' and 'NEXT >' buttons.

4. In **Listener Settings** window, select which databases to collect logs from.
5. If needed, choose and modify additional settings such as time, port, trace, network, size, memory, SSL, and more.

New Agent Wizard ×

## Listener Settings

Select the databases you want to collect logs

pcap.devices	<input type="text" value="*"/>
oracle.enabled	<input checked="" type="checkbox"/>
oracle.server_port	<input type="text" value="1521"/>
mysql.enabled	<input type="checkbox"/>
mysql.server_port	<input type="text" value="3306"/>
postgre.enabled	<input type="checkbox"/>
postgre.server_port	<input type="text" value="5432"/>
mssql.enabled	<input type="checkbox"/>
mssql.server_port	<input type="text" value="1433"/>

6. **msg.file.max\_age** value is 10 as default, set this value to 1.
7. Click **Next**.

New Agent Wizard

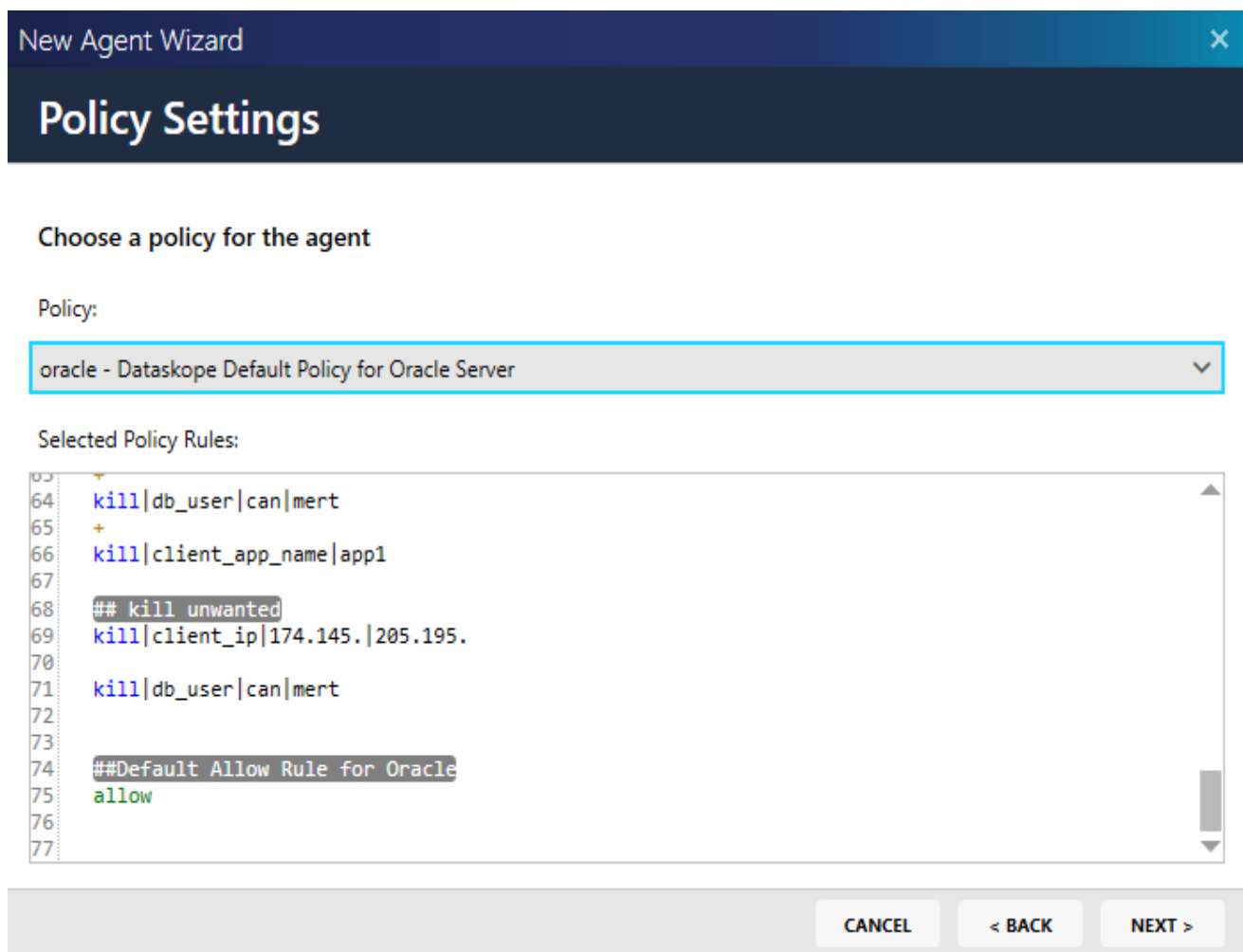
## Listener Settings

Select the databases you want to collect logs

elastic.enabled	<input type="checkbox"/>
elastic.server_port	9200
netezza.enabled	<input type="checkbox"/>
netezza.server_port	5480
gauss.enabled	<input type="checkbox"/>
gauss.server_port	1888
sybase.enabled	<input type="checkbox"/>
sybase.server_port	5000
msg.file.max_age	1

CANCEL < BACK NEXT >

8. In **Policy Settings** window, set the agent policy according to your drop rules or perform your operations with the default policy.
9. Click **Next**.



10. Check the collector settings.
11. If everything is OK, click **Finish**.

When clicked on Finish button, agent is created.

