

# **OpenText™ Database Activity Monitoring**

## **User Guide**

Version : 25.3

PDF Generated on : 04/08/2025

# Table of Contents

1. User Guide .....	5
1.1. Abbreviations .....	6
1.2. DAM Users and Roles .....	7
1.3. DAM Architecture .....	8
1.4. Logging in to DAM .....	9
1.5. Console .....	10
1.5.1. Home .....	12
1.5.1.1. Cluster Status .....	13
1.5.1.2. Health and Disk .....	14
1.5.1.3. Index Size .....	15
1.5.1.4. Database Info .....	16
1.5.1.5. Top Activity .....	17
1.5.1.5.1. Events .....	18
1.5.1.6. Ongoing Alerts .....	19
1.5.2. Search .....	20
1.5.2.1. Search Panel .....	21
1.5.2.1.1. Date Range Section .....	22
1.5.2.1.2. Range .....	23
1.5.2.1.3. Export and Save Actions .....	24
1.5.2.1.4. Field Chooser .....	25
1.5.2.1.5. Historical Alert Processor .....	28
1.5.2.1.6. Breakdowns .....	29
1.5.2.2. Existing Assets .....	30
1.5.2.3. DAM Query Examples .....	34
1.5.2.4. Regular Expression Queries .....	36
1.5.3. Alerts .....	38

---

1.5.4. Dashboard .....	40
1.5.4.1. Edit Dashboard .....	43
1.5.4.2. Actions .....	44
1.5.5. Agents .....	46
1.5.5.1. Agents Tab .....	51
1.5.5.2. Policies Tab .....	52
1.5.5.3. Options Tab .....	54
1.5.6. Alert Rules .....	55
1.5.6.1. Adding New Alert Rule .....	56
1.5.6.1.1. Generic Rule .....	57
1.5.6.1.2. Missed Rule .....	58
1.5.6.1.3. Multi-hit Rule .....	59
1.5.7. Mappings .....	60
1.5.7.1. Add New Mappings .....	61
1.5.8. Lookup Lists .....	62
1.5.9. Settings .....	64
1.5.9.1. User Settings .....	66
1.5.9.1.1. Adding New User .....	67
1.5.9.2. Audit Logs Settings .....	68
1.5.9.3. Roles Settings .....	69
1.5.9.3.1. Adding a New Role .....	70
1.5.9.4. API Users Settings .....	73
1.5.9.5. Security Policies Settings .....	75
1.5.9.6. Notification Group Settings .....	76
1.5.9.7. Storage Settings .....	77
1.5.9.8. System Notification Settings .....	80
1.5.9.9. SMTP Server Settings .....	81

---

1.5.9.10. Lookup List Source Settings .....	82
1.5.9.11. Action Account Settings .....	83
1.5.9.12. Distributed Search Settings .....	84
1.5.9.13. Multi-Tenant Mapping Settings .....	85
1.5.9.14. DAM Mapping Settings .....	86
1.5.9.15. OpenVAS Account Settings .....	87
1.5.9.16. File Server Settings .....	88
1.5.9.17. All Settings .....	89
1.5.10. Changing Company Logo .....	94
1.6. Transferring Reports .....	95

# 1. User Guide

## Introduction

OpenText™ Database Activity Monitoring (DAM) is a security solution used to monitor and analyze database activity for potential security threats or policy violations. DAM captures events in real-time, allowing organizations to detect and respond to suspicious activities and compliance violations. With the increasing volume and complexity of data and database systems, DAM has become essential in protecting sensitive information and ensuring regulatory compliance.

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.

# 1.1. Abbreviations

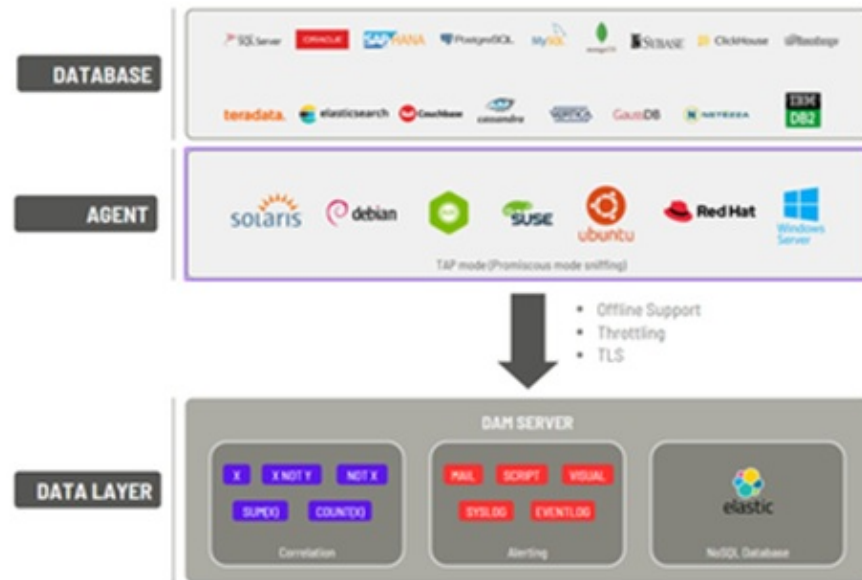
Abbreviations	Definition
DAM	Database Activity Monitoring
DSIM	DAM Installation Manager
DSPL	DAM Socket TAP Module
DSTAP	DAM TAP Module
LDAP	Lightweight Directory Access Protocol
OpenVAS	Open Vulnerability Assessment Scanner
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol

## 1.2. DAM Users and Roles

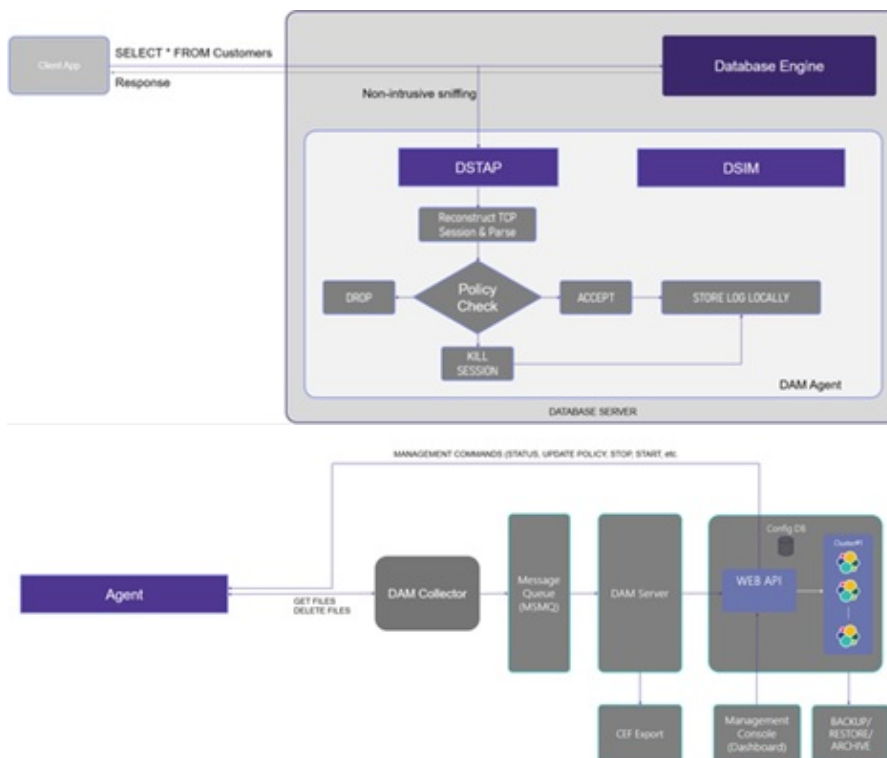
DAM has flexible user role management support that makes DAM available to create its roles depending on the privileges defined before. These roles are like groups in DAM. New roles can be created by admin, and users can be assigned to these roles. For more details, see [All Settings](#).

