

OpenText™ Database Activity Monitoring

Software Version 24.4.0

User Guide

opentext™

Document Release Date: October 2024
Software Release Date: October 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
DAM Users and Roles	7
DAM Architecture	7
Logging in to DAM	9
DAM Usage	10
Menu and Controls	10
Home	11
Cluster Status	12
Health and Disk	13
Index Size	13
Database Info	13
Top Activity	14
Events	14
Ongoing Alerts	15
Search	15
Search Panel	15
Date Range Section	16
Range	16
Export and Save Actions	17
Field Chooser	17
Historical Alert Processor	19
Breakdowns	20
Existing Assets	21
Queries	21
Reports	21
Schedule Properties	21
DAM Query Examples	24
String Queries	24
Specific Field-Based Queries	24
Regular Expression Queries	25
Regex String Queries	25
Regex Queries on Specific Fields	26

- Alerts 27
- Dashboard 28
 - Edit Dashboard 31
 - Actions 33
 - Creating a New Dashboard 33
- Agents 34
 - Agents Tab 40
 - Policies 41
 - Options 43
- Alert Rules 43
 - Adding New Alert Rule 44
 - Generic Rule 44
 - Missed Rule 45
 - Multi-hit Rule 46
- Mappings 47
 - Add New Mappings 47
- Lookup Lists 48
- Settings 50
 - User Settings 51
 - Adding New User 52
 - User Activities Settings 52
 - Roles Settings 53
 - Adding a New Role 53
 - API Users Settings 56
 - Adding a New API User 56
 - Security Settings 57
 - Notification Group Settings 57
 - Adding a New Notification Group 58
 - Storage Settings 58
 - Main Storage Settings 58
 - Storage Security Settings 59
 - Import Archive Settings 59
 - Restore from Backup 59
 - Storage Curator Settings 60
 - System Notification Settings 60
 - SMTP Server Settings 61
 - LDAP Server Settings 61
 - Action Account Settings 62
 - Alert Forwarding Settings 62
 - Distributed Search Settings 63

Multi-Tenant Mapping Settings	63
DAM Mapping	64
OpenVAS Account Settings	64
File Server Settings	64
All Settings	65

Introduction

OpenText™ Database Activity Monitoring (DAM) 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.

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 separation-of-duties principle. 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.

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

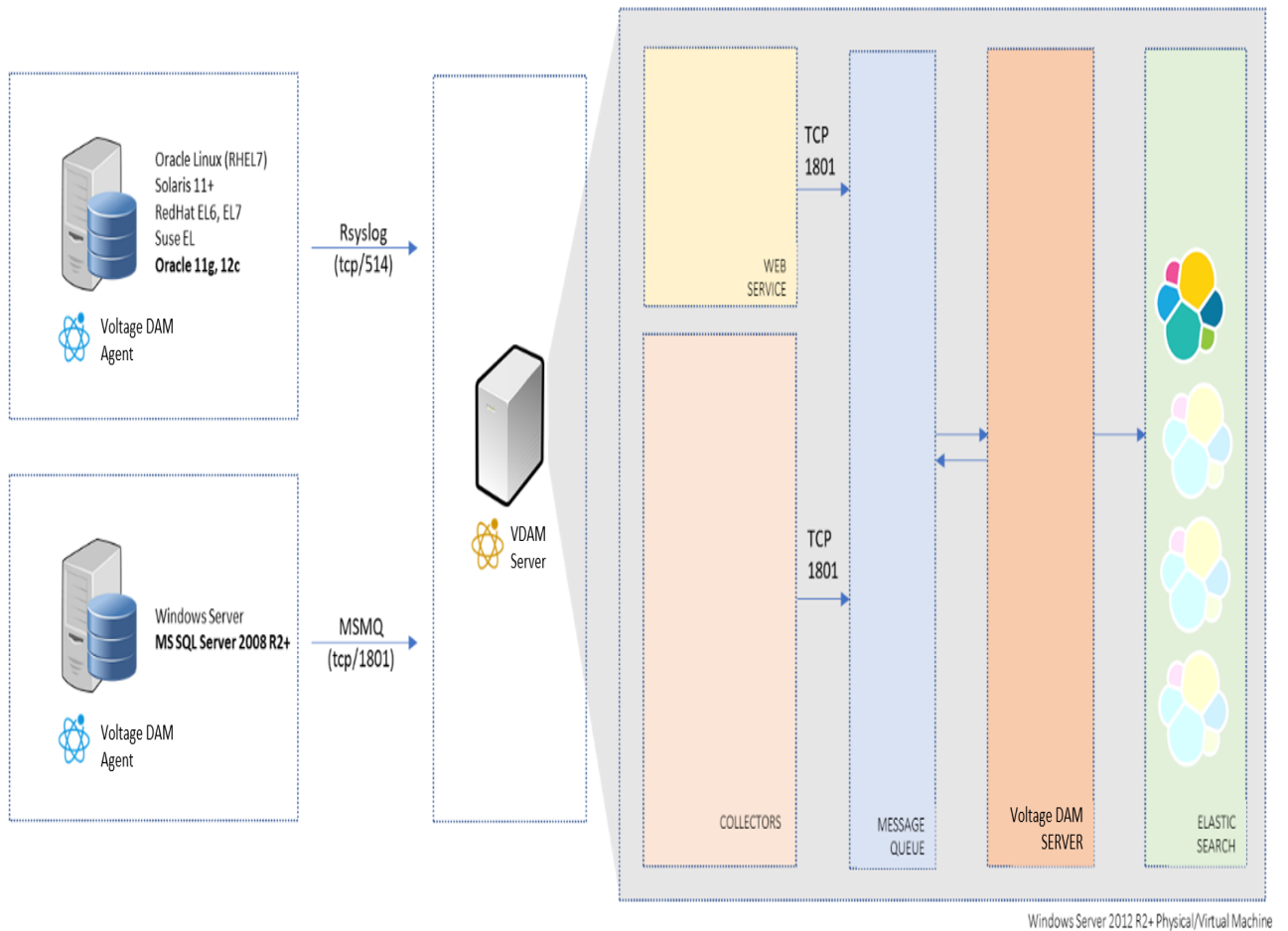
Abbreviations

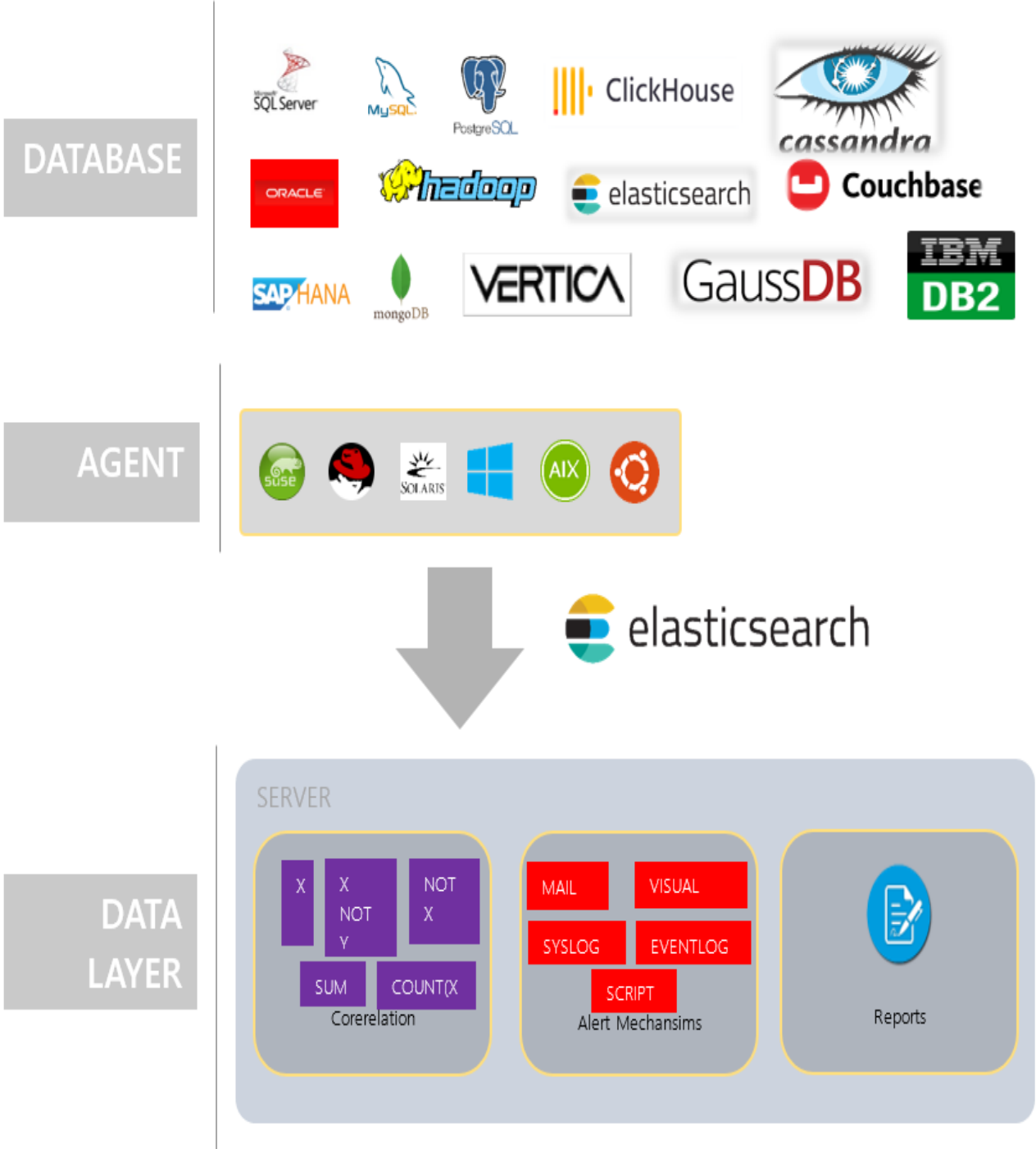
Abbreviations	Definition
DAM	Database Activity Monitoring
DSIM	DAM Installation Manager
DSPL	DAM Socket TAP Module
DSTAP	DAM TAP Module
LDAP	Lightweight Directory Access Protocol
OpenVAS	Open Vulnerability Assessment Scanner
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol

DAM Users and Roles

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

DAM Architecture





Logging in to DAM

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

1. Double click on OpenText™ Database Activity Monitoring icon.



2. Enter **Server Name**, **Username**, and **Password** on the DAM login page.

A screenshot of the OpenText Database Activity Monitoring login page. The page has a dark blue background. At the top left, the 'opentext™' logo is displayed in white, followed by a vertical line and the text 'Database Activity Monitoring'. Below this, there are three white input fields stacked vertically, labeled 'Server Name', 'User Name', and 'Password'. Under the 'Password' field, there is a small white checkbox labeled 'Remember me'. At the bottom center, there is a white rounded rectangular button labeled 'Sign In'.