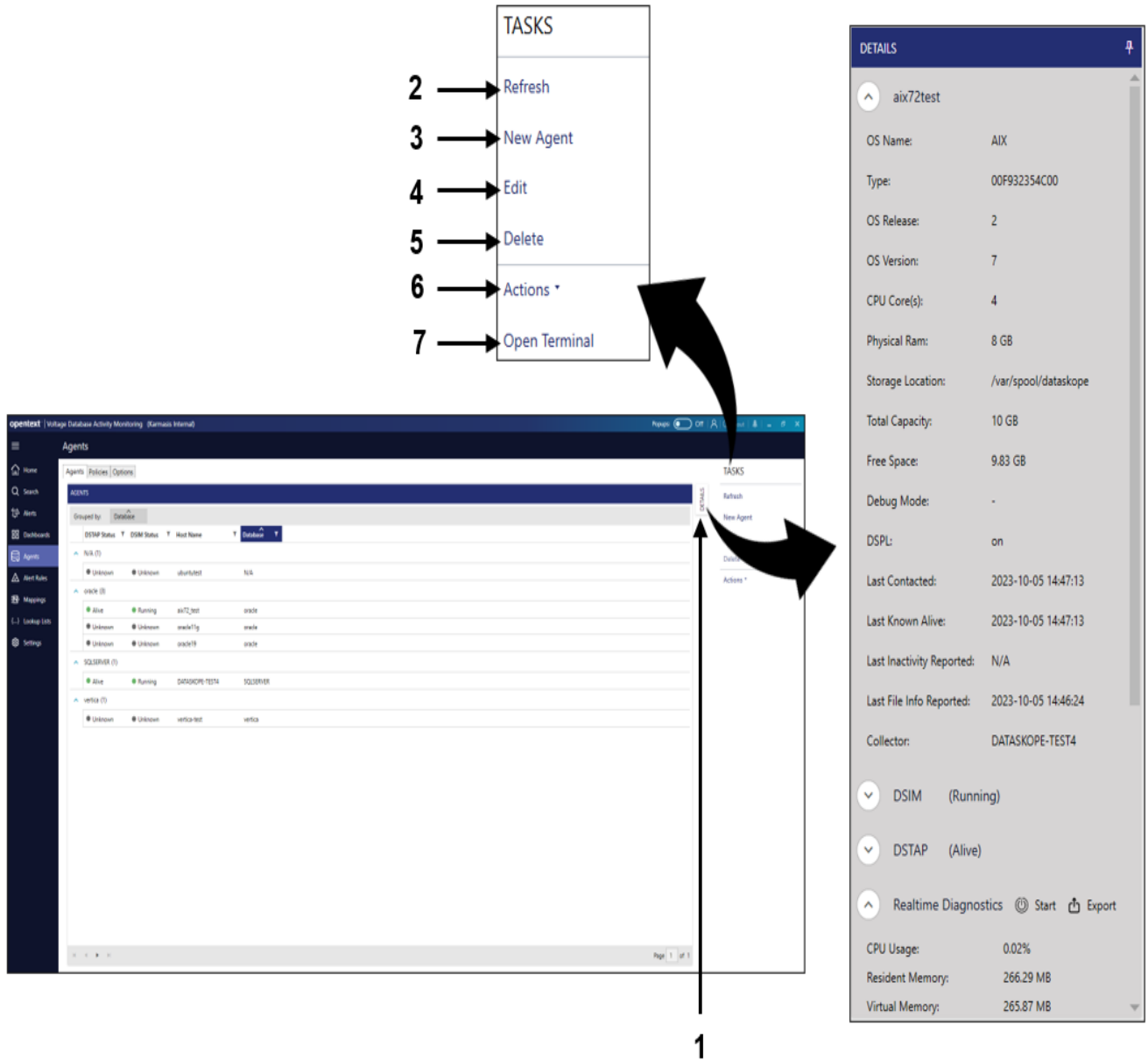
New Agent Wizard ✕

## Collector Settings

Enter settings and create new agent

Cluster Name:	Suppress Inactivity Event Minutes:
<input type="text" value="New cluster name"/>	<input type="text" value="60"/>
Max Idle Minutes:	Idle Threshold Minutes:
<input type="text" value="10"/>	<input type="text" value="10"/>
Suppress File Info Event Minutes:	Suppress Status Event Minutes:
<input type="text" value="1"/>	<input type="text" value="60"/>
Tag	
<input type="text" value="Type a tag"/>	

## Agents Tab



Ref.	Controls	Function
1	DETAILS	Used to reach details of the selected agent. Real-time Diagnostics tool available here allows user to view the agent's activities and performance in real-time.
2	Refresh	Used to refresh the agents tab.
3	New Agent	Used to add new agent. For more details, see <b>Adding a New Agent</b> .



4	Edit	Used to edit the selected agent.
5	Delete	Used to delete the selected agent.
6	Actions	Used to reach various actions related to the agents. Includes Export and Send as Email.
7	Open Terminal	Used to open terminal.

## Policies

The screenshot shows the 'Agents' page in the VAM interface. A list of agents is displayed with columns for Name, Database, and Description. On the right side, there is a 'TASKS' menu with four buttons: Refresh, New Policy, Edit, and Delete. Arrows numbered 1 through 4 point to these buttons respectively.

Ref.	Controls	Functions
1	Refresh	Used to refresh the policy tab.
2	New Policy	Used to add new policy.
3	Edit	Used to edit the selected policy.
4	Delete	Used to delete the selected policy.

### New Policy

To create a new policy, click the **New Policy** button on Agents-Policy tab and follow the steps given below.

1. Enter the **Policy Name**.
2. Select **Database**.
3. Add a **Description** if necessary.
4. Add **Rules**. It can be tested with the **Test Rule** option.
5. Click the **Save** button to save the created policy.

The screenshot shows a 'New Policy' dialog box with the following elements:

- Title Bar:** 'New Policy' with minimize, maximize, and close buttons.
- Name \*:** A text input field with a red border.
- Database \*:** A dropdown menu with the text 'Select database type' and a downward arrow.
- Description:** A text input field.
- Rules:** A large text area containing the number '1'.
- Buttons:** 'TEST RULE', 'IMPORT', 'SAVE', and 'CANCEL' buttons at the bottom.

## Options

The default certificate details can be changed via the Options tab. The upper part of the screen is used for agents older than version 3.2.0.4084, and the lower part of the screen is used for agents of

version 3.2.0.4084 and higher.

## Agents

Agents Policies Options

### Default Certificate

Used for agents older than version 3.2.0.4084

Certificate \*

dsim\_client.pfx file selected. Remove

Password \*

.....

SAVE CANCEL

Used for agents of version 3.2.0.4084 and higher

Certificate \*

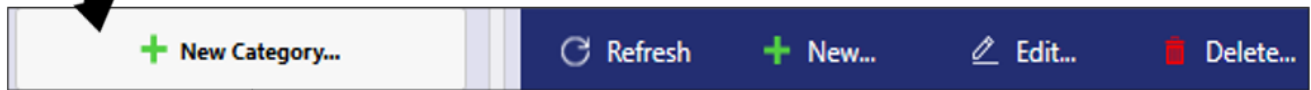
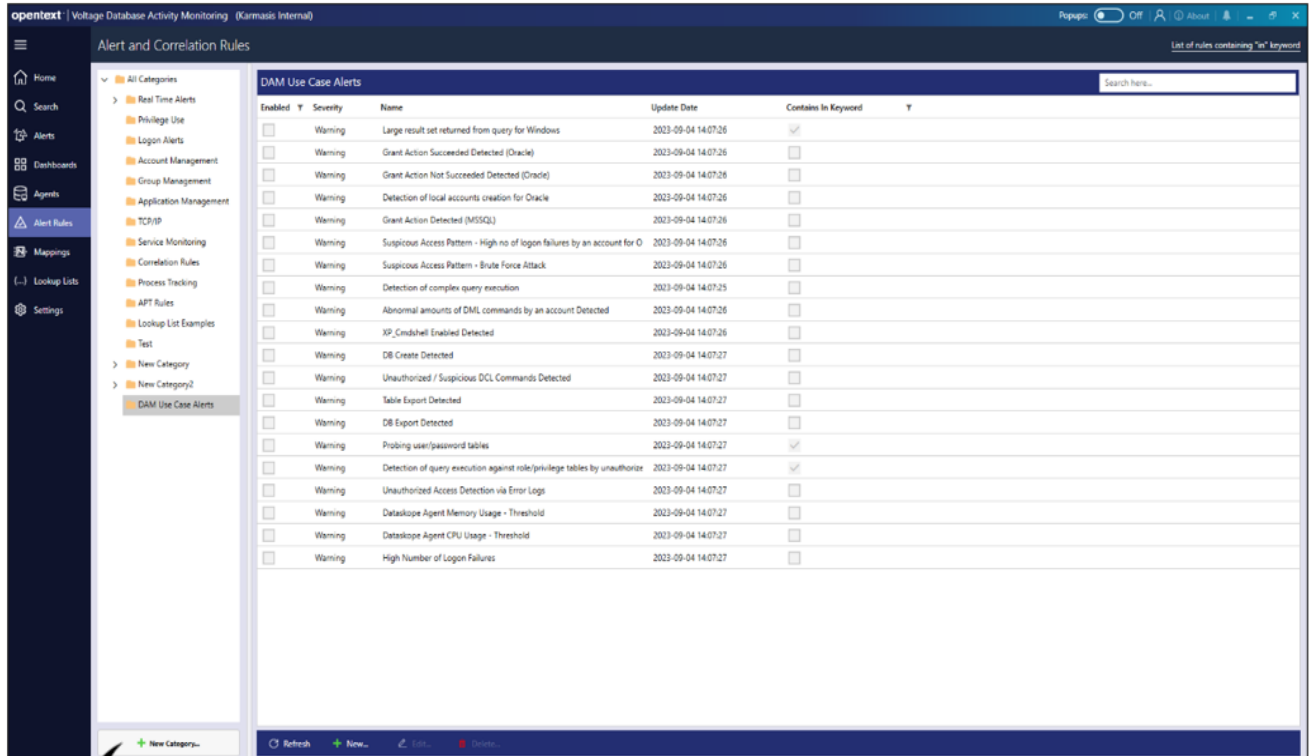
dsim\_client.pfx file selected. Remove

Password \*

.....