# 1.3. DAM Architecture

## System Architecture



## Logical Architecture





## 1.4. 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.

The login page for OpenText Database Activity Monitoring. It has a dark blue background with the 'opentext™ | Database Activity Monitoring' logo at the top. Below the logo are three input fields: 'Server Name', 'User Name', and 'Password'. There is a 'Remember me' checkbox below the password field. At the bottom is a 'Sign in' button.

3. Click **Sign In**.



### Note

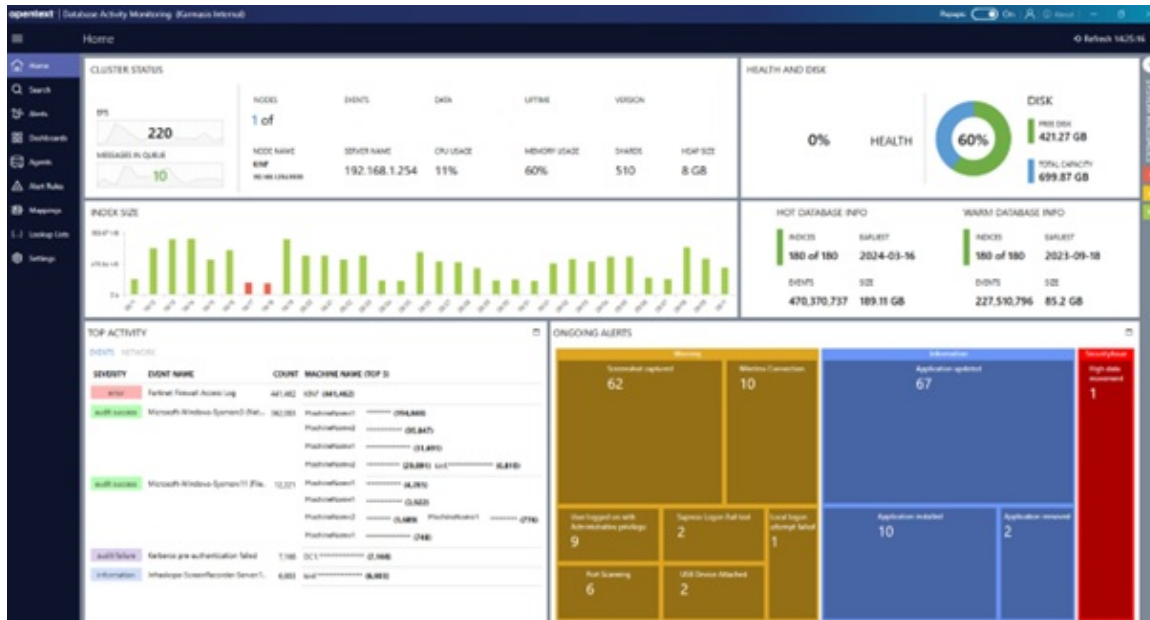
The Server Name field can be filled in 3 ways: localhost, Server IP, or Server hostname.



- 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.


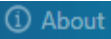

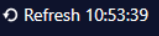

# 1.5. Console

## Menu and Controls

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

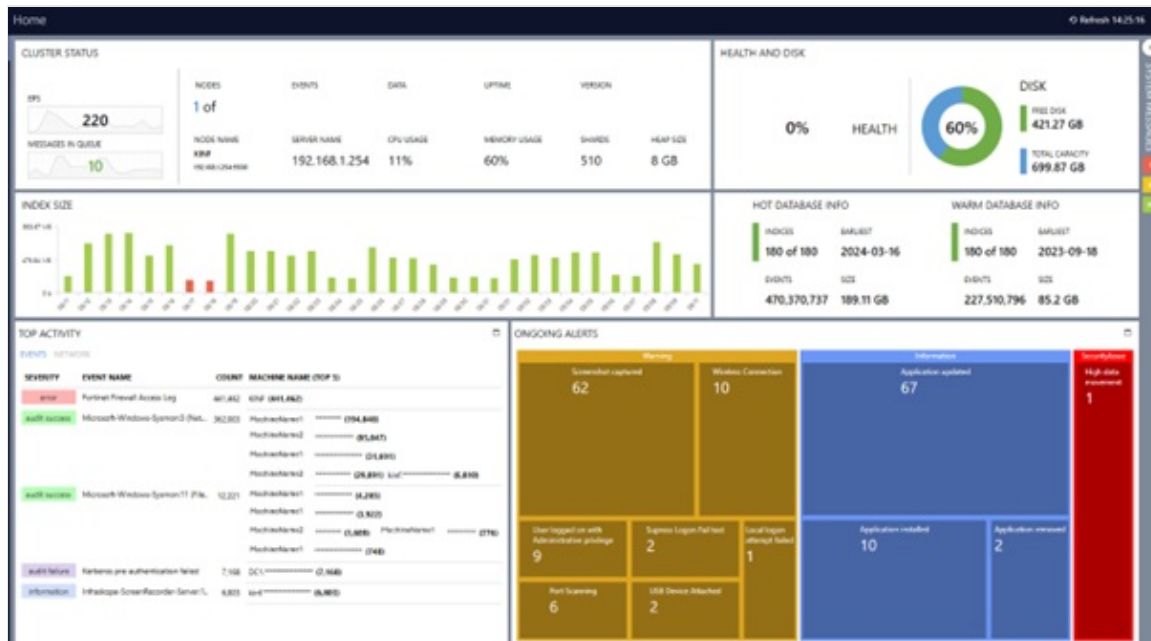


Menus	Function
Home	Used to display the home screen of DAM.
Search	Used to search events and export search results as xls or pdf.
Alerts	Used to view alerts in detail.
Dashboards	Used to view and edit dashboards.
Agents	Used to show Agents, Policies and Options tabs, and Refresh, New Agent, Edit, Delete, 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.
Lookup List	Used to show Lookup Lists.
Settings	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 <b>Logged On Users</b> , <b>My Profile</b> and <b>Logout</b> submenus.
	Used to show Copyright, Version, Disclaimer, Product, Client and License information
	Used to check updates
	Used to refresh.
	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.

## 1.5.1. 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.



## 1.5.1.1. Cluster Status

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

### CLUSTER STATUS

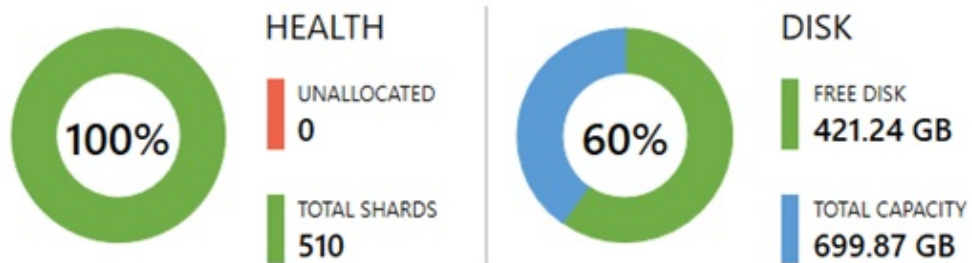


- **Nodes** shows the number of shards in the database (determined based on the system size).
- **Events** shows the number of events in the database.
- **Data** shows the record size.
- **Uptime** shows the system's active time period.
- **Version** shows database version number.
- **Node Name** shows 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, which 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.