3. Click **Sign In**.

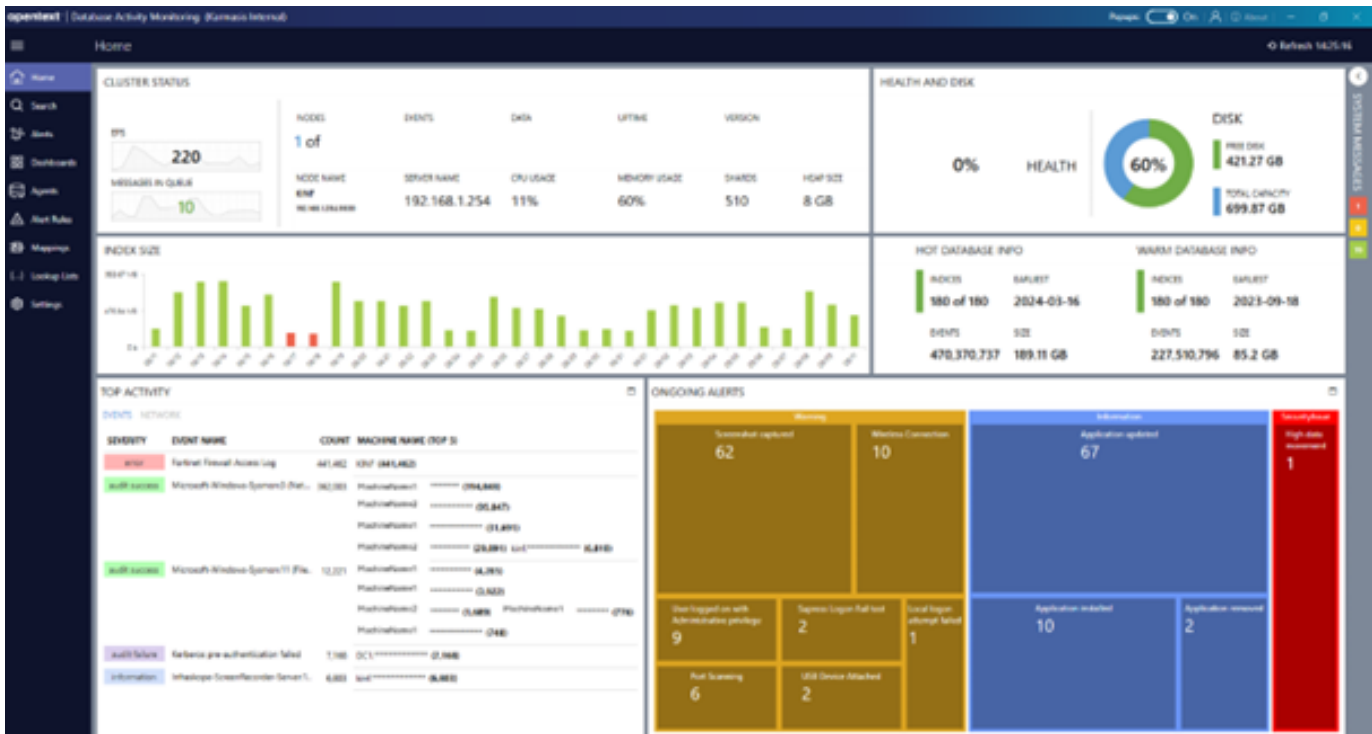
NOTE: The Server Name field can be filled in 3 ways: localhost, Server IP, or Server hostname.

- 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.






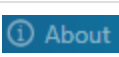

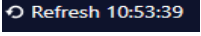


DAM Usage

Menu and Controls

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

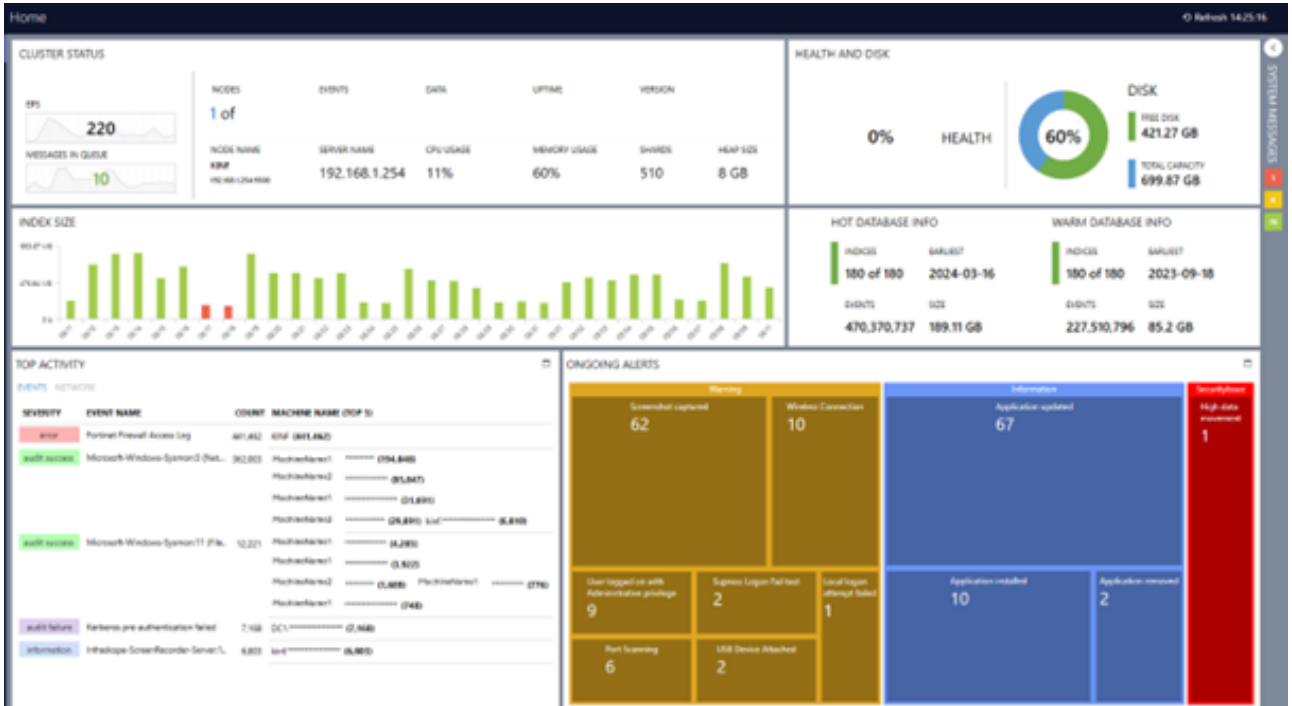


Menus	Function
Home	Used to display the home screen of DAM.
Search	Used to search events and export search results as x1s or pdf.
Alerts	Used to view alerts in detail.
Dashboards	Used to view and edit dashboards.
Agents	Used to show Agents, Policies and Options tabs, and Refresh, New Agent, Edit, Delete, Actions (Export, Send as E-mail) and Open Terminal tasks.
Alert Rules	Used to show alert and correlation rules.
Mappings	Used to view, edit and manage mappings in detail.

	Used to show Lookup Lists.
	Used to reach Settings as Users, User Activities, Roles, API Users etc.
	Used to close and open the menu on the left. The menu part can be closed for a wider graphic view.
	Used to turn pop-up contents on or off.
	Used to reach user details. Includes Logged On Users , My Profile and Logout submenus.
	Used to show Copyright, Version, Disclaimer and License information
	Used to check updates
	Used to refresh.
	<p>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.</p>

Home

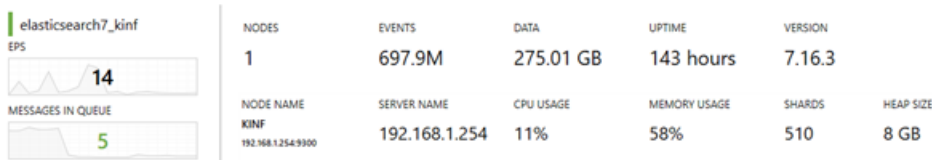
Performing an analysis of the current situation using a single screen facilitates efficient work management by enabling prompt actions to be executed. Accordingly, **Home** screen presents **Cluster Status**, **Health** and **Disk**, **Index Size**, **Database Info**, **Top Activity** and **Ongoing Alerts**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

CLUSTER STATUS



- **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

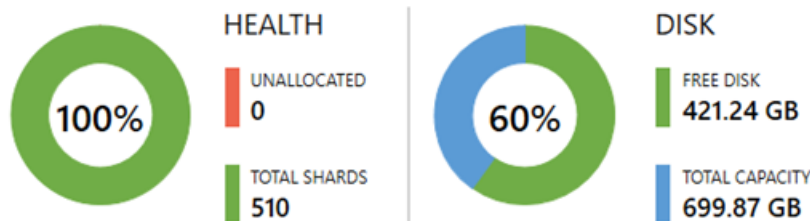
value for ElasticSearch is given as 3 GB max.

- **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 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.