SAVE CANCEL

## Alert Rules



- 1
- 2
- 3
- 4
- 5

Ref.	Controls	Function
1	New Category	Used to add new category about alert rules.
2	Refresh	Used to refresh alert rules.
3	New	Used to add new alert rule.
4	Edit	Used to edit the alert rule.
5	Delete	Used to delete the alert rule.

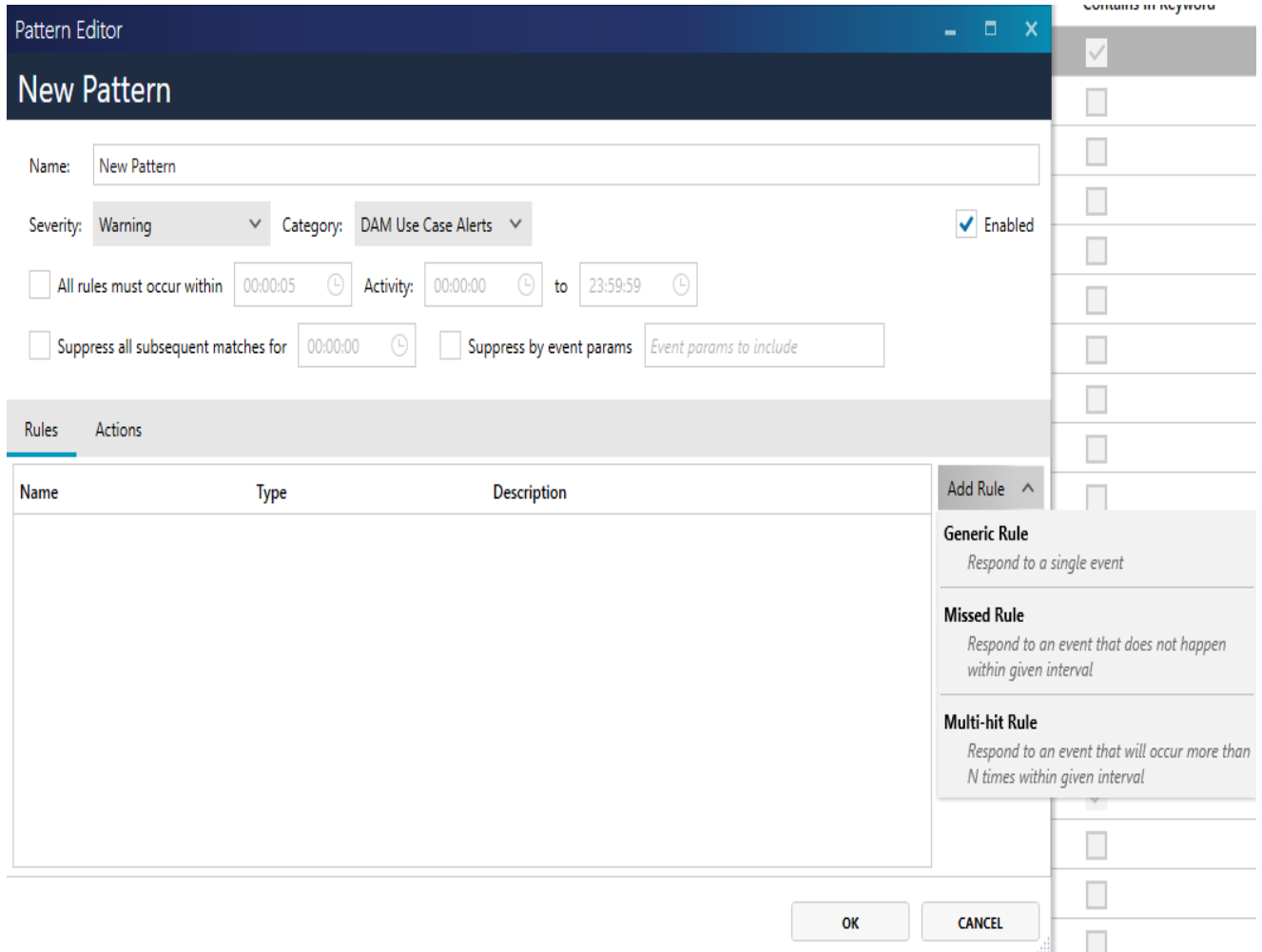
### Column Details

- **Enabled** shows the enabled or disabled status.
- **Severity** shows the type of the alert.
- **Name** shows the alert name/description.
- **Update Date** shows the date and time of the alert.
- **Contains in Keyword** shows whether it contains the specific keyword or not.

### Adding New Alert Rule

To add a new alert rule, click the **New** button on **Alert Rules** menu and follow the steps given below.

1. Enter the **Pattern Name** in the opened **Pattern Editor**.
2. Select the **Severity** and **Category** options.
3. Select and fill the other pattern options related with time, matching and parameters if necessary.
4. Click **Add Rule** button and select the **Alert Rule Type** [**Generic Rule**, **Missed Rule**, **Multi-hit Rule**].
5. Follow the steps for selected **Alert Rule Type**.
6. Click the **OK** button to add the created alert rule.



### Generic Rule

Generic Rule type is used to respond to a single event. User must enter the **Name**, **Criteria**, **Correlation Key**, and **Description** fields to add a generic alert rule in **Rule Editor** window. Users can see **Criteria Helper** by clicking ? button.

Rule Editor \_ □ ×

## New Rule

Name:

Criteria:  ?