## 1.5.1.2. Health and Disk

This panel shows information about cluster health and disk capacities.

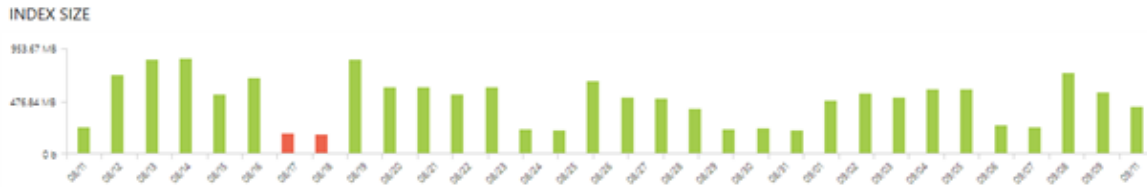
### HEALTH AND DISK



- **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.

## 1.5.1.3. 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.



## 1.5.1.4. 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. By 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
<b>180 of 180</b>	<b>2024-03-16</b>
EVENTS	SIZE
<b>470,388,139</b>	<b>189.12 GB</b>

### WARM DATABASE INFO

INDICES	EARLIEST
<b>180 of 180</b>	<b>2023-09-18</b>
EVENTS	SIZE
<b>227,510,796</b>	<b>85.2 GB</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.



## 1.5.1.5. 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)

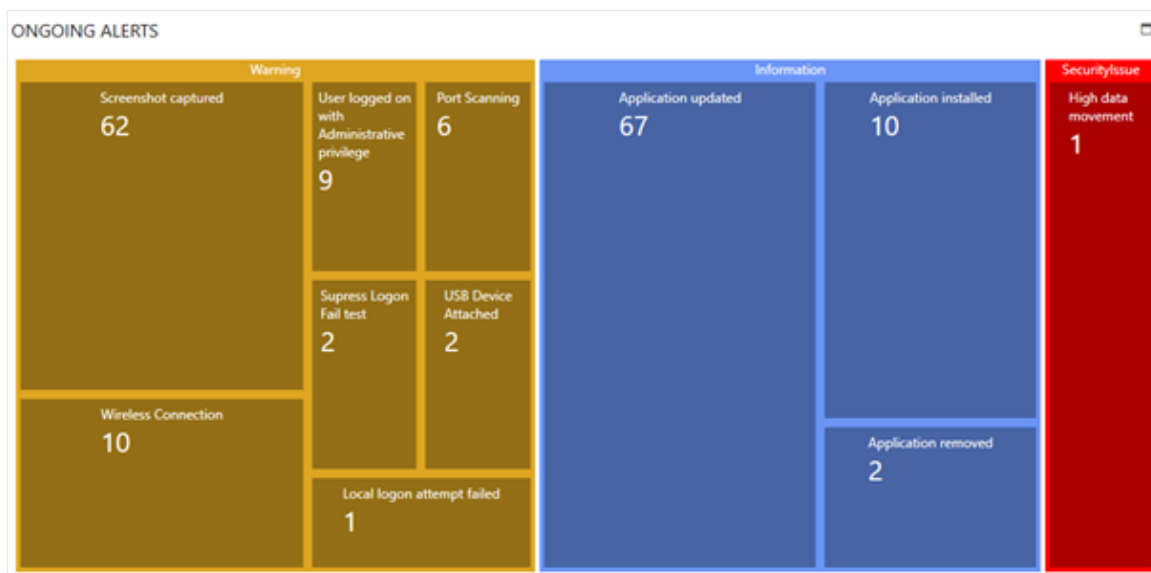
## 1.5.1.5.1. Events

- **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.

## 1.5.1.6. 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.

## 1.5.2. Search

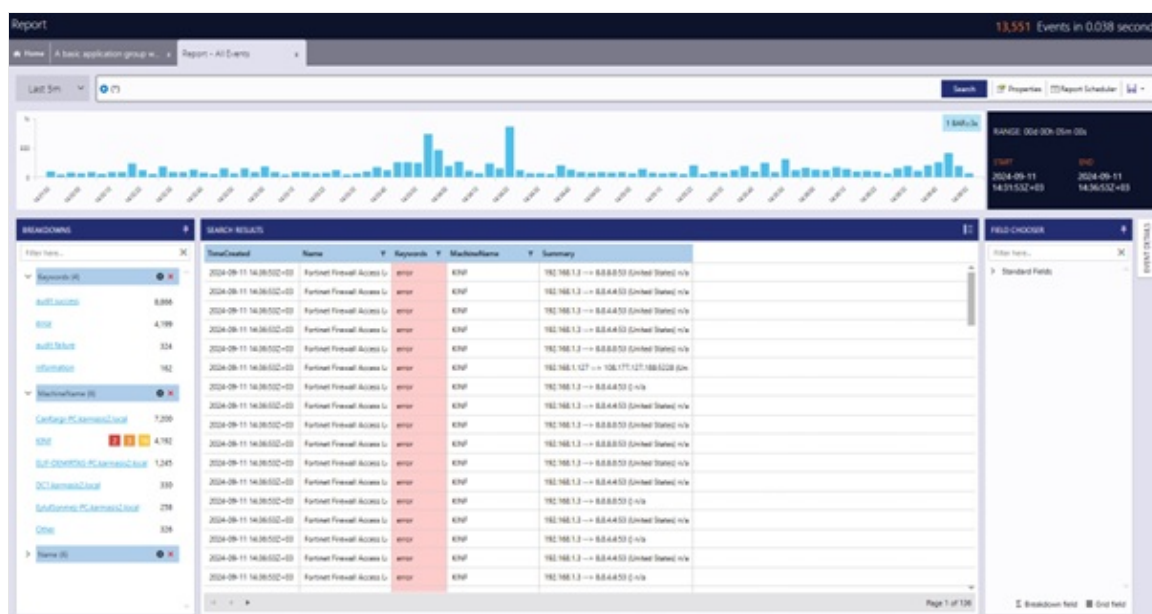
Search panel provides a search engine where user can examine event records in detail.