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
180 of 180	2024-03-16
EVENTS	SIZE
470,388,139	189.12 GB

WARM DATABASE INFO

INDICES	EARLIEST
180 of 180	2023-09-18
EVENTS	SIZE
227,510,796	85.2 GB

- 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)
error	Fortinet Firewall Access Log	441,462	KINF (441,462)
audit success	Microsoft-Windows-Sysmon:3 (Net...	362,003	MachineName1 ***** (194,848) MachineName2 ***** (95,847) MachineName1 ***** (31,691) MachineName2 ***** (29,891) kinf***** (6,810)
audit success	Microsoft-Windows-Sysmon:11 (File...	12,221	MachineName1 ***** (4,285) MachineName1 ***** (3,922) MachineName2 ***** (1,689) MachineName1 ***** (776) MachineName1 ***** (748)
audit failure	Kerberos pre-authentication failed	7,168	DC1.***** (7,168)
information	Infraskope-ScreenRecorder-Server:1..	6,803	kinf.***** (6,803)

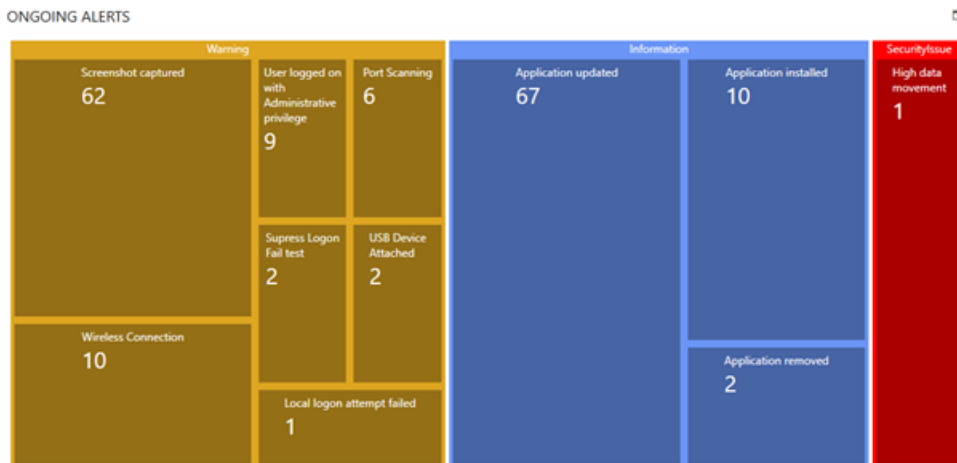
Events

- **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.



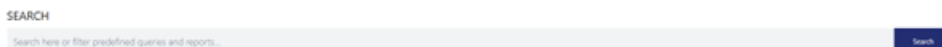
- **Warning** shows the warnings on clients.
- **Error** shows the unsuccessful attempts on clients.
- **Security Issue** shows the security breaches and vulnerabilities.
- **Information** shows the information of actions on clients.
- **Success** shows the successful actions.

Search

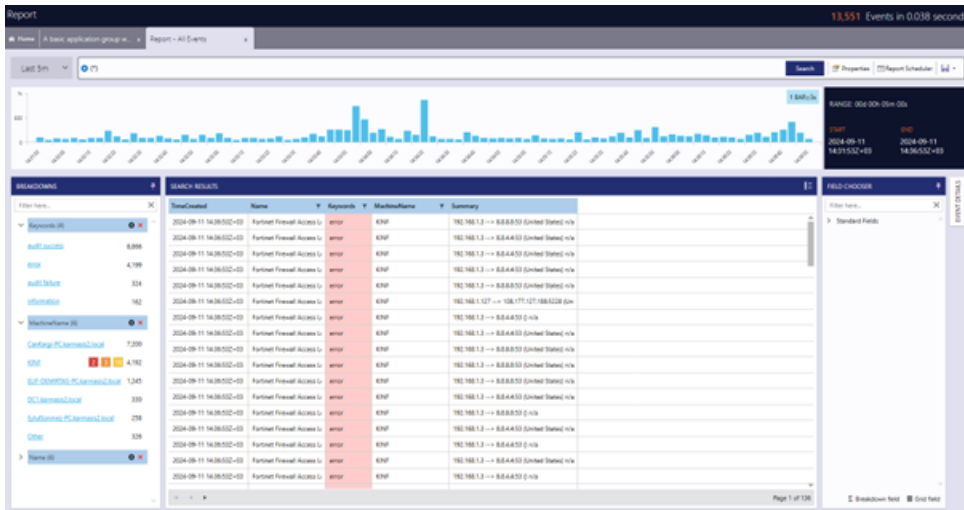
Search panel provides a search engine where user can examine event records in detail.

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.

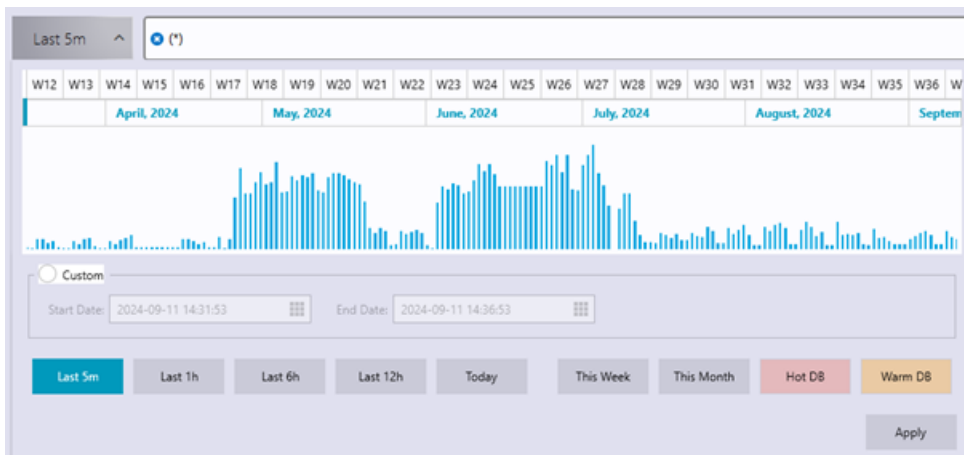


Accordingly, the Search screen presents **Breakdowns**, **Search Results**, **Event Details** and **Field Chooser** to the user.



Date Range Section

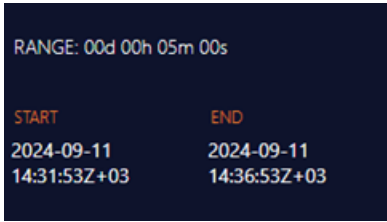
The date range section is automatically set to scan events that occurred within the last 5 minutes. Additionally, users can click on the relevant section to customize the date range according to their preferences.




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.

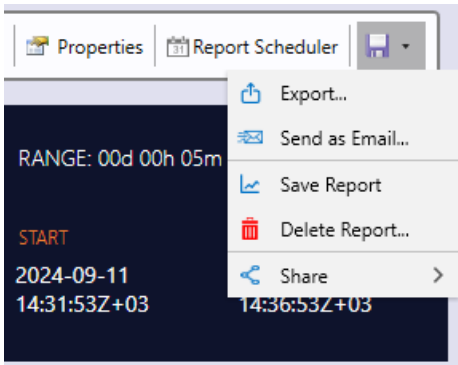
Range

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

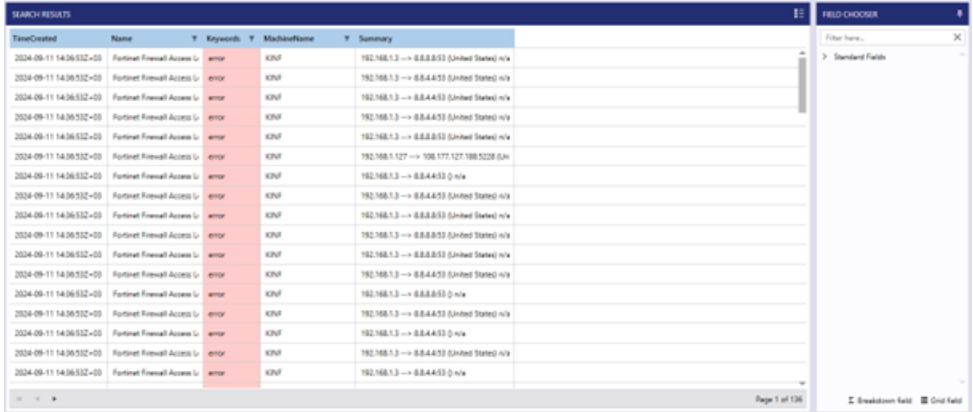


Export and Save Actions

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




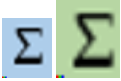

When you right-click on the unwanted columns in the query report and select "Remove" the respective column will be removed from the report area.

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.

Controls	Function
	Used to hide the Field Chooser panel.
<input type="text" value="Filter here..."/>	Used to filter the fields.
	Used to add the filter to the Breakdowns list.
	Used to add the filter to the search results table as a column.

SEARCH RESULTS					
TimeCreated	Name	Keywords	MachineName	Summary	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.8.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.8.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.8.53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 157.240.238.63:443 (United	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.134 --> 3.254.236.24:443 (United	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 57.144.126.192:443 (France)	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.134 --> 3.254.236.24:443 (United S	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.119 --> 8.8.4.53 (United States) r	
2024-09-11 14:36:53Z+03	Microsoft-Winc		argi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Winc		argi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Winc		argi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Winc		argi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Winc		argi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.134 (-)	

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.

SEARCH RESULTS

TimeCreated	Name	Keywords	MachineName	Summary
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.8.8:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.8.8:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 8.8.8.8:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 157.240.238.63:443 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.134 --> 3.254.236.24:443 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.3 --> 57.144.126.192:443 (France) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.134 --> 3.254.236.24:443 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Log	error	KINF	192.168.1.119 --> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.local	KARMASIS2\can.kargi -> 192.168.1.78 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.local	KARMASIS2\can.kargi -> 192.168.1.78 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.local	KARMASIS2\can.kargi -> 10.10.10.1 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.local	KARMASIS2\can.kargi -> 10.10.10.1 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.local	KARMASIS2\can.kargi -> 192.168.1.134 (-)

Page 1 of 136

Breakdowns

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

BREAKDOWNS

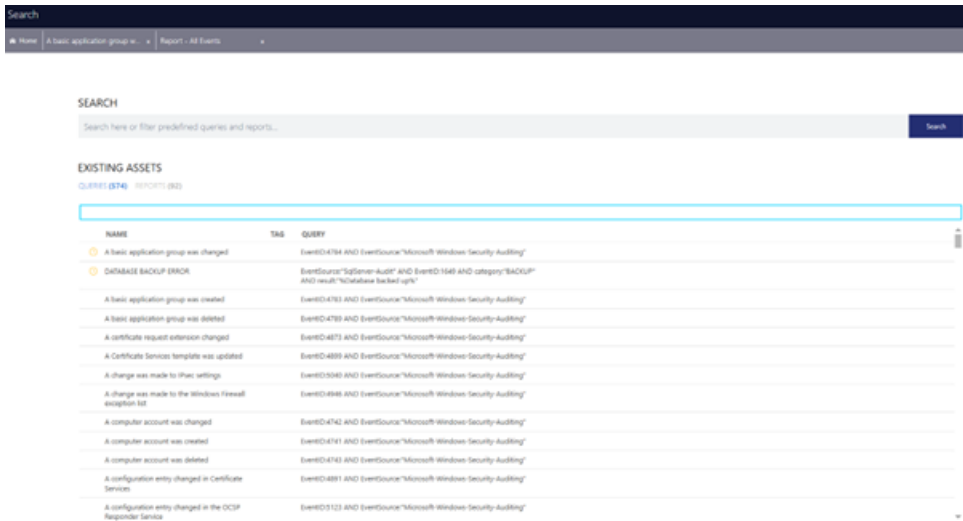
Filter here...