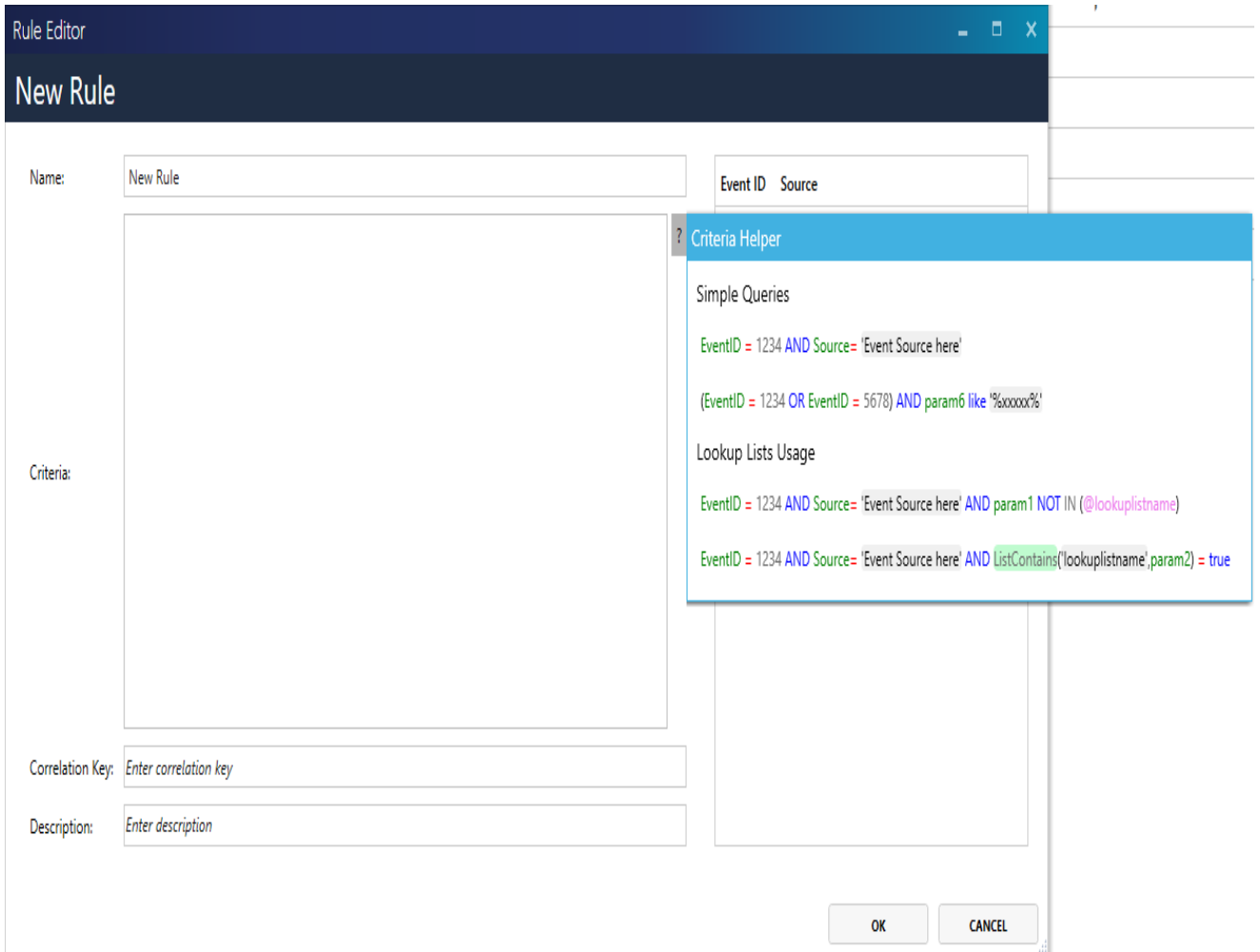
Correlation Key:

Description:

Event ID	Source

Parameter	Name



### Missed Rule

Missed Rule type is used to respond to an event that does not happen within given interval. User must enter the **Name**, **Criteria**, **Correlation Key**, **Description**, **From**, **To** and **Interval** fields to add a missed alert rule in **Rule Editor** window.



The screenshot shows a window titled "Rule Editor" with a subtitle "New Missed Rule". The form contains the following fields and components:

- Name:** A text box containing "New Missed Rule".
- Criteria:** A large empty text area with a question mark icon to its right.
- Correlation Key:** A text box containing the placeholder text "Enter correlation key".
- Description:** A text box containing the placeholder text "Enter description".
- From:** A time selection box with "00:00:00" and a clock icon.
- To:** A time selection box with "00:00:00" and a clock icon.
- Interval:** A time selection box with "00:01:00" and a clock icon.
- Event ID Source Table:** A table with two columns: "Event ID" and "Source". It is currently empty.
- Parameter Name Table:** A table with two columns: "Parameter" and "Name". It is currently empty.
- Buttons:** "OK" and "CANCEL" buttons are located at the bottom right of the window.

### Multi-hit Rule

Multi-hit Rule type is used to respond to an event that will occur more than N times within given interval. User must enter the **Name**, **Criteria**, **Correlation Key**, **Description**, **Group By Key**, **Interval**, and **Match Condition** fields to add a multi-hit alert rule in **Rule Editor** window.

Rule Editor

## New Multi-hit Rule

Name:

Criteria:  ?

Event ID	Source
----------	--------

Parameter	Name
-----------	------

Correlation Key:

Description:

Group By Key:

Interval:  ⌚

Match Condition:



1	New Category	Used to add new category about mappings.
2	Refresh	Used to refresh mappings.
3	New	Used to add new mapping.
4	Edit	Used to edit the mapping.
5	Delete	Used to delete the mapping.

### Column Details

- **Enabled** shows the enabled or disabled status.
- **Name** shows the mapping name.
- **Description** shows the mapping description.
- **Event Source** shows the event source about mappings.
- **Event ID** shows the event ID about mappings.
- **Event Type** shows the event type about mappings.

### Add New Mappings

To add a new mapping, click New from the **Mapping** menu.

1. Enter **Mapping Name**.
2. Enter **Description**.
3. Fill in the **Criteria**, **Events Source** and **Event Type** sections.

4. Complete the **Input**, **Code** and **Output** sections as appropriate.

⌵ ⌵ ✕

Name:

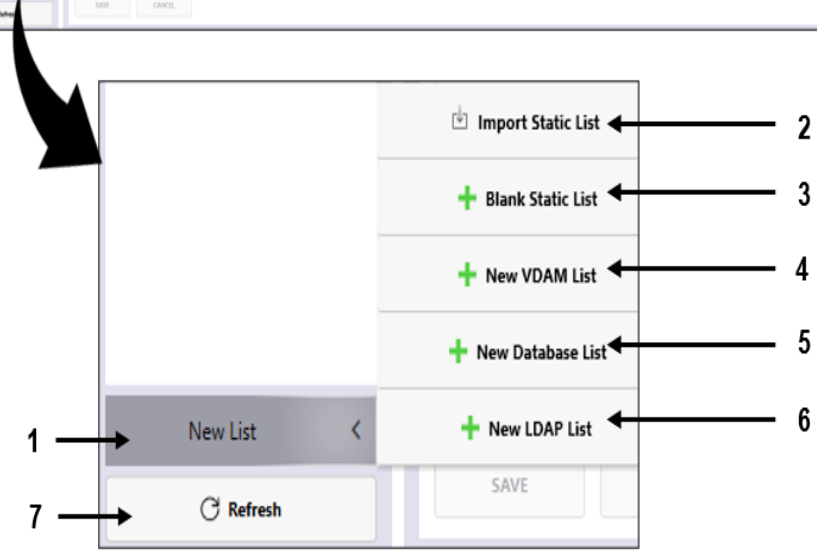
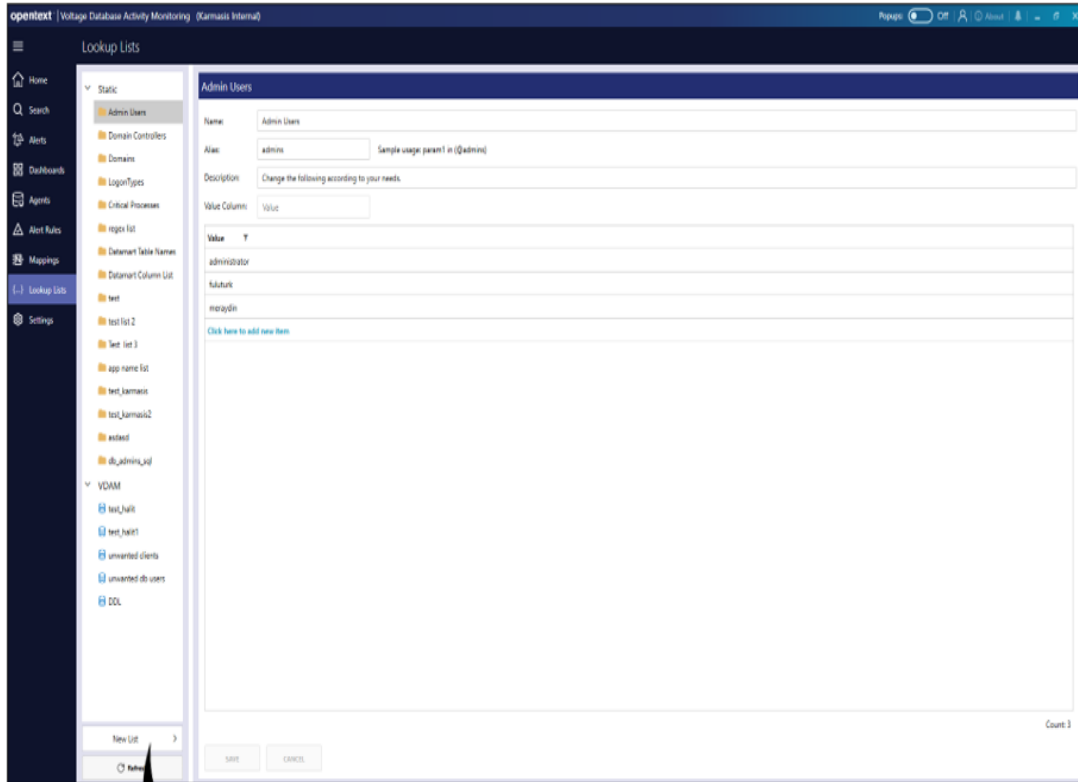
Description:

Criteria:    ⌵

Input <span>⌵</span>	Code <span>▶</span>	Output <span>⌵</span>
	1	

Enabled

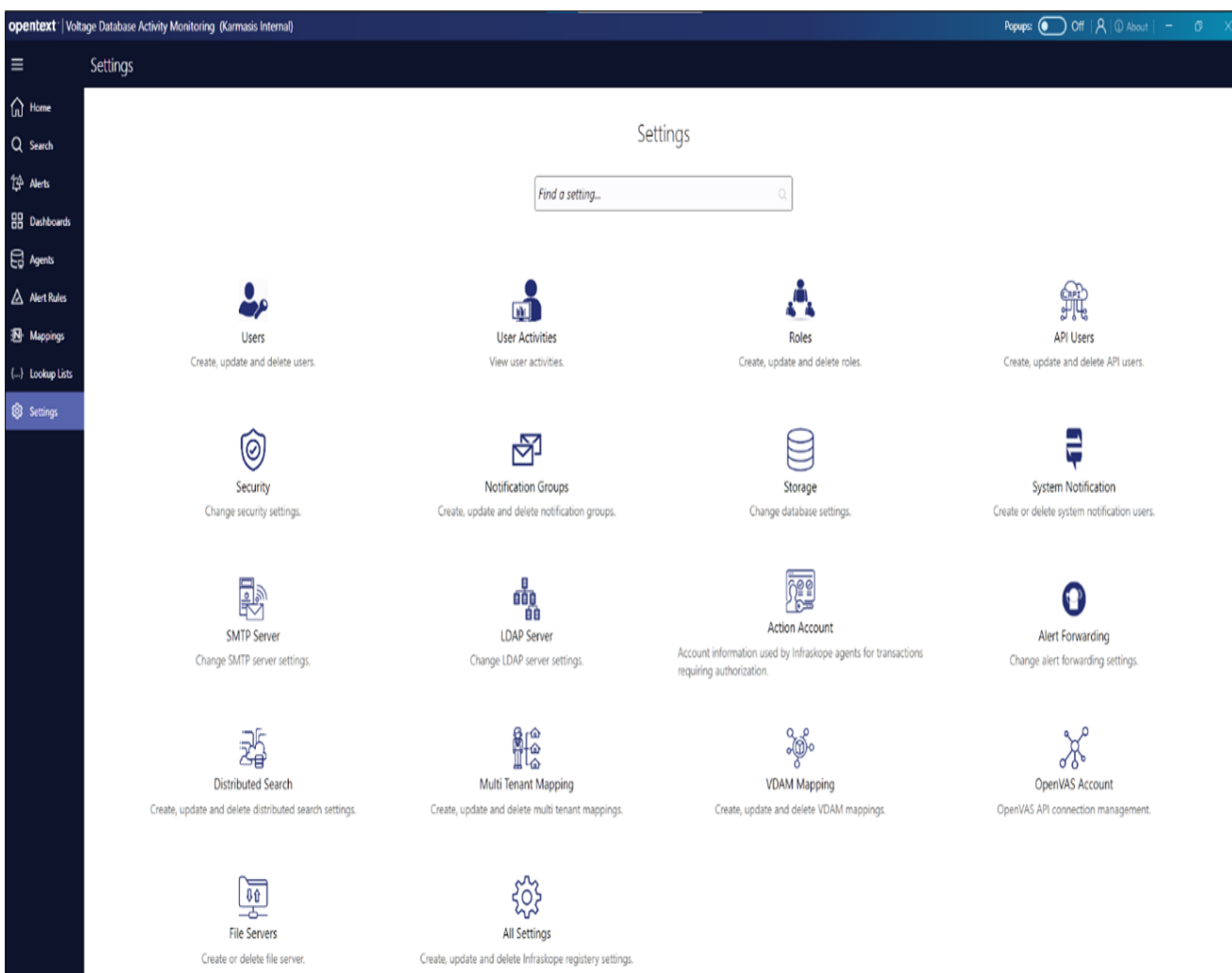
## Lookup Lists





















Ref.	Controls	Functions
1	New List	Used to add new category about mappings.
2	Import Static List	Used to import a list from an external source.

3	Blank Static List	Used to start creating a list from scratch.
4	New VDAM List	Used to specially formatted list for VDAM.
5	New Database List	Used to allow querying the database and speed up search operations.
6	New LDAP List	Used to specially formatted list for LDAP.
7	Refresh	Used to refresh Lookup Lists.

## Settings



Ref.	Controls	Function
	Users	Used to create, update, and delete users.

	User Activities	Used to view user activities.
	Roles	Used to create, update, and delete roles.
	API Users	Used to create, update, and delete API Users.
	Security	Used to change security settings.
	Notification Groups	Used to create, update, and delete notification groups.
	Storage	Used to change database settings.
	System Notification	Used to create and delete system notification users.
	SMTP Server	Used to change SMTP server settings.
	LDAP Server	Used to change LDAP server settings.
	Action Account	Used to reach account information by Voltage DAM agents.
	Alert Forwarding	Used to change alert forwarding settings.
	Distributed Platform	Used to create, update, and delete distributed platform settings.
	Multi-Tenant Mapping	Used to create, update, and delete multi-tenant mappings.
	VDAM Mapping	Used to create, update and delete VDAM Mappings
	OpenVAS Account	Used to OpenVAS API connection management.
	File Servers	Used to create or delete file server.
	All Settings	Used to create, update, and delete Voltage DAM registry settings.

## User Settings

This setting is used to show the existing users and allows to perform editing, deletion, and addition operations.