### 1.5.2.1. 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.

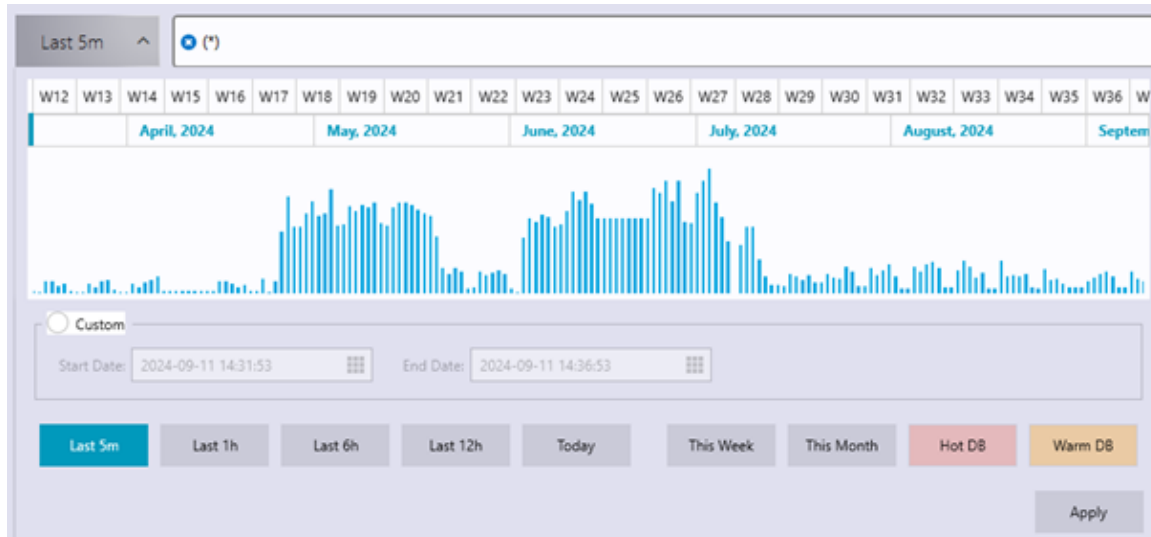
SEARCH

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



## 1.5.2.1.1. Date Range Section

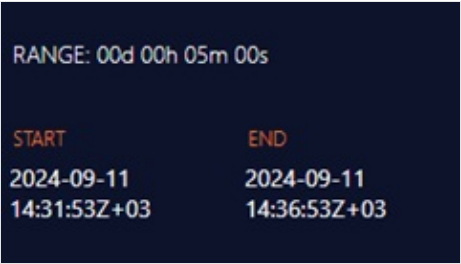
The date range section is automatically set to scan events that occurred within the last 5 minutes. Additionally, users can click on the relevant section to customize the date range according to their preferences.



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.

## 1.5.2.1.2. Range

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

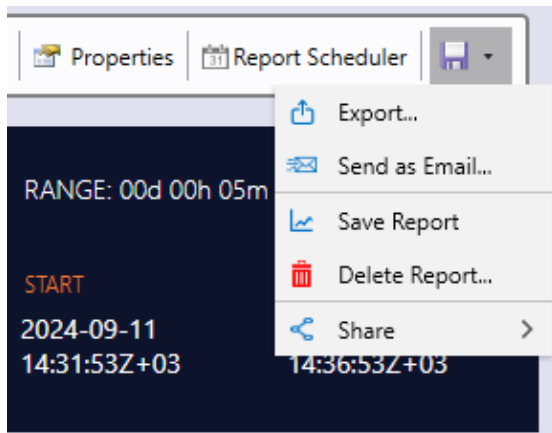


A screenshot of a dark-themed interface showing time range information. At the top, it says 'RANGE: 00d 00h 05m 00s'. Below this, there are two columns: 'START' and 'END'. The 'START' column shows '2024-09-11 14:31:53Z+03' and the 'END' column shows '2024-09-11 14:36:53Z+03'.

RANGE: 00d 00h 05m 00s	
START	END
2024-09-11 14:31:53Z+03	2024-09-11 14:36:53Z+03

## 1.5.2.1.3. 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.





## 1.5.2.1.4. Field Chooser

The screenshot displays the 'SEARCH RESULTS' table with columns: TimeCreated, Name, Keywords, MachineName, and Summary. The table contains 18 rows of data, all showing 'error' keywords and 'KINF' machine names. To the right, the 'FIELD CHOOSER' panel is visible, showing a search bar and a list of 'Standard Fields'.

TimeCreated	Name	Keywords	MachineName	Summary
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.127 -> 106.177.127.188 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.8.8 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a
2024-09-11 14:36:53Z+00	Fortinet Firewall Access U	error	KINF	192.168.1.3 -> 8.8.4.4 (United States) n/a

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:

The first screenshot shows the 'FIELD CHOOSER' panel with a search bar and a list of 'Standard Fields'. The second screenshot shows the 'FIELD CHOOSER' panel with a search bar and a list of 'Dynamic Fields'.





Field Name	Field Type	Field Icon
Category	Σ	≡
Channel	Σ	≡
DataLabel	Σ	≡
EventID	Σ	≡
EventSource	Σ	≡
Hash	Σ	≡
Keywords	Σ	≡
Level	Σ	≡
MachineName	Σ	≡
Name	Σ	≡
Severity	Σ	≡
Summary	Σ	≡
TimeCreated	Σ	≡
TimeInserted	Σ	≡
UserName	Σ	≡

Field Name	Field Type	Field Icon
1 sourceaddress	Σ	≡
2 srcip	Σ	≡
3 dstip	Σ	≡
4 srcport	Σ	≡
5 dstport	Σ	≡
6 action	Σ	≡
7 type	Σ	≡
8 subtype	Σ	≡
9 proto	Σ	≡
10 dstcountry	Σ	≡
11 srcmac	Σ	≡
12 facility	Σ	≡
13 severity	Σ	≡
14 date	Σ	≡
15 time	Σ	≡
16 devname	Σ	≡
17 devid	Σ	≡

**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.
	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 --> 8.8.8.8:53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.4.4:53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.8.8:53 (United States) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.3 --> 8.8.8.8:53 (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 f	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.119 --> 8.8.4.4:53 (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.

## 1.5.2.1.5. 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 L	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 L	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 L	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 L	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 L	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 L	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 L	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 L	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 L	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 L	error	KINF	192.168.1.3 --> 57.144.126.192:443 (France) n/a	
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	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 L	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.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)	
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysmon	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.134 (-)	

## 1.5.2.1.6. Breakdowns

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

BREAKDOWNS	
Filter here...	
Keywords (4)	
<a href="#">audit_success</a>	8,866
<a href="#">error</a>	4,199
<a href="#">audit_failure</a>	324
<a href="#">information</a>	162
MachineName (6)	
<a href="#">CanKargi-PC.karmasis2.local</a>	7,200
<a href="#">KINE</a>	4,192
<a href="#">ELIF-DEMIRTAS-PC.karmasis2.local</a>	1,245
<a href="#">DC1.karmasis2.local</a>	330
<a href="#">EylulSonmez-PC.karmasis2.local</a>	258
<a href="#">Other</a>	326
Name (6)	
<a href="#">Microsoft-Windows-Sysmon3 (Network Co...</a>	
<a href="#">Fortinet Firewall Access Log</a>	

## 1.5.2.2. 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.

SEARCH

Search here or filter predefined queries and reports...

SEARCH

EXISTING ASSETS

QUERIES (574) REPORTS (92)

NAME	TAG	QUERY
A basic application group was changed		EventID:4784 AND EventSource:"Microsoft Windows Security Auditing"
DATABASE BACKUP ERROR		EventSource:"SQLServer-Audit" AND EventID:1545 AND category:"BACKUP" AND result:"Database backed up!"
A basic application group was created		EventID:4783 AND EventSource:"Microsoft Windows Security Auditing"
A basic application group was deleted		EventID:4789 AND EventSource:"Microsoft Windows Security Auditing"
A certificate request extension changed		EventID:4873 AND EventSource:"Microsoft Windows Security Auditing"
A Certificate Services template was updated		EventID:4889 AND EventSource:"Microsoft Windows Security Auditing"
A change was made to IIS settings		EventID:5040 AND EventSource:"Microsoft Windows Security Auditing"
A change was made to the Windows Firewall exception list		EventID:4946 AND EventSource:"Microsoft Windows Security Auditing"
A computer account was changed		EventID:4742 AND EventSource:"Microsoft Windows Security Auditing"
A computer account was created		EventID:4741 AND EventSource:"Microsoft Windows Security Auditing"
A computer account was deleted		EventID:4743 AND EventSource:"Microsoft Windows Security Auditing"
A configuration entry changed in Certificate Services		EventID:4881 AND EventSource:"Microsoft Windows Security Auditing"
A configuration entry changed in the OCP Responder Service		EventID:5123 AND EventSource:"Microsoft Windows Security Auditing"

### Reports

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

SEARCH

Search here or filter predefined queries and reports...