- Keywords (4)
 - audit success 8,866
 - error 4,199
 - audit failure 324
 - information 162
- MachineName (6)
 - CanKargi-PC.karmasis2.local 7,200
 - KINF 4,192
 - ELIF-DEMIRTAS-PC.karmasis2.local 1,245
 - DC1.karmasis2.local 330
 - EylulSonmez-PC.karmasis2.local 258
 - Other 326
- Name (6)
 - Microsoft-Windows-Sysmon3 (Network Co...
 - Fortinet Firewall Access Log

Existing Assets

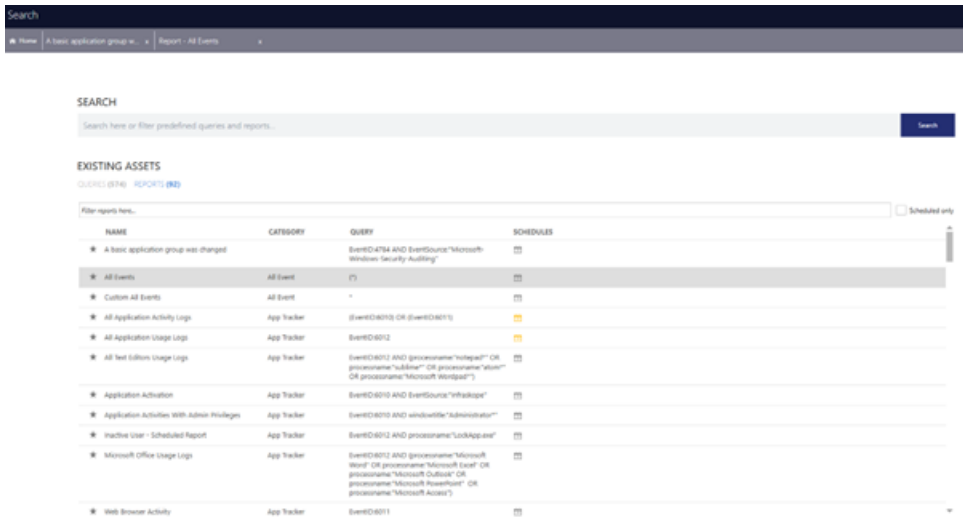
Queries

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

Users can select options and fill areas specific to their needs.

NOTE: When sending scheduled reports via email,

- Data used to generate reports is classified based on the classification feature associated with the role assigned to the recipients. This ensures that users only receive reports related to documents they are authorized to access.
- In case of an error the relevant log entry can be displayed in the System Messages section of the home page.

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: 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

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: 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

File sending with FTP enabled File sending with SFTP enabled

192.168.1.129 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

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

To perform searches with restrictions on different fields, you can use the following syntax:	Keywords: (critical OR error) AND EventSource: 'productname' EventSource: 'productname' AND (Keywords: 'critical' OR Keywords: 'error')
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 DAM, user can utilize the tilde (~) operator to perform fuzzy searches.	EventSource: producme~ (Correct spelling is productname) EventSource: productme~ EventSource: proutname~ EventSource: prouctnae~
To perform searches with restrictions on a single field:	EventSource: 'productname OR OSname' EventSource: 'productname OSname' (Works in the same way with OR)
To perform a search using a specified range:	TimeCreated: '[Date to Date]' TimeCreated: [* TO 2017-12-01] (Returns all dates before the specified date)
Search with sorting	EventID: >10 EventID: >=10 EventID: >= 500 AND EventID: <=1000 EventID: [500 TO 1000]

Regular Expression Queries

Regex String Queries

PURPOSE	QUERY
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)ro(ductname file)/ 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)ro./ 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",

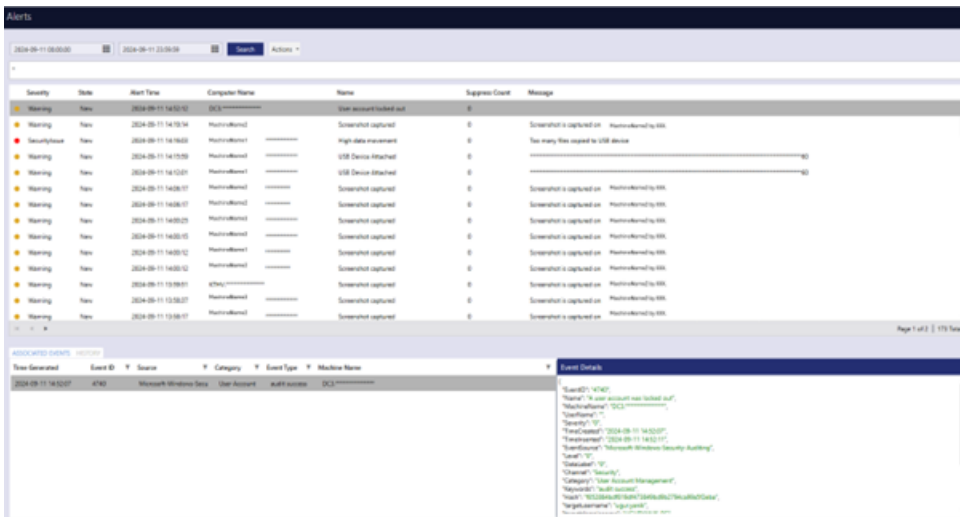
	and the "." represents any number of characters after "pro" or "Pro"
To search log entries start with a given character or word:	/a.*/ /companyname.*/
To search log entries ends with a given character or word:	/.*a/ /.*companyname /
To search for a keyword using wildcard characters, you can use the following 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:

Severity	State	Alert Time	Computer Name	Name
Warning	New	2024-09-11 14:42:12	PC2 *****	User account locked out
Warning	New	2024-09-11 14:16:03		Change Resolution State...
SecurityIssue	New	2024-09-11 14:16:03		Alert...
Warning	New	2024-09-11 14:15:59		All...
Warning	New	2024-09-11 14:12:01		Selected...
Warning	New	2024-09-11 14:06:17		New
				Acknowledged
				Assigned To Helpdesk
				Outsourced
				Resolved

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.

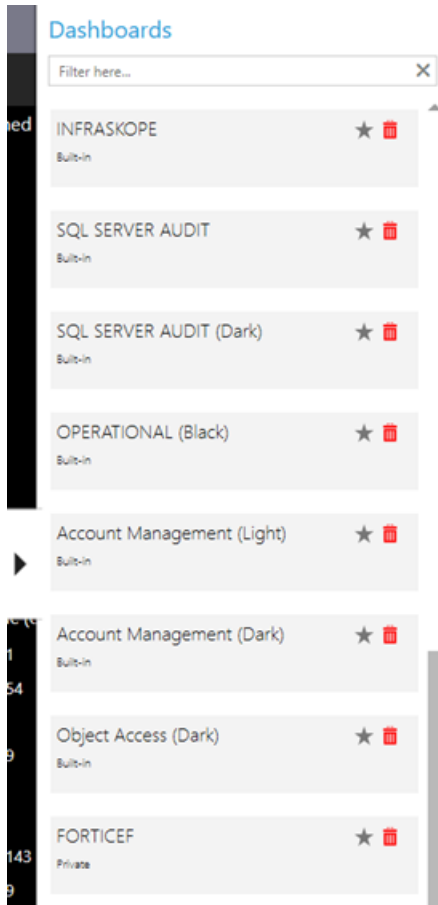
Dashboard


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.



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

When users want to delete one of the dashboard designs, they can click on the  icon.

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



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

Edit Dashboard

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

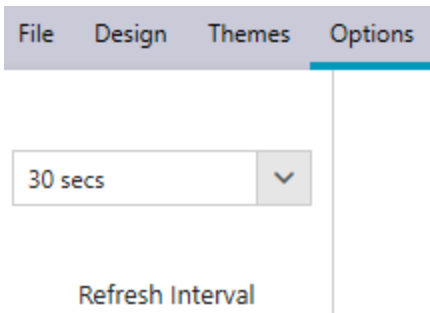
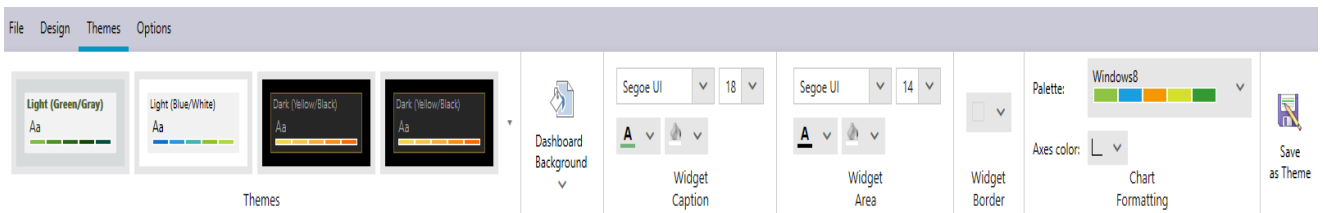
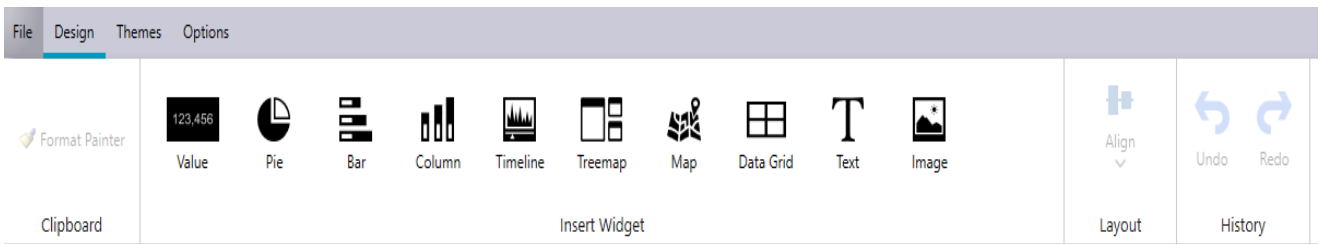
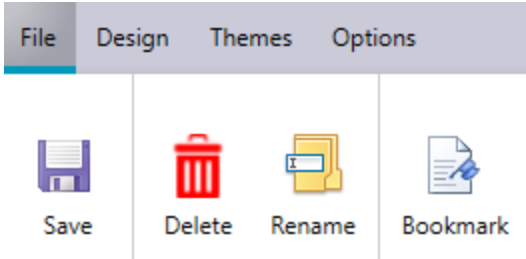
The **File** tab is used for **Save, Delete, Rename** and **Bookmark** operations.