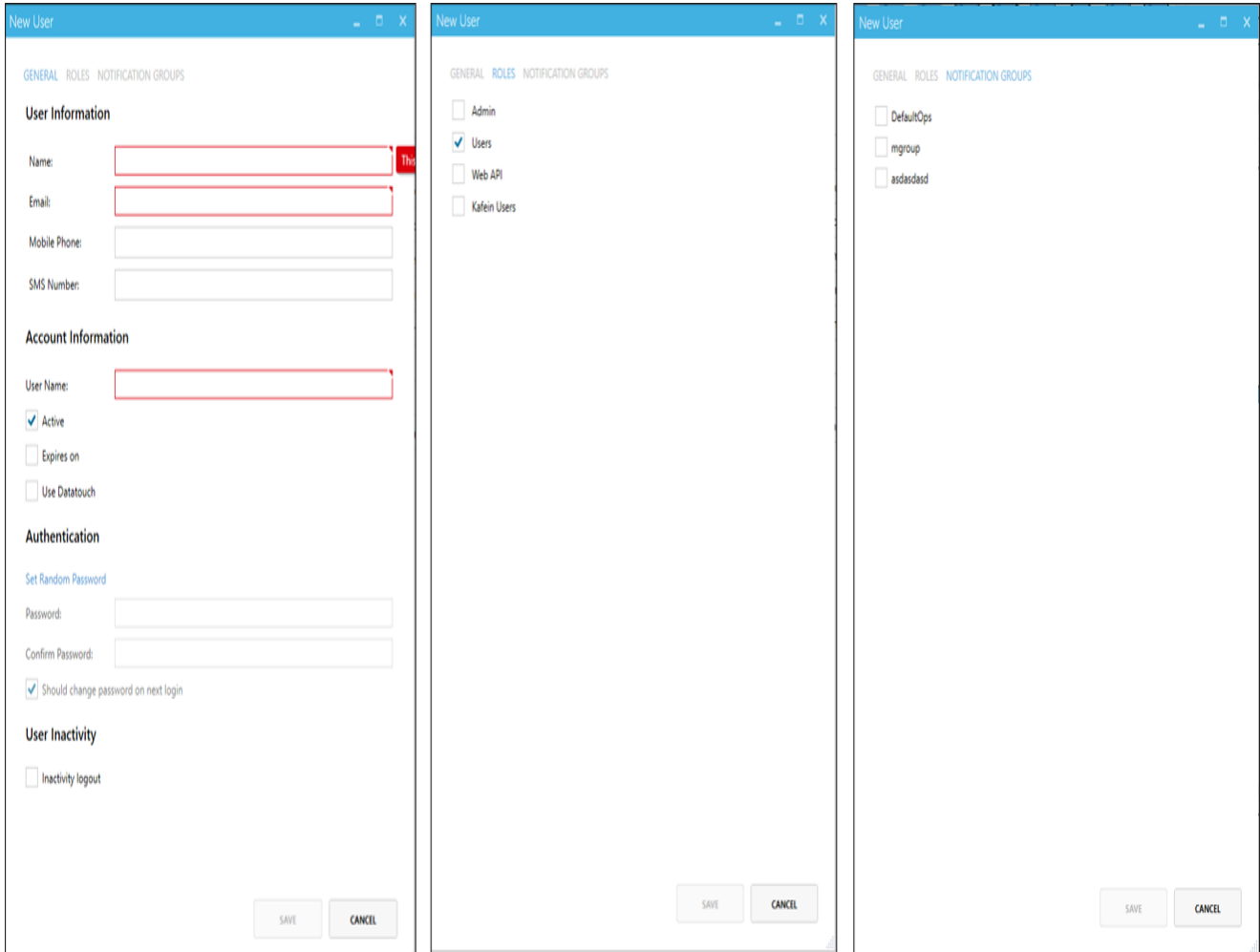
## Users

 Refresh  New...  Edit...  Delete...

Login Enabled	Name	User Name	Roles	Email	Last Password Change Time	Last Login Time
<input checked="" type="checkbox"/>	Log Admin	logadmin	Admin	halit.dursun@karmasis.com	-	2023-10-04 14:40:15
<input checked="" type="checkbox"/>	Can Çopur	cancopur	Admin	bedircancopur@gmail.com	2023-03-15 18:03:57	-
<input checked="" type="checkbox"/>	user1	user1	Admin	can.copur@karmasis.com	2023-08-18 15:06:14	-
<input checked="" type="checkbox"/>	Anıl Çelebi	anil.celebi	Kafein Users	anil.celebi@kafein.com.tr	2023-08-07 16:17:55	2023-08-11 16:00:26
<input checked="" type="checkbox"/>	Büşra Küçük	busrakucuk	Kafein Users	busra.kucuk@kafein.com.tr	2023-08-15 11:11:50	2023-10-04 14:20:26
<input checked="" type="checkbox"/>	cadasdas	can1-can@karma1-1.com	Users	canasdas@gmail.com	-	-
<input checked="" type="checkbox"/>	data touch user1	datatouch1	Users	adas@gasdas.com	2023-08-31 00:00:00	-
<input checked="" type="checkbox"/>	can kargı	cankargı	Admin	can.kargı@karmasis.com.tr	2023-09-01 00:00:00	-

### Adding New User

Adding a new user and updating login information can be done by clicking on the **New** button.



## User Activities Settings

This setting is used to show user activities and allows to export the actions of permitted users in JSON format within specific date ranges.

## User Activities

2023-10-04 00:00:00 2023-10-04 23:59:59 

V DAM Usage Logs
  V DAM API Usage Logs
 Search
Actions ▾
Preferences

Drag a column header and drop it here to group by that column							ACTIVITY DETAILS
Time Generated	Computer Name	OS User Name	IP Address	Operator	Module	Action	
2023-10-04 15:09:00	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	User Activities	GetSessionLogs2	<pre>{   "Service": "User Activities",   "Action": "GetSessionLogs2",   "Method": "POST",   "Record": {     "StartDate": "2023-10-04T00:00:00",     "EndDate": "2023-10-04T23:59:59",     "SearchText": null,     "LogType": 0   } }</pre>
2023-10-04 15:08:55	DATASKOPE-TEST4	Administrator	127.0.0.1	Log Admin	ElasticFunctions	Alerts	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:41	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:40	DATASKOPE-TEST4	Administrator	127.0.0.1	Log Admin	ElasticFunctions	Alerts	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:35	DATASKOPE-TEST4	can.kargi	192.168.1.81	Log Admin	ElasticFunctions	Search	
2023-10-04 15:08:30	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	ElasticFunctions	Search	
2023-10-04 15:08:30	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	ElasticFunctions	Search	
2023-10-04 15:08:30	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	ElasticFunctions	Search	
2023-10-04 15:08:30	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	ElasticFunctions	Search	
2023-10-04 15:08:30	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	ElasticFunctions	Search	
2023-10-04 15:08:30	KFNDDT003	busra.kucuk	192.168.1.99	Büşra Küçük	ElasticFunctions	Search	
2023-10-04 15:08:25	DATASKOPE-TEST4	Administrator	127.0.0.1	Log Admin	ElasticFunctions	Alerts	

Session ID: **2b8ec3c2-cb66-4bc6-92cd-17b81d406001** [Minimize](#)

Computer Name: **KFNDDT003** OS User Name: **busra.kucuk**

IP Address: **192.168.1.99** Operator: **Büşra Küçük**





Service: **User Activities** Action: **GetSessionLogs2**

Page 1 of 51

## Roles Settings

This setting is used to separate roles on the system according to their permissions. Users can add new roles, edit existing roles, or delete roles.

# Roles

 Refresh  New...  Edit...  Delete...