SEARCH

EXISTING ASSETS

QUERIES (574) REPORTS (92)

Filter reports here...

NAME	CATEGORY	QUERY	SCHEDULES
A basic application group was changed		EventID:4784 AND EventSource:"Microsoft Windows Security Auditing"	
All Events	All Event	*	
Custom All Events	All Event	*	
All Application Activity Logs	App Tracker	(EventID:6010 OR EventID:6011)	
All Application Usage Logs	App Tracker	EventID:6012	
All Test Edition Usage Logs	App Tracker	(EventID:6012 AND processname:"notepad" OR processname:"ultrima" OR processname:"ultra" OR processname:"Microsoft Wordpad")	
Application Activation	App Tracker	EventID:6010 AND EventSource:"trhskape"	
Application Activities With Admin Privileges	App Tracker	EventID:6010 AND windows:"Administrator"	
Inactive User - Scheduled Report	App Tracker	EventID:6012 AND processname:"LockApp.exe"	
Microsoft Office Usage Logs	App Tracker	EventID:6012 AND processname:"Microsoft Word" OR processname:"Microsoft Excel" OR processname:"Microsoft Outlook" OR processname:"Microsoft PowerPoint" OR processname:"Microsoft Access"	
Web Browser Activity	App Tracker	EventID:6011	

# 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:

Format:

Page Size:

Page Orientation:

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:

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

Deliminator: ☐ 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

Deliminator: ☐ 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: 02:00:00

☐ Between Specific Time: 02:00:00 02:00:00

Runs at 02:00 every day. Generates report for the previous day.

SAVE CANCEL

## 1.5.2.3. 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]

## 1.5.2.4. Regular Expression Queries

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

## 1.5.3. Alerts

The screenshot shows the 'Alerts' interface. At the top, there are filters for '2024-09-11 08:00:00' and '2024-09-11 20:00:00', a search bar, and an 'Actions' dropdown. Below this is a table of alerts with columns: Severity, State, Alert Time, Computer Name, Name, Suppress Count, and Message. The table lists several alerts, mostly 'Warning' and 'SecurityIssue' types, with states like 'New'. A detailed view of a selected alert is shown on the right, displaying fields like 'Event ID', 'Source', 'Category', 'Event Type', 'Machine Name', and 'Event Details'.

- **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:

The screenshot shows the alert list with a right-click context menu open over one of the rows. The menu options are: 'Change Resolution State...', 'Alert...', 'All...', 'Selected...', 'New', 'Acknowledged', 'Assigned To Helpdesk', 'Outsourced', and 'Resolved'.

### Change Resolution State Menu:

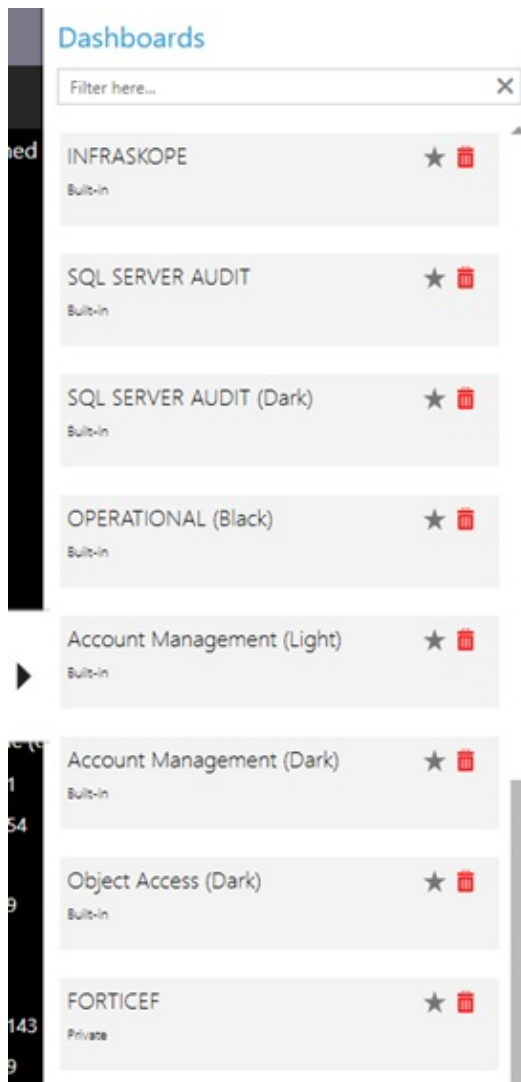
- **All:** Allows you to change the resolution state for all records.
  - **New:** Indicates a newly received alarm.
  - **Acknowledged:** Indicates that the alarm has been reviewed and acknowledged by the authorized person.
  - **Assigned to Helpdesk:** Indicates the assignment of the alarm to the helpdesk 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.
- **Alerts:**
  - **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 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.




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 <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> .

## 1.5.4.1. Edit Dashboard

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

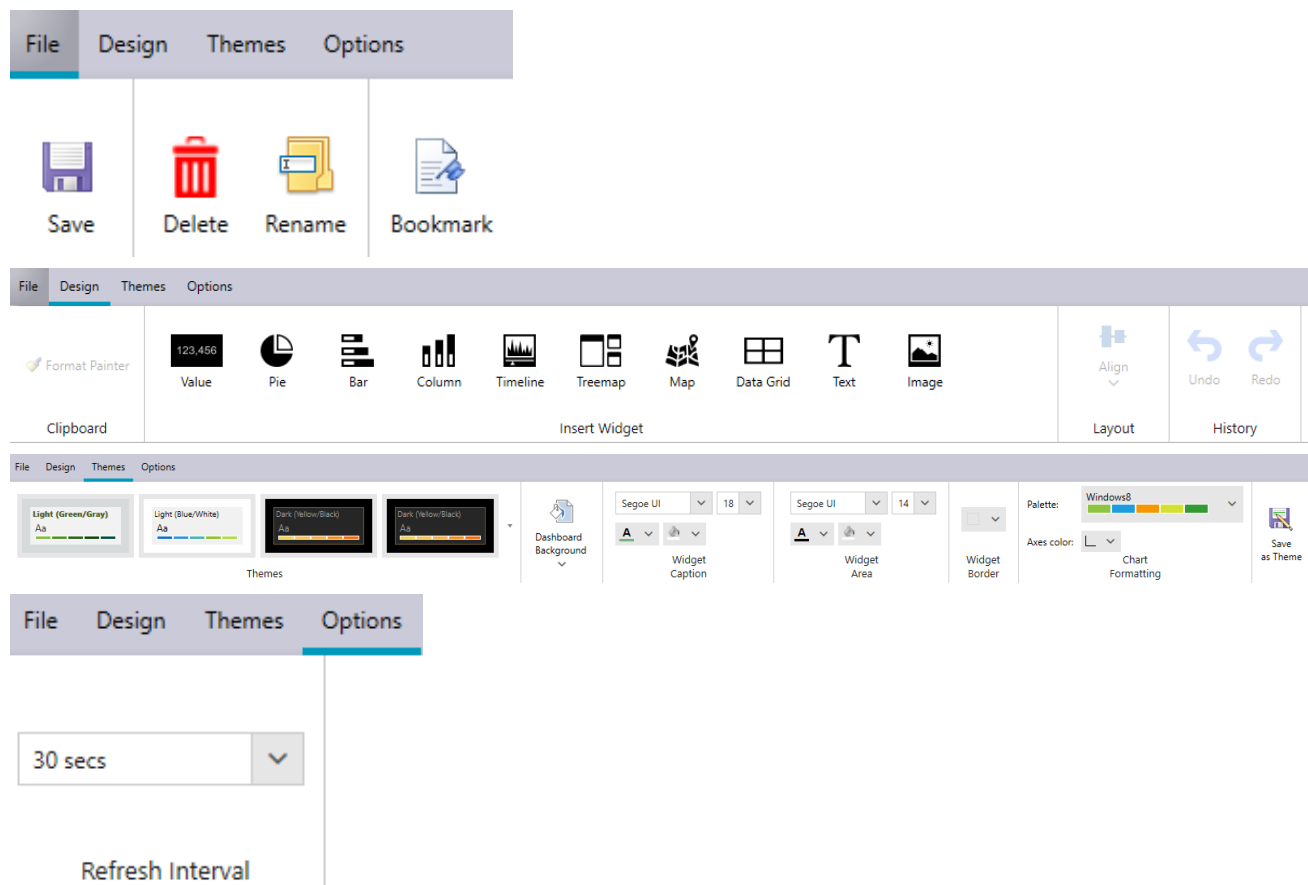
The **File** tab is used for **Save**, **Delete**, **Rename** and **Bookmark** operations.