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.

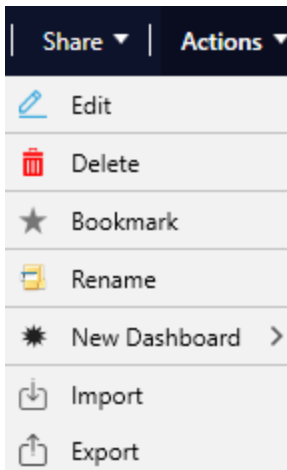
The **Themes** tab offers various **Theme Designs**. It also provides separate customization opportunities for **Background, Widget Caption, Widget Area, Widget Border** and **Chart Formatting**.

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,

1. Click **Actions > New Dashboard > Blank Dashboard**.
2. In the New Dashboard window, enter the Dashboard name and description.

3. 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:

Light (Green/Gray) Aa [Color bar]	Light (Blue/White) Aa [Color bar]	Dark (Yellow/Black) Aa [Color bar]	Dark (Yellow/Black) Aa [Color bar]
Dark (Khaki/Gray) Aa [Color bar]	Dark (Khaki/Gray) Aa [Color bar]	Dark (Green/Black) Aa [Color bar]	Dark (Green/Black) Aa [Color bar]

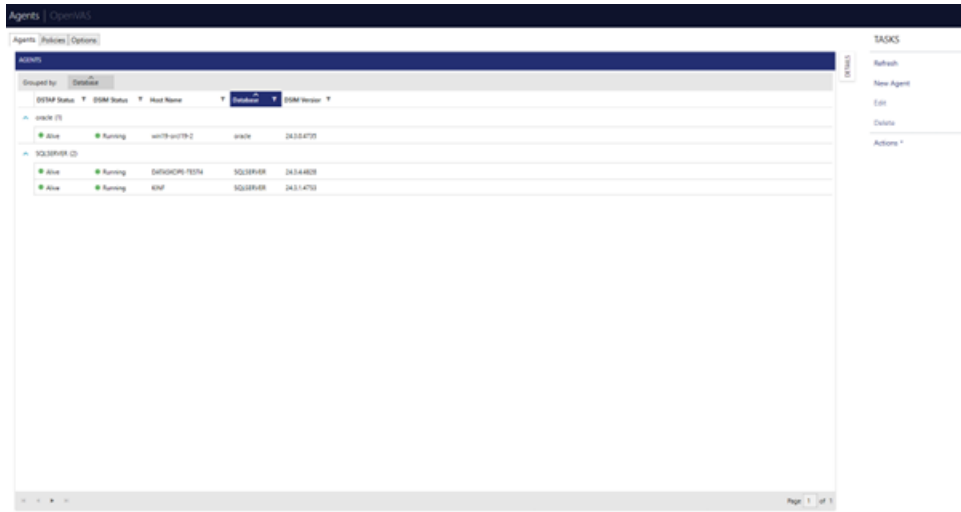
OK CANCEL

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**.

New Agent Wizard

Connection

Enter the connection information to connect to the agent

IP Address: : 8765

Protocol: TLS 1.2

Certificate

Use old default certificate Use new default certificate Upload certificate

Client Certificate: Browse

Password:

Use old certificate Use new certificate

CANCEL NEXT >

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

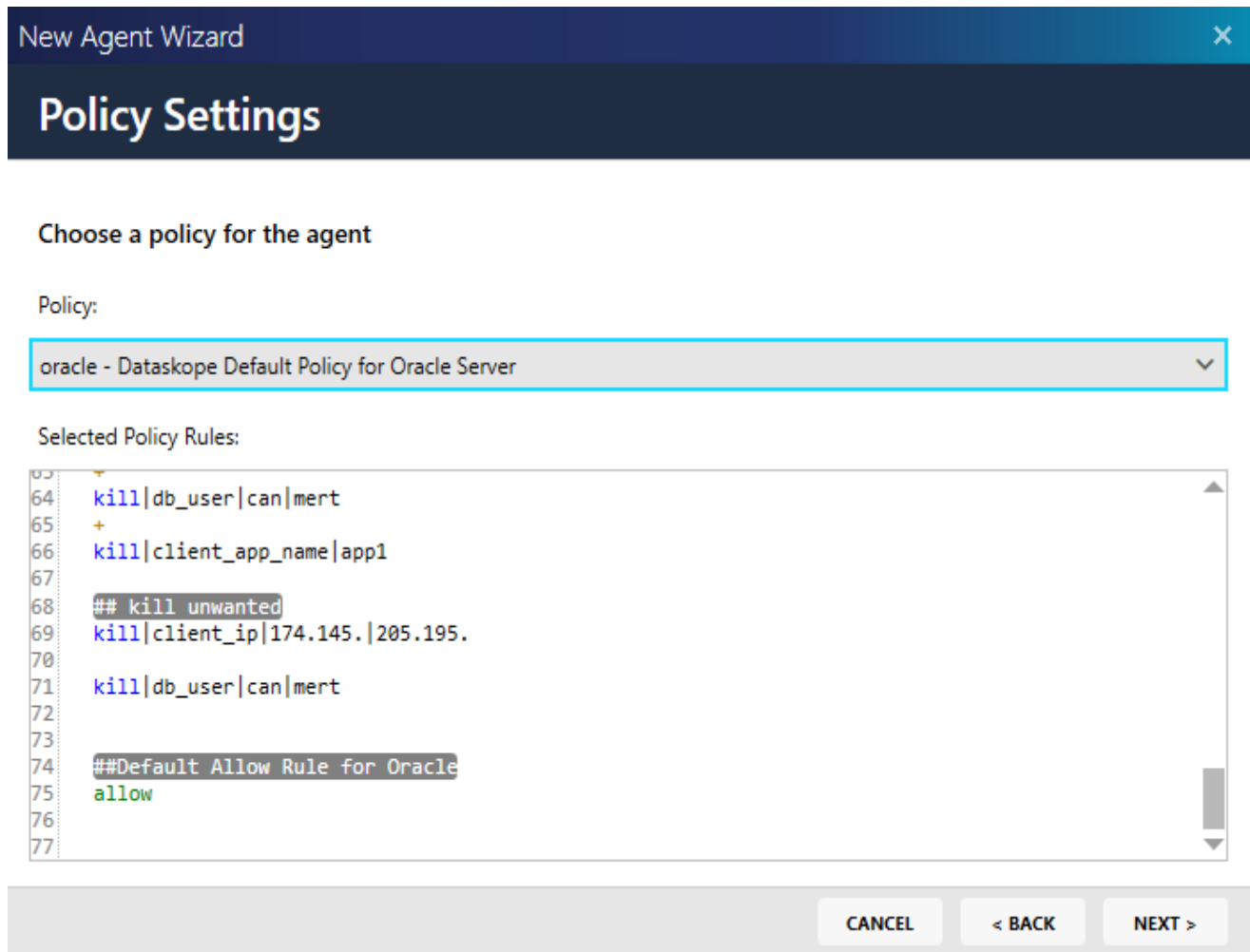
Listener Settings

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

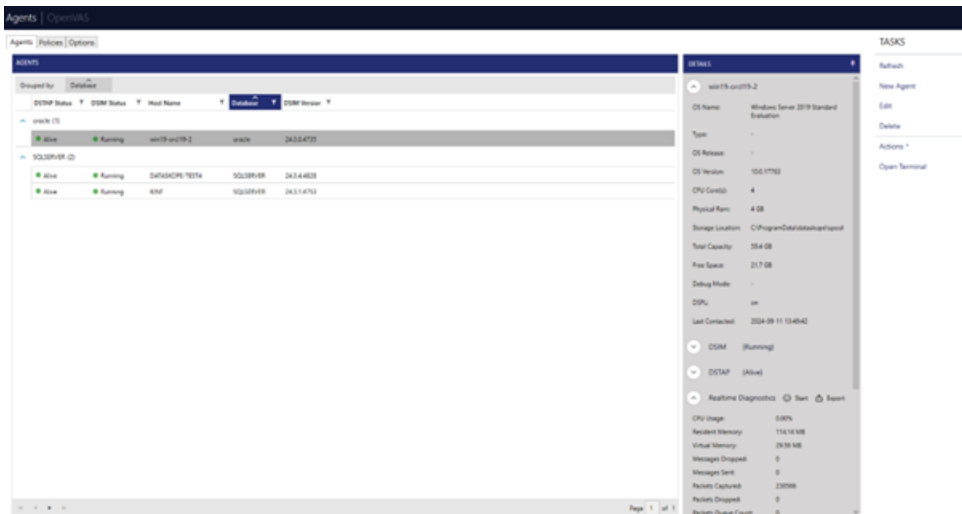
Collector Settings

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"/>	

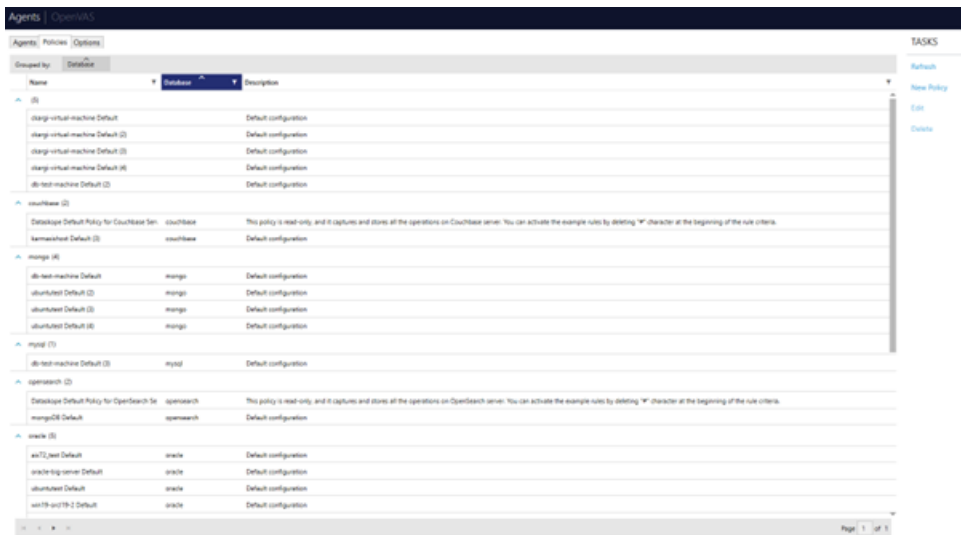
CANCEL **< BACK** **FINISH**

Agents Tab



Controls	Function
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.
Refresh	Used to refresh the agents tab.
New Agent	Used to add new agent. For more details, see Adding a New Agent .
Edit	Used to edit the selected agent.
Delete	Used to delete the selected agent.
Actions	Used to reach various actions related to the agents. Includes Export and Send as Email.
Open Terminal	Used to open terminal.