Default	Outside Connection	Role Name	Description
<input type="checkbox"/>	<input type="checkbox"/>	Admin	This role has access to all features.
<input type="checkbox"/>	<input type="checkbox"/>	Kafein Users	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Users	Read only user with full logs access.
<input type="checkbox"/>	<input type="checkbox"/>	Web API	Used for connections outside the Infraskope

## Adding a New Role

This is used to customize the access scope as desired when adding a new role.

To add a New role, click New button on the **Roles Settings**.

1. Enter the **Role Name**.
2. Enter the **Description**.
3. Check **Assign to new users as default** if necessary.
4. In **UI ACCESS**, turn **On** the actions that users of this role want to be authorized for.










### New Role

Name:

Description:

Assign to new users as default

[UI ACCESS](#) [CLASSIFICATION CRITERIA](#) [MEMBERS](#)

 Home	Displays database status and overall system information.	<input type="checkbox"/> Off
 Search	Search logs, create, update and delete queries.	<input type="checkbox"/> Off
 Alerts	You can view and export alarms.	<input type="checkbox"/> Off
 Dashboards	Dashboards that are created by users with log types of their choice that displays strategical information of their system. Users can also view built-in dashboards published by OpenText.	<input type="checkbox"/> Off
 Agents	Agents management.	<input type="checkbox"/> Off
 Alert Rules	Built-in alert rules published by OpenText and custom alert rules that are defined by users.	<input type="checkbox"/> Off
 Mappings	Create, update and delete event mappings.	<input type="checkbox"/> Off
 Lookup Lists	Built-in look-up lists published by OpenText and custom look-up lists that are defined by users.	<input type="checkbox"/> Off
 Settings	System settings.	<input type="checkbox"/> Off

5. In **CLASSIFICATION CRITERIA**, check **Activate Classification** if necessary.
6. Select **Field Queries** or **Raw Query String** and complete the relevant details.

New Role

Name:

Description:

Assign to new users as default

[UI ACCESS](#) [CLASSIFICATION CRITERIA](#) [MEMBERS](#)

Activate Classification

Field Queries

Must Filters

Must NOT Filters

Raw Query String

Company Name:

7. In **MEMBERS**, select the users you want to have in this role. Then, click **Save**.

### New Role

Name:

Description:

Assign to new users as default

[UI ACCESS](#) [CLASSIFICATION CRITERIA](#) [MEMBERS](#)

- Anil Çelebi
- Büğra Küçük
- cadasdad
- Can Çopur
- can kargı
- data touch user1
- Log Admin
- user1

## API Users Settings

This setting is used to define, delete, and edit API users.

## API Users

Refresh New... Edit... Delete...

Active	User Name	Name
<input checked="" type="checkbox"/>	test1	test

### Adding a New API User Guide

1. Enter Name, User Name and Password fields.
2. For active users, click on the Active checkbox.
3. For expired users, click on Expires on checkbox and select the date.

The screenshot shows a 'New User' dialog box with the following fields and options:

- Account Information:**
  - Name: [Text Input Field]
  - User Name: [Text Input Field]
  - Active
  - Expires on
- Authentication:**
  - Password: [Text Input Field] (with visibility and copy icons)

Buttons: SAVE, CANCEL

### Security Settings

This setting is used to perform users' current password settings and they can also set the duration for periodic password changes.



# Security

## Password Complexity

- Use default settings
- Require digit
- Require lowercase
- Require non alphanumeric
- Require uppercase

Required length

## Password Change

- Set password change interval for all users

Interval (as months)

## Notification Group Settings

This setting is used to to determine the groups to which notifications will be sent.

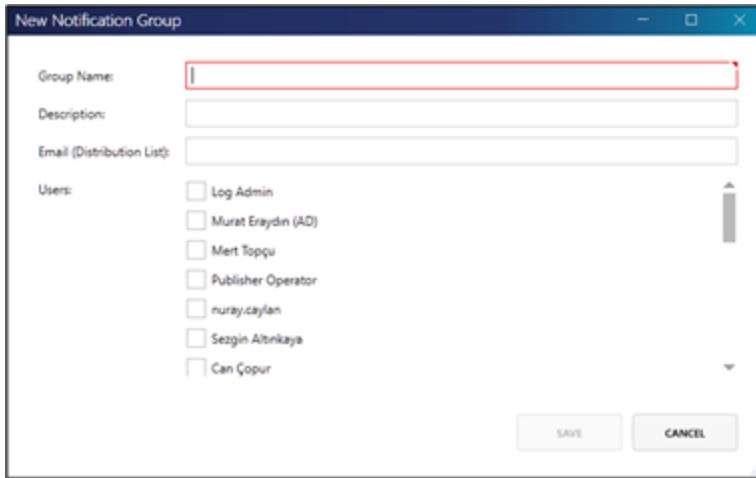
## Notification Groups

 Refresh  New...  Edit...  Delete...

Group Name	Description	Email
DefaultOps	Default Operators Group	
mgroup		can.copur@karmasis.com;bedircancopur@gr
asdasdasd		halit.dursun@karmasis

### Adding a New Notification Group

1. Enter **Group Name**, **Description**, and **Email** fields.
2. Click on **Users** who will be included in the group.



### Storage Settings

#### Main Storage Settings

This setting and its submenus are used to modify detailed storage settings related to Elasticsearch.

#### Storage

[SETTINGS](#) [SECURITY](#) [IMPORT ARCHIVE](#) [RESTORE FROM BACKUP](#) [CURATOR SETTINGS](#)

**WARNING: DO NOT CHANGE THESE PROPERTIES WITHOUT CONSULTING OPENTEXT SUPPORT.**

#### Database

Number of Shards:

Number of Replicas:

Hot Database Capacity (Days):

Warm Database Capacity (Days):

Hot Archive Capacity (Days):

Warm Archive Capacity (Days):

#### Data Sources

Activate warm database  Backup live database  Archive logs

Path: \\Dataskope-test1(esrepo)\backup Path: \\Dataskope-test1(esrepo)\hot

Last Backup: N/A Warm archive not found. [Create warm archive](#)

Last Archive: N/A

Send back-up files to ftp server  Send archive files to ftp server

Notify system administrators when process ends  Notify system administrators when process ends

SFTP **FTP** None

FTP Server:  FTP Port:

FTP User:

FTP Password:

### Storage Security Settings

This setting is used to set password for secure access to Elasticsearch.

## Storage

SETTINGS SECURITY IMPORT ARCHIVE RESTORE FROM BACKUP CURATOR SETTINGS

### Elasticsearch Credentials

User Name: **elastic**

Old Password:

New Password:

Confirm Password:

SAVE

CANCEL

### Import Archive Settings

This setting is used to restore users' old indexes from their archive.

## Storage

SETTINGS SECURITY IMPORT ARCHIVE RESTORE FROM BACKUP CURATOR SETTINGS

2021-10-07



2021-10-07



RESTORE

REFRESH

Select dates and click restore to start import from archive process.

### Restore from Backup

This setting is for viewing and restoring users' backed-up indexes.

# Storage

SETTINGS SECURITY IMPORT ARCHIVE RESTORE FROM BACKUP CURATOR SETTINGS

🔄 Refresh

[Create & Restore All](#)

2023-07-26	Missing index. (Backup not found.)	<a href="#">Re-create Index</a>
2023-07-27	Missing index. (Backup not found.)	<a href="#">Re-create Index</a>
2023-09-01	Missing index. (Backup not found.)	<a href="#">Re-create Index</a>
2023-09-02	Missing index. (Backup not found.)	<a href="#">Re-create Index</a>


## Storage Curator Settings

This setting can be used the necessary settings for the curator operation performed on Elasticsearch on a daily basis.