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.

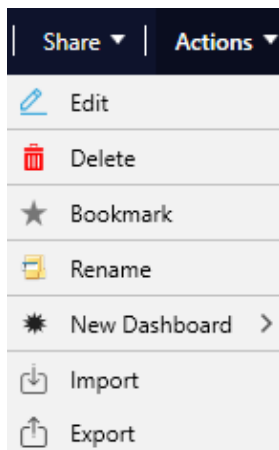
The **Themes** tab offers various **Theme Designs**. It also provides separate customization opportunities for **Background**, **Widget Caption**, **Widget Area**, **Widget Border** and **Chart Formatting**.

The **Options** tab allows the 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.



## 1.5.4.2. 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 one.
- **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:

<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 

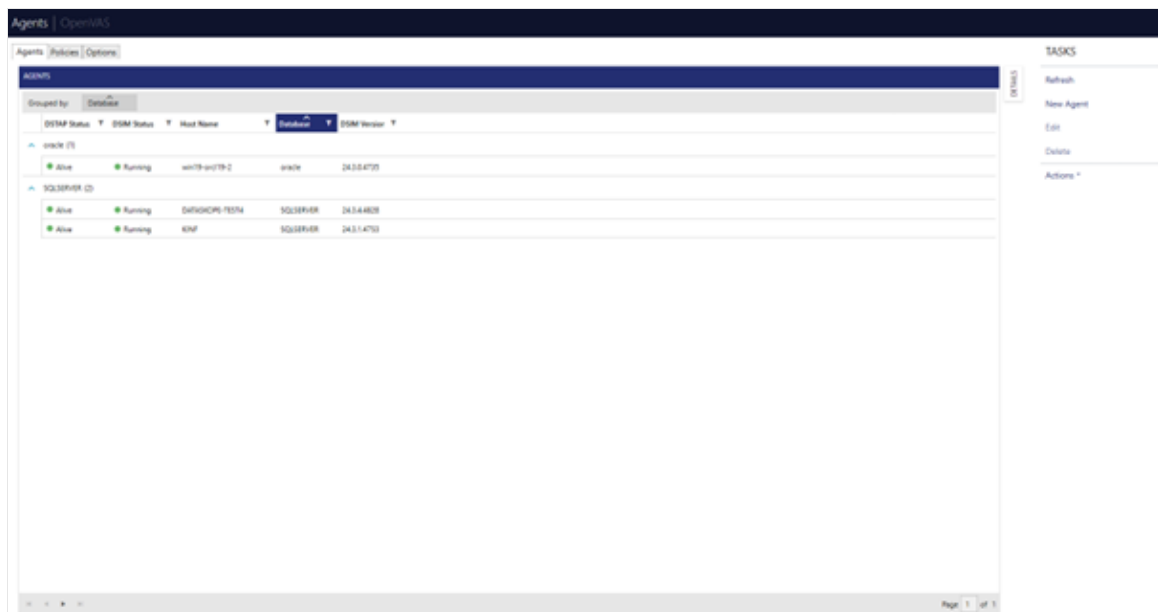
OK

CANCEL

## 1.5.5. Agents

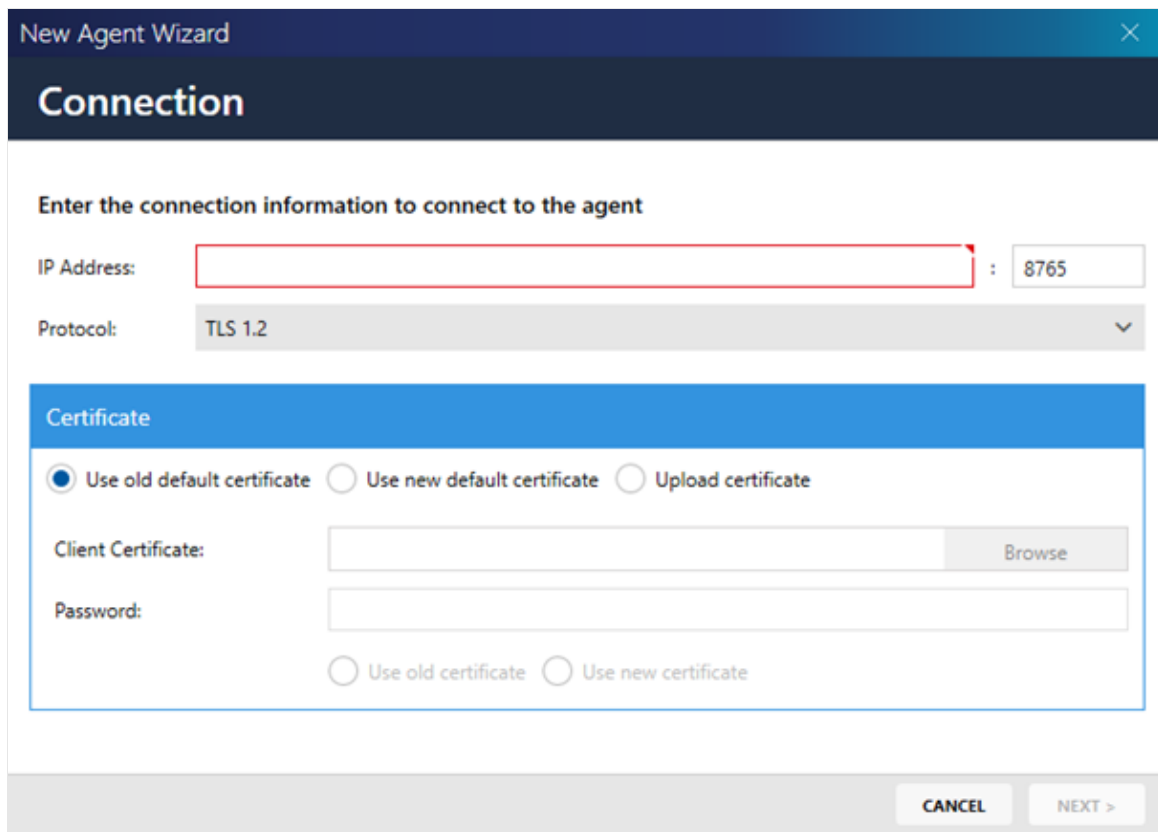
Agents Menu allows you to manage, monitor, and configure your agents. It consists of panels where users can define and modify settings for the agents installed on client machines. With **Agents**, **Policies**, and **Options** tabs.