Policies



Controls	Functions
Refresh	Used to refresh the policy tab.
New Policy	Used to add new policy.
Edit	Used to edit the selected policy.
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.

Alert Rules

Controls	Function
New Category	Used to add new category about alert rules.
Refresh	Used to refresh alert rules.
New	Used to add new alert rule.
Edit	Used to edit the alert rule.
Delete	Used to delete the alert rule.

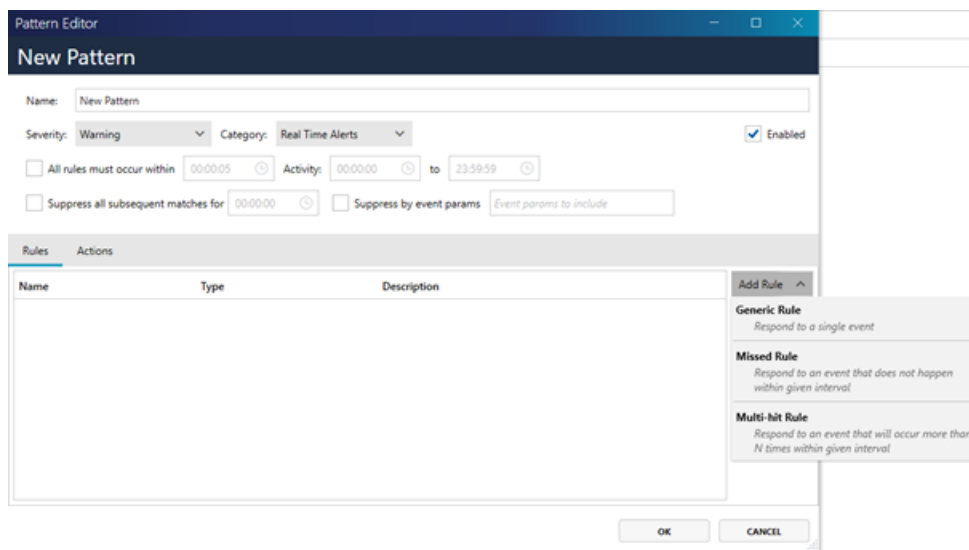
Column Details

- **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

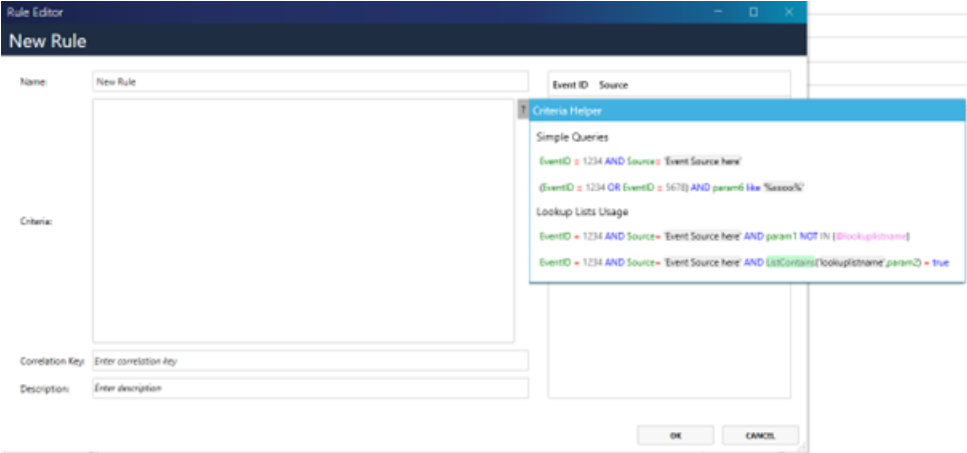
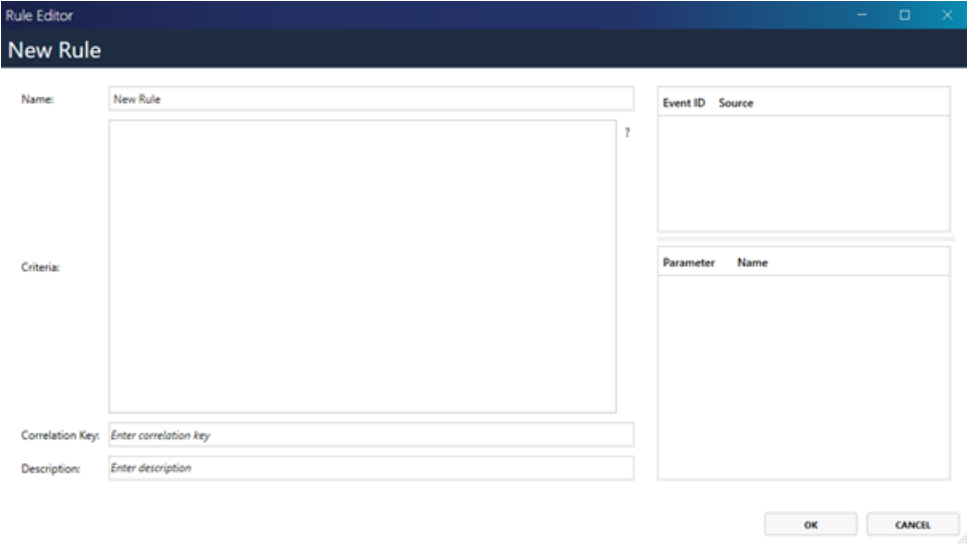
To add a new alert rule, click the **New** button on **Alert Rules** menu and follow the steps given below.

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 ? icon.



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 the 'Rule Editor' window with the title 'New Missed Rule'. The interface includes 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 with the placeholder text 'Enter correlation key'.
- Description:** A text box with the placeholder text 'Enter description'.
- From:** A time selection box set to '00:00:00'.
- To:** A time selection box set to '00:00:00'.
- Interval:** A time selection box set to '00:01:00'.
- Event ID Source:** A table with two columns: 'Event ID' and 'Source'. The table is currently empty.
- Parameter Name:** A table with two columns: 'Parameter' and 'Name'. The table is currently empty.
- Buttons:** 'OK' and 'CANCEL' buttons at the bottom right.

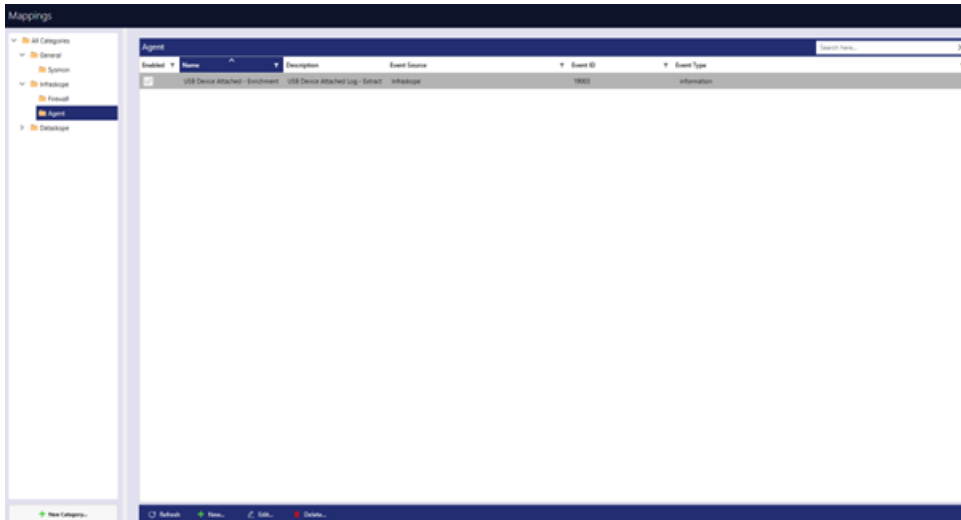
Multi-hit Rule

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.

The screenshot shows the 'Rule Editor' window with the title 'New Multi-hit Rule'. The interface includes the following fields and components:

- Name:** A text box containing 'New Multi-hit Rule'.
- Criteria:** A large empty text area with a question mark icon to its right.
- Correlation Key:** A text box with the placeholder text 'Enter correlation key'.
- Description:** A text box with the placeholder text 'Enter description'.
- Group By Key:** A text box with the placeholder text 'Enter group by key'.
- Interval:** A time selection box set to '00:00:30'.
- Match Condition:** A text box containing the expression 'COUNT() >= 100'.
- Event ID Source:** A table with two columns: 'Event ID' and 'Source'. The table is currently empty.
- Parameter Name:** A table with two columns: 'Parameter' and 'Name'. The table is currently empty.
- Buttons:** 'OK' and 'CANCEL' buttons at the bottom right.

Mappings



Controls	Function
New Category	Used to add new category about mappings.
Refresh	Used to refresh mappings.
New	Used to add new mapping.
Edit	Used to edit the mapping.
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.

The screenshot shows a configuration window for a mapping. It includes fields for Name, Description, Criteria, Event Source, and Event Type. Below these are three tabs: Input, Code, and Output. The Code tab is selected and contains a C# code snippet. At the bottom left, there is a checked 'Enabled' checkbox. At the bottom right, there are 'SAVE' and 'CLOSE' buttons.