# Storage

SETTINGS SECURITY IMPORT ARCHIVE RESTORE FROM BACKUP CURATOR SETTINGS

## Curator Schedule

Daily Task Start Time:  

## Records Clean up

- |                       |                                     |                   |                                  |
|-----------------------|-------------------------------------|-------------------|----------------------------------|
| Delete alerts         | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="7"/>   |
| Resolve alerts        | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="2"/>   |
| Delete session logs   | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="10"/>  |
| Delete agents         | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="90"/>  |
| Delete resource usage | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="365"/> |

## Other operations

Import intelli search parameters  Send summary information

## System Notification Settings

This setting can be used to receive important system notifications in the form of an end-of-day report.

## System Notification

### E-mail Addresses

Summary information of the system will be delivered to these e-mail addresses.

 Refresh  New...  Delete...

bedircanCopur@gmail.com

can.copur@karmasis.com

halit.dursun@karmasis.com

### SMTP Server Settings

This setting can be utilized to configure mail service settings.

## SMTP Server

### SMTP Settings

SMTP Server:

SMTP Port:   SSL Enabled

SMTP From Address:

### Authentication Settings

Authentication Required

User Name:

Password:

SAVE

CANCEL

SEND TEST E-MAIL

### LDAP Server Settings

The server information related to users' LDAP service can be entered on this screen.

## LDAP Server

### LDAP Server

LDAP Server:

Example: **companydc.karma.intra/OU=CompanySUBOU,OU=CompanyOU,DC=karma,DC=intra**

IP / Host	Sub OU (Optional)	Parent OU (Optional)	Domain Name
-----------	-------------------	----------------------	-------------

### Authentication Settings

Authentication Required

User Name:

Password:

SAVE

CANCEL

TEST CONNECTION

### Action Account Settings

Domain Name, User Name and Password details of the action account can be entered on this screen.



## Action Account

Domain Name:

User Name:

Password:

SAVE

CANCEL

TEST CONNECTION

### Alert Forwarding Settings

This setting can be used to redirect alarms to another domain.

## Alert Forwarding

VDAM can send desired alerts to parent site. Please enter necessary information if you want this functionality. Consult your network administrator to find out Parent Site Name value.

Enable Alert Forwarding

Site Name (Active Directory):

Parent Site Name (Active Directory):

Test Alert Forwarding

### Forward Alerts On

Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

### Hours Allowed

0AM 6AM 12PM 18PM 23PM

CHECK ALL

CLEAR ALL

SAVE

CANCEL

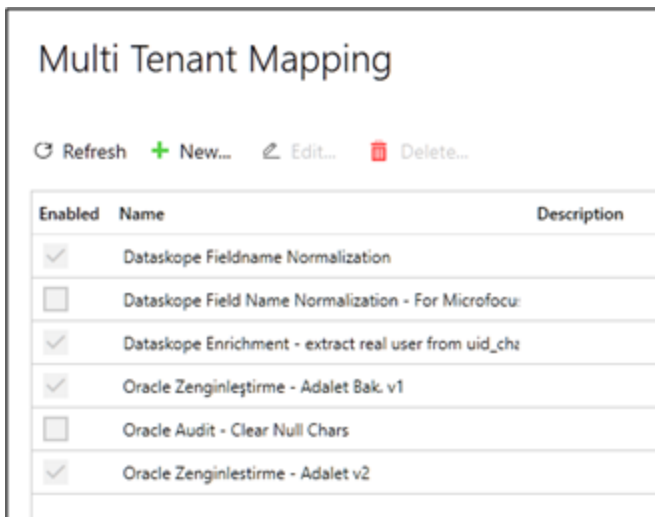
## Distributed Search Settings

This setting can be used to connect independent Elasticsearch instances together and perform searches from a single interface.



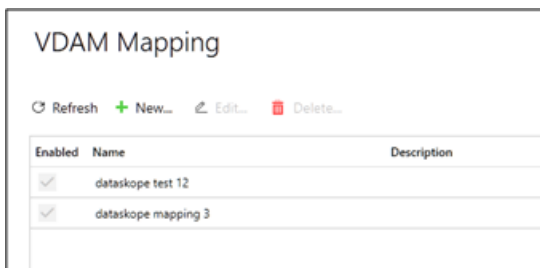
## Multi-Tenant Mapping Settings

Code can be written as a mapping to perform normalization, enrichment, and taxonomy on events.



## VDAM Mapping

VDAM Mapping enables the enrichment of logs at the VDAM Collector stage.



## OpenVAS Account Settings

To connect an OpenVAS account, credentials should be entered.

## OpenVAS Account

API Address:

User Name:

Password:

Enable OpenVAS API connection

TEST CONNECTION

SAVE

CANCEL

### File Server Settings

This setting can be used to define a new file server.

#### File Servers

[Refresh](#) [+ New...](#) [Edit...](#) [Delete...](#)

InUse	Name	Description	Protocol	SSL Mode	Server Address	Port	Path
-------	------	-------------	----------	----------	----------------	------	------

Figure 1: File Server Settings

### New File Server ✕

Name:

Description:

Protocol: SFTP ▼

SSL Mode: None ▼

Server Address:

Port:

User Name:

Password:

Path:

### All Settings

Accessing and modifying all settings on this screen is possible.

## All Settings

**WARNING: DO NOT CHANGE THESE PROPERTIES WITHOUT CONSULTING OPENTEXT SUPPORT.**

 Refresh  New...  Edit...  Delete...

Name	Value
▼ Section: AlertRules (1)	
▼ Section: ClientMonitoring (3)	
▼ Section: DailyJobs (6)	
▼ Section: DataMaskExpressions (2)	
▼ Section: Dataskope (1)	
▼ Section: dataskopecollectors (2)	
▼ Section: ESServer (20)	
▼ Section: InfraskopeSiemPlus (1)	
▼ Section: Register (5)	
▼ Section: Reports (1)	
▼ Section: Server (29)	
▼ Section: ServerRoles (4)	
▼ Section: Throttler (2)	

## Setting Editor



Section:

Name:

Value:

Is Password

Password:





Confirm Password:

SAVE

CANCEL

## All Settings

**WARNING: DO NOT CHANGE THESE PROPERTIES WITHOUT CONSULTING OPENTEXT SUPPORT.**

 Refresh
  New...
  Edit...
  Delete...

Name	Value
▲ Section: AlertRules (1)	
ConvertParamsToFieldName	False
▲ Section: ClientMonitoring (3)	
CpuUsageThreshold	90
MonitorEventsTotal	0
MonitorPerformanceCounters	0
▲ Section: DailyJobs (6)	
DeleteLoggedOnUsersOlderThanD	30
DeleteMessagesOlderThanHours	1
DomainControllerCheckInstalledAg	True
MSMQWarningGroupName	DefaultOps
MSMQWarningThreshold	1000000
NoAgentWarningGroupName	DefaultOps
▲ Section: DataMaskExpressions (2)	
executable_name	explorer\exe
sql_text	(WITH PASSWORD with password IDENTIFIED BY identified by)[\s\ W].*[a-zA-Z0-9!@#&()\\-'.+,\\"].*
▲ Section: Dataskope (1)	
maxnumberofagents	100
▲ Section: dataskopecollectors (2)	
DATASCOPE-TEST4	29fa2cc2-603e-4c96-b50a-fb652024df06
GOKHANKAYA-PC-2	cd34fdbb-dc0c-43bb-8406-48a5043102c0