- 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** [Close]

## Connection

Enter the connection information to connect to the agent

IP Address:  : 8765

Protocol: TLS 1.2 [v]

### Certificate

☒ Use old default certificate
 ☐ Use new default certificate
 ☐ Upload certificate

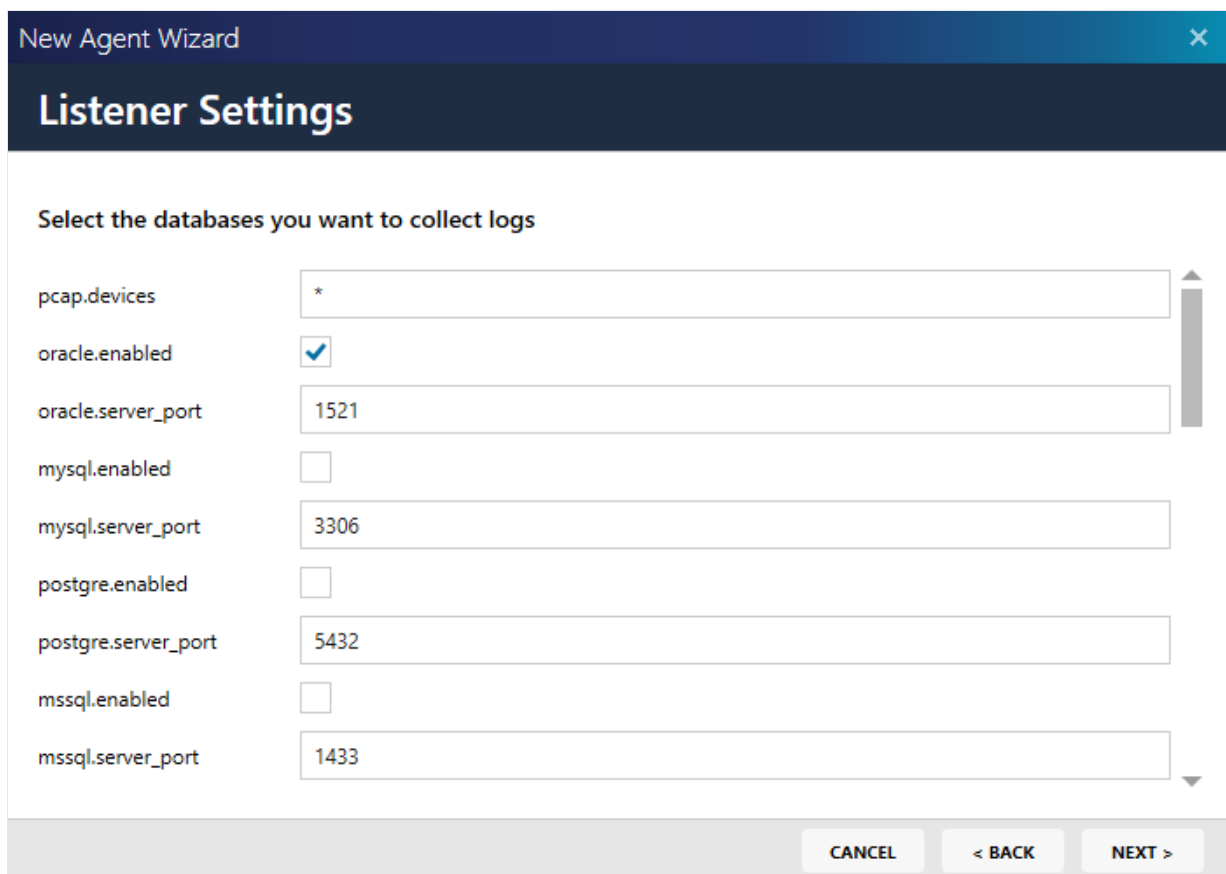
Client Certificate:  Browse

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** [Close]

## 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"/>

CANCEL < BACK NEXT >

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**.



New Agent Wizard

## Policy Settings

Choose a policy for the agent

Policy:

oracle - Dataskope Default Policy for Oracle Server

Selected Policy Rules:

```
64 kill|db_user|can|mert
65 +
66 kill|client_app_name|app1
67
68 ## kill unwanted
69 kill|client_ip|174.145.|205.195.
70
71 kill|db_user|can|mert
72
73
74 ##Default Allow Rule for Oracle
75 allow
76
77
```

CANCEL < BACK 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:

New cluster name

60

Max Idle Minutes:

Idle Threshold Minutes:

10

10

Suppress File Info Event Minutes:

Suppress Status Event Minutes:

1

60

Tag

Type a tag

CANCEL

< BACK

FINISH

## 1.5.5.1. 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 <b>Adding a New Agent</b> .
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.

## 1.5.5.2. Policies Tab

The screenshot shows the OpenVAS interface with the 'Policies' tab selected. The main area displays a table of policies, grouped by database. The table has three columns: Name, Database, and Description. The policies are listed for various databases including virtual-machine, couchbase, mongo, mysql, opensearch, and oracle. On the right, there is a TASKS sidebar with buttons for Refresh, New Policy, Edit, and Delete.

Name	Database	Description
(5)		
ckargi-virtual-machine Default		Default configuration
ckargi-virtual-machine Default (2)		Default configuration
ckargi-virtual-machine Default (3)		Default configuration
ckargi-virtual-machine Default (4)		Default configuration
db-test-machine Default (2)		Default configuration
couchbase (2)		
Dataskope Default Policy for Couchbase Sen	couchbase	This policy is read-only, and it captures and stores all the operations on Couchbase server. You can activate the example rules by deleting "R" character at the beginning of the rule criteria.
karmasshost Default (3)	couchbase	Default configuration
mongo (4)		
db-test-machine Default	mongo	Default configuration
ubuntutest Default (2)	mongo	Default configuration
ubuntutest Default (3)	mongo	Default configuration
ubuntutest Default (4)	mongo	Default configuration
mysql (1)		
db-test-machine Default (3)	mysql	Default configuration
opensearch (2)		
Dataskope Default Policy for OpenSearch Se	opensearch	This policy is read-only, and it captures and stores all the operations on OpenSearch server. You can activate the example rules by deleting "R" character at the beginning of the rule criteria.
mongoDB Default	opensearch	Default configuration
oracle (5)		
aix72_test Default	oracle	Default configuration
oracle-big-server Default	oracle	Default configuration
ubuntutest Default	oracle	Default configuration
win19-orcl19-2 Default	oracle	Default configuration

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.