Lookup Lists

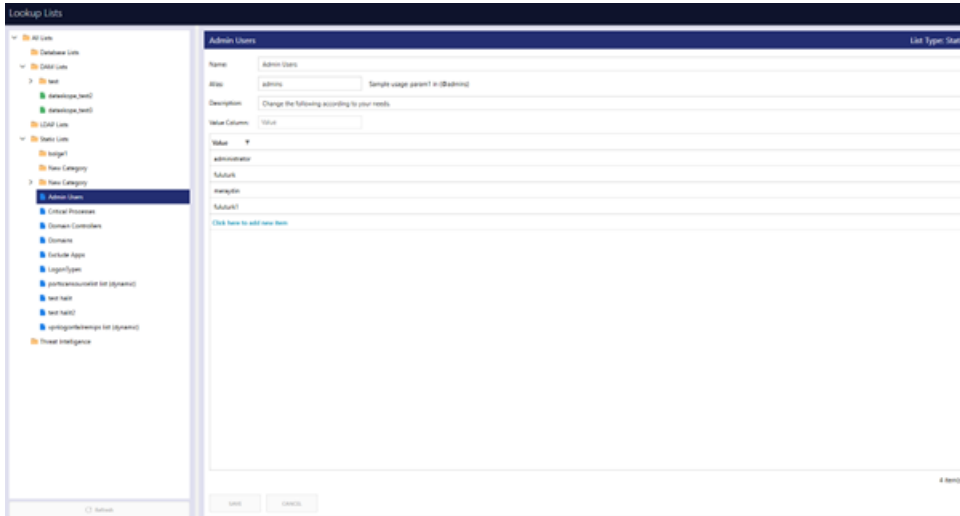
Lists that are used to modify the outputs of goals and are specifically tailored to the situation. These lists customize the outputs of goals, thereby increasing the accuracy of the outputs.

Purpose of use

- Adding lists to queries and reports on the search page.
- Adding lists to the alarm rules.
- Adding lists to Dataskope policies.
- Adding lists specific to the database.
- Adding lists specific to LDAP.

List Types

- Static List: Used to add lists to Search queries, Search reports, and Alarm rules.
- Dataskope List: Used to add lists to Dataskope policies.
- Database List: Used to customize database outputs.
- LDAP List: Used to customize LDAP outputs.



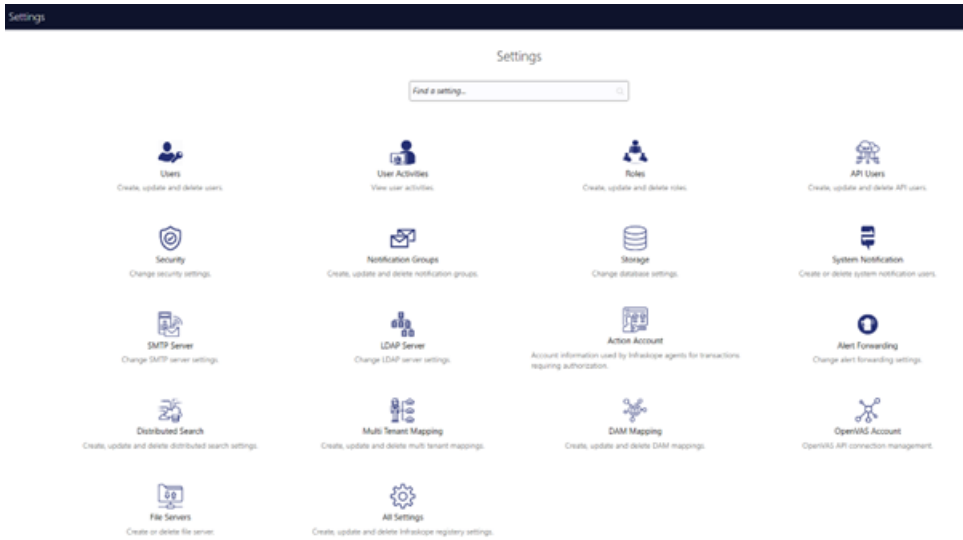
Clicking the Save button after each change to the list disables the automatic submission process, giving users the option to submit their modifications directly.










To activate this new change, click the **Commit**.















NOTE: Lookup list items can be easily moved to their relevant categories, enabling users to efficiently and quickly reorganize items within the category structure, making list management more flexible.

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 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.									
<p>DAM Mapping</p> <p>  Refresh  New...  Edit...  Delete... </p> <table border="1"> <thead> <tr> <th>Enabled</th> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>dataskope mapping 3</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>dataskope test 12</td> <td></td> </tr> </tbody> </table>	Enabled	Name	Description	<input checked="" type="checkbox"/>	dataskope mapping 3		<input checked="" type="checkbox"/>	dataskope test 12		VDAM Mapping	Used to create, update and delete VDAM Mappings
Enabled	Name	Description									
<input checked="" type="checkbox"/>	dataskope mapping 3										
<input checked="" type="checkbox"/>	dataskope test 12										
	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 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	2023-09-29 22:29:20	2024-09-11 14:49:40
<input checked="" type="checkbox"/>	Murat Ercaydin (AD)	meraydin@karmasis2.local	Users, Admin	murat.ercaydin@karmasis.com	2022-06-22 19:25:31	-
<input checked="" type="checkbox"/>	Mert Topcu	mert.topcu@karmasis2.local	Admin	mert.topcu@karmasis.com	2022-06-22 19:25:31	2023-08-03 14:01:59
<input checked="" type="checkbox"/>	Publisher Operator	publiher	Admin	fujyuk.turk@karmasis.com	2022-06-22 19:25:31	2022-10-04 13:32:19
<input checked="" type="checkbox"/>	nuray caylan	Nuray Caylan	Admin	nuray.caylan@karmasis.com	2022-06-22 19:25:31	-
<input checked="" type="checkbox"/>	Sevgin Altinkaya	saltinkaya@karmasis2.local	Admin	sevgin.altinkaya@karmasis.com	2022-06-22 19:25:31	2023-02-13 14:30:22
<input checked="" type="checkbox"/>	Can Copur	can.copur@karmasis2.local	Admin, Datastope	can.copur@karmasis.com	2022-06-22 19:25:31	2023-12-20 10:24:57
<input checked="" type="checkbox"/>	Database Audit Admin	dbadmin	Datastope	dbadmin@karmasis.com	2022-06-22 19:25:31	-
<input checked="" type="checkbox"/>	Micro Focus	microfocus	Admin	karmasiapi@karmasis.com	2022-06-22 19:25:31	-
<input type="checkbox"/>	Ali Ekortobi	ekortobi	Datastope Group	aliekortobi@microfocus.com	2022-06-22 19:25:31	2019-12-17 10:44:33
<input checked="" type="checkbox"/>	SEM Test	semtest	TestSEM	sem@karmasis.com	2022-06-22 19:25:31	2020-06-17 12:31:34
<input checked="" type="checkbox"/>	STM	stm	Read-Only User	stm@karmasis.com	2022-06-22 19:25:31	2020-07-08 11:01:29
<input checked="" type="checkbox"/>	STM2	stm2	test_default	stm@karmasis.com	2022-06-22 19:25:31	2020-07-08 10:36:05
<input checked="" type="checkbox"/>	Company1	company1	Company1	company1@karmasis.com	2022-06-22 19:25:31	2021-02-25 14:03:01
<input checked="" type="checkbox"/>	Company2	company2	Company2	company2@karmasis.com	2022-06-22 19:25:31	2021-02-25 14:06:51
<input checked="" type="checkbox"/>	Company3	company3	Company3	company3@karmasis.com	2022-06-22 19:25:31	2021-02-25 14:12:38
<input checked="" type="checkbox"/>	Gokhan KAYA	gokhan.kaya	Admin	tgokhankaya@gmail.com	2022-08-16 15:00:01	-
<input checked="" type="checkbox"/>	Hasan Keskin	hasan.keskin	Users, test_default, EGM TEST - AD	hasan.keskin@karmasis.com	2023-01-18 10:03:56	2023-01-18 10:04:53
<input checked="" type="checkbox"/>	Halit Dursun	halit.dursun@karmasis2.local	Admin	halit.dursun@gmail.com	-	2023-11-01 11:12:48
<input checked="" type="checkbox"/>	can kargi	ckargi	Users, test_default, Admin	can.kargi@karmasis.com	2024-02-26 00:00:00	-

Adding New User

Click **New** to add a new user and update the login information.

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

2024-09-11 00:00:00 2024-09-11 23:59:59 Search here... DAM Usage Logs DAM API Usage Logs Search Actions Preferences

Drag a column header and drop it here to group by that column

Time Generated	Computer Name	OS User Name	IP Address	Operator	Module	Action
2024-09-11 16:55:51	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	Publisher	GetCustomer
2024-09-11 16:57:47	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	Users	GetOperators
2024-09-11 16:51:13	CD07JANCKR-PC	ezger	192.168.1.132	Log Admin	Publisher	GetCustomer
2024-09-11 16:50:12	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	Operations	GetCursorSettings
2024-09-11 16:46:17	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:46:03	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:46:03	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:46:03	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:46:02	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:45:47	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:45:33	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:45:33	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:45:33	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:45:32	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:45:17	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:45:03	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:45:02	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:44:47	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts
2024-09-11 16:44:33	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:44:33	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:44:33	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Search
2024-09-11 16:44:32	KPNCTT300	bsnrskucuk	192.168.1.3	Log Admin	EventFunctions	Alerts

ACTIVITY DETAILS

```
{
  "Service": "Publisher",
  "Action": "GetCustomer",
  "Method": "GET"
}
```

Session ID: 548162f-a312-4035-867d-4db3ac6ae7f4 [Monitor](#)

Computer Name: KPNCTT300 OS User Name: bsnrskucuk
IP Address: 192.168.1.3 Operator: Log Admin
Service: Publisher Action: GetCustomer

Page 1 of 9

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...](#)

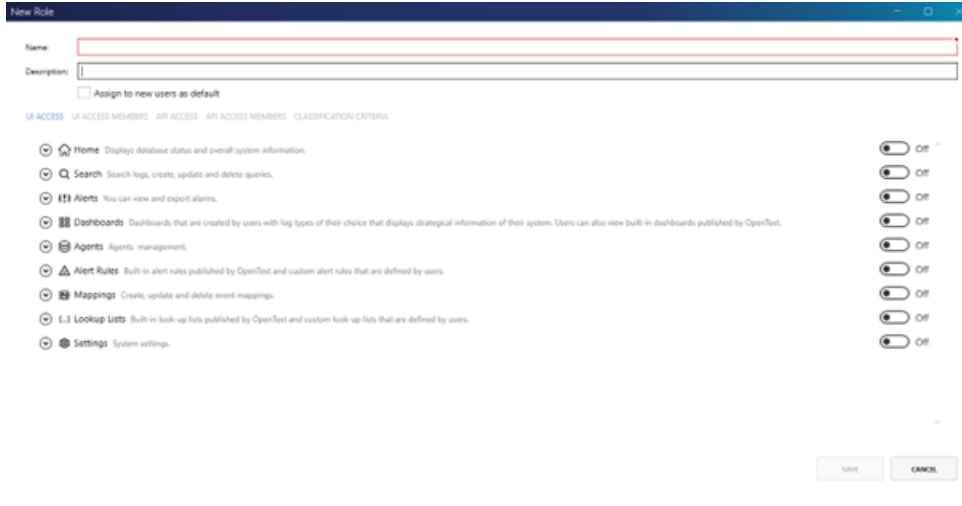
Default	Outside Connection	Role Name	Description
<input type="checkbox"/>	<input type="checkbox"/>	Admin	This role has access to all features.
<input type="checkbox"/>	<input type="checkbox"/>	Admin Role Test	
<input type="checkbox"/>	<input type="checkbox"/>	Company1	
<input type="checkbox"/>	<input type="checkbox"/>	Company2	
<input type="checkbox"/>	<input type="checkbox"/>	Company3	
<input type="checkbox"/>	<input type="checkbox"/>	Dataskope	
<input type="checkbox"/>	<input type="checkbox"/>	Dataskope Group	
<input type="checkbox"/>	<input type="checkbox"/>	EGM TEST - ADMIN ROLE	
<input type="checkbox"/>	<input type="checkbox"/>	EGM TEST - USER ROLE	
<input type="checkbox"/>	<input type="checkbox"/>	INTERN	Stajyer Grubu
<input type="checkbox"/>	<input type="checkbox"/>	Read-Only User	
<input type="checkbox"/>	<input type="checkbox"/>	Sales	
<input type="checkbox"/>	<input type="checkbox"/>	Test	Halit test1
<input checked="" type="checkbox"/>	<input type="checkbox"/>	test_default	
<input type="checkbox"/>	<input type="checkbox"/>	TestSIEM	
<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

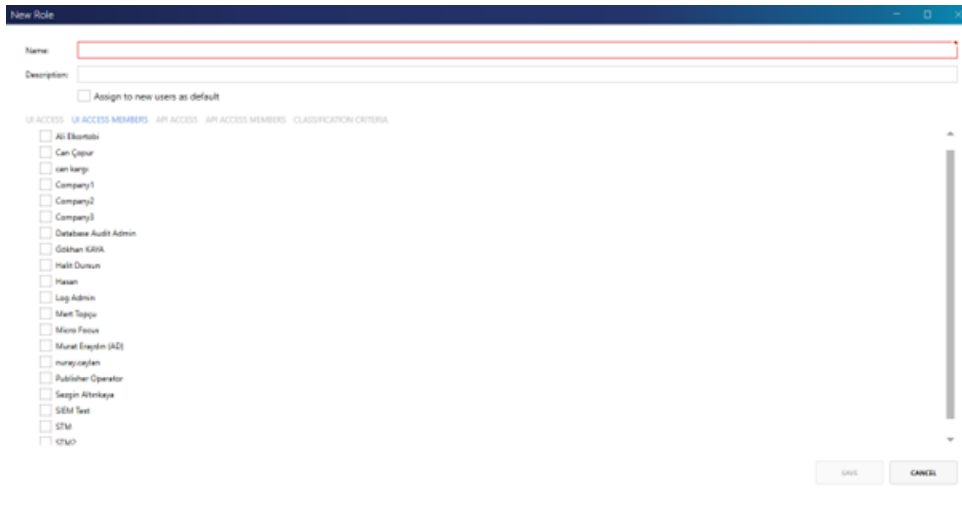
This is used to customize the access scope as desired when adding a new role.

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.



5. In **UI ACCESS MEMBERS**, select the users you want to have in this role.



6. In **API Access** tab, configure permissions for accessing public endpoints.

New Role

Name:

Description:

Assign to new users as default

API ACCESS | API ACCESS MEMBERS | API ACCESS | API ACCESS MEMBERS | CLASSIFICATION CRITERIA

Search By Events Off

SAVE CANCEL

7. In **API Access Members** tab, select the API Users assigned to that role.

New Role

Name:

Description:

Assign to new users as default

API ACCESS | API ACCESS MEMBERS | API ACCESS | API ACCESS MEMBERS | CLASSIFICATION CRITERIA

api-user
 microsoft
 test
 testapiuser
 user-test

SAVE CANCEL

8. In **CLASSIFICATION CRITERIA**, check **Activate Classification** if necessary.

9. Select **Field Queries** or **Raw Query String** and complete the relevant details.

Filter Rule

Name:

Description:

Assign to new users as default

UI ACCESS | UI ACCESS MEMBERS | API ACCESS | API ACCESS MEMBERS | CLASSIFICATION CRITERIA

Activate Classification

Field Queries

Must Filter

Must NOT Filter

Raw Query String

Company Name:

SAVE CANCEL

API Users Settings

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

API Users

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

Active	User Name	Name	Role
<input checked="" type="checkbox"/>	api-user	api-user	
<input checked="" type="checkbox"/>	microfocus	Microfocus API	
<input checked="" type="checkbox"/>	test	test	Admin Role Test
<input checked="" type="checkbox"/>	TestApiUser	TestApiUser	
<input checked="" type="checkbox"/>	user-test	user-test	Admin Role Test

Adding a New API User

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.

New User

Account Information

Name:

User Name:

Role:

Active

Expires on

Authentication

Password:

NOTE:

- Access to API users using public endpoints is granted based on assigned roles.
- Users attempting to access endpoints they are not authorized to are notified accordingly.
- Furthermore, data queried through endpoints is filtered based on the classification defined in the user's role, ensuring that only authorized records are displayed.

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

Notification Group Settings

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

Notification Groups

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

Group Name	Description	Email
DefaultOPS	Default Operators Group.	
Security Ops		
İdari		idari@karmasis.com
Teknik		
MSMQ Ops		
Test		
Dev	Dev	
Dev2		
EGM TEST		
Schedule Test Group		halit.001@

Adding a New Notification Group

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

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

- Group Name: [Empty text box]
- Description: [Empty text box]
- Email (Distribution List): [Empty text box]
- Users: A list of users with checkboxes:
 - Log Admin
 - Murat Eraydin (AD)
 - Mert Topçu
 - Publisher Operator
 - nuray.caylan
 - Sezgin Altinkaya
 - Can Çopur

Buttons: SAVE, CANCEL

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):

Archive Capacity (Days):

Data Sources

Activate warm database

Backup live database

Archive logs

Path: \\KINP\es7backup Path: \\KINP\infraelastic_hot_repository

Last Backup: 2024-09-11 01:01 Last Archive: 2024-09-11 01:00

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

FTP Server:

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:

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

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.)	Re-create Index
2023-07-27	Missing index. (Backup not found.)	Re-create Index
2023-09-01	Missing index. (Backup not found.)	Re-create Index
2023-09-02	Missing index. (Backup not found.)	Re-create Index

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 older than (days)
- Resolve alerts older than (days)
- Delete session logs older than (days)
- Delete agents older than (days)
- Delete resource usage older than (days)

Other operations

- Import intelli search parameters
- Include inactive machines in the summary report
- 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...

halit.dursun@karmasis.com

SMTP Server Settings

This setting can be utilized to configure mail service settings.

SMTP Server

SMTP Settings

SMTP Server:	<input type="text" value="smtp.office365.com"/>
SMTP Port:	<input type="text" value="587"/> <input checked="" type="checkbox"/> SSL Enabled
SMTP From Address:	<input type="text" value="infraskope@karmasis.com"/>

Authentication Settings

Authentication Required

User Name:	<input type="text" value="infraskope@karmasis.com"/>
Password:	<input type="password" value="••••••••"/>

<input type="button" value="SAVE"/>	<input type="button" value="CANCEL"/>	<input type="button" value="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:
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

DAM 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):

Forward Alerts On

Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Hours Allowed

0AM 6AM 12PM 18PM 23PM

Distributed Search Settings

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

Distributed Search

Enable Cross Cluster Search

Cluster Manage Url:

Authentication

UserName:

Password:

Seeds

Name	Cluster Name	ES URL(s)	Cross Cluster Search Status	IP Address	Port	Include in Cross Cluster Search	Include in Manage Alerts
------	--------------	-----------	-----------------------------	------------	------	---------------------------------	--------------------------

Multi-Tenant Mapping Settings

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

Multi Tenant Mapping

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

Enabled	Name	Description
<input checked="" type="checkbox"/>	Dataskope Fieldname Normalization	
<input type="checkbox"/>	Dataskope Field Name Normalization - For Microfocu:	
<input checked="" type="checkbox"/>	Dataskope Enrichment - extract real user from uid_chz	
<input checked="" type="checkbox"/>	Oracle Zenginleştirme - Adalet Bak. v1	
<input type="checkbox"/>	Oracle Audit - Clear Null Chars	
<input checked="" type="checkbox"/>	Oracle Zenginleştirme - Adalet v2	

DAM Mapping

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

DAM Mapping

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

Enabled	Name	Description
<input checked="" type="checkbox"/>	dataskope mapping 3	
<input checked="" type="checkbox"/>	dataskope test 12	

OpenVAS Account Settings

To connect an OpenVAS account, credentials should be entered.

OpenVAS Account

API Address:

User Name:

Password:

Enable OpenVAS API connection

File Server Settings

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

File Servers

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

Hide	Name	Description	Protocol	SSL Mode	Server Address	Port	Path
<input checked="" type="checkbox"/>	192.168.1.40		FTP	None	192.168.1.40	21	
<input type="checkbox"/>	192.168.1.74		SFTP	None	192.168.1.74	22	
<input type="checkbox"/>	192.168.1.129 (ftp)	Ftp	FTP	None	192.168.1.129	21	/home/schedula-reports
<input type="checkbox"/>	Curator FTP Server		SFTP	Explicit	192.168.1.254	21	

Figure 1: File Server Settings

New File Server

Name:

Description:

Protocol: SFTP

SSL Mode: None

Server Address:

Port: 22

User Name:

Password:

Path:

TEST CONNECTION SAVE CANCEL

Figure 2:

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: Admins (1)	
Section: AlertRules (1)	
Section: ClientMonitoring (3)	
Section: DailyArchiver (1)	
Section: DailyJobs (4)	
Section: DataMaskExpressions (7)	
Section: DataMaskSettings (2)	
Section: dataskopecollectors (5)	
Section: ESServer (24)	
Section: Helpdesk (4)	
Section: InfraskopeSiemPlus (1)	
Section: Kafka (1)	
Section: KafkaCluster (4)	
Section: Nessus (3)	

Setting Editor

Section:

Name:

Value:

Is Password

 Password:

 Confirm Password:

SAVE CANCEL