New Policy

Name \*

Database \*

Select database type

Description

Rules

1

TEST RULE

IMPORT

SAVE

CANCEL

## 1.5.5.3. Options Tab

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 | OpenVAS

Agents | Policies | Options

Default Certificate

Used for agents of version 3.2.0.4084 and higher

Agent Security Certificate (.cert) \*

dim\_server.cert file selected. Remove

Agent Key File (.key) \*

dim\_server.key file selected. Remove

Client Certificate \*

dim\_client.pem file selected. Remove

Password \*

\*\*\*\*\*

SAVE CANCEL

Old Default Certificate

Used for agents older than version 3.2.0.4084

Certificate \*

dim\_client.pem file selected. Remove

Password \*

\*\*\*\*\*

SAVE CANCEL

## 1.5.6. Alert Rules

Alert and Correlation Rules List of rules containing "en" keyword

All Categories

- Real Time Alerts
  - Logon Alerts
  - Account Management
  - Group Management
  - Application Management
  - TCP/IP
  - Correlation Rules
  - Process Tracking
  - APT Rules
  - Lookup List Examples
  - Tunneling Apps
  - Service Availability
  - MissedRule
  - DatakeopsSQL
  - Track Logged on Users
  - Threat Intelligence
  - Rages Test
  - SMS Test
  - Fortigate
  - DAM Use Case Alerts
- THIS RULE SET WILL BE PUBLISHED
- Test Syslog Forward
- EGM Rule Set
- Test2
- New Category
- New Category
- Repository

Real Time Alerts

Enabled	Severity	Name	Update Date	Contains In Keyword	Y
<input type="checkbox"/>	Warning	Policy violation	2023-11-02 21:29:20	<input type="checkbox"/>	
<input type="checkbox"/>	Warning	Hardware Configuration Changed	2023-11-02 21:48:51	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Warning	Low disk space	2023-08-22 11:06:30	<input type="checkbox"/>	
<input type="checkbox"/>	Warning	HP Mouse takıldı	2018-01-08 13:40:44	<input type="checkbox"/>	
<input type="checkbox"/>	Warning	Takip Edilen Kelime Kullanımı	2022-08-15 10:42:45	<input type="checkbox"/>	
<input type="checkbox"/>	Warning	Hardware Configuration Changed (copy)	2023-01-28 00:22:33	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Warning	New Pattern Halt	2024-08-07 15:13:49	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Warning	New Pattern	2024-08-19 14:56:10	<input type="checkbox"/>	

New Category...

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

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.

## 1.5.6.1. 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 in 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 the selected **Alert Rule Type**.
6. Click the **OK** button to add the created alert rule.

The screenshot shows the 'Pattern Editor' dialog box with the 'New Pattern' tab selected. The 'Name' field is set to 'New Pattern'. The 'Severity' is set to 'Warning' and the 'Category' is set to 'Real Time Alerts'. The 'Enabled' checkbox is checked. The 'All rules must occur within' field is set to '00:00:05'. The 'Activity' field is set to '00:00:00' to '23:59:59'. The 'Suppress all subsequent matches for' field is set to '00:00:00'. The 'Suppress by event params' checkbox is unchecked. The 'Event params to include' field is empty. The 'Rules' tab is selected, showing a table with columns 'Name', 'Type', and 'Description'. The 'Add Rule' button is visible, and a dropdown menu is open showing three options: 'Generic Rule' (Respond to a single event), 'Missed Rule' (Respond to an event that does not happen within given interval), and 'Multi-hit Rule' (Respond to an event that will occur more than N times within given interval). The 'OK' and 'CANCEL' buttons are at the bottom right.

Name	Type	Description
------	------	-------------

**Add Rule** ^

- Generic Rule**  
Respond to a single event
- Missed Rule**  
Respond to an event that does not happen within given interval
- Multi-hit Rule**  
Respond to an event that will occur more than N times within given interval

OK CANCEL



## 1.5.6.1.1. Generic Rule

Generic Rule type is used to respond to a single event. Users 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.

The screenshot displays the 'Rule Editor' window with the 'New Rule' tab selected. The window contains several input fields: 'Name' (containing 'New Rule'), 'Criteria' (a large text area), 'Correlation Key' (containing 'Enter correlation key'), and 'Description' (containing 'Enter description'). To the right of the 'Criteria' field is a table with columns 'Event ID' and 'Source'. Below this table is another table with columns 'Parameter' and 'Name'. At the bottom right of the window are 'OK' and 'CANCEL' buttons. A 'Criteria Helper' dialog box is open over the 'Criteria' field, displaying a list of queries under the heading 'Simple Queries'. The queries are: 'EventID = 1234 AND Source = 'Event Source here'', '(EventID = 1234 OR EventID = 5678) AND param1 like 'Saxxon%', 'EventID = 1234 AND Source = 'Event Source here' AND param1 NOT IN (lookupidname)', and 'EventID = 1234 AND Source = 'Event Source here' AND listcontains(lookupidname param2) = true'. The dialog also has 'OK' and 'CANCEL' buttons at the bottom.

Rule Editor  
New Rule

Name: New Rule

Criteria:

Correlation Key: Enter correlation key

Description: Enter description

Event ID Source

Parameter Name

OK CANCEL

Rule Editor  
New Rule

Name: New Rule

Criteria:

Correlation Key: Enter correlation key

Description: Enter description

Event ID Source

Criteria Helper

Simple Queries

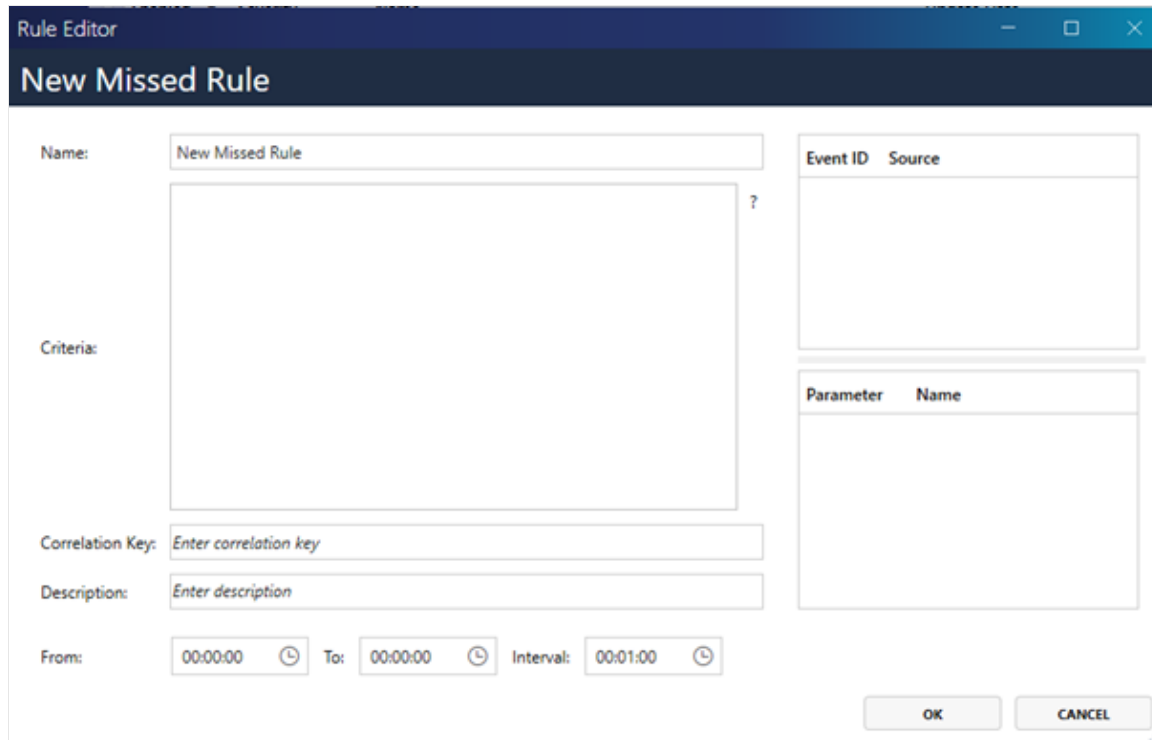
- EventID = 1234 AND Source = 'Event Source here'
- (EventID = 1234 OR EventID = 5678) AND param1 like 'Saxxon%'
- Lookup Lists Usage
- EventID = 1234 AND Source = 'Event Source here' AND param1 NOT IN (lookupidname)
- EventID = 1234 AND Source = 'Event Source here' AND listcontains(lookupidname param2) = true

OK CANCEL

## 1.5.6.1.2. 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 form contains the following fields and sections:

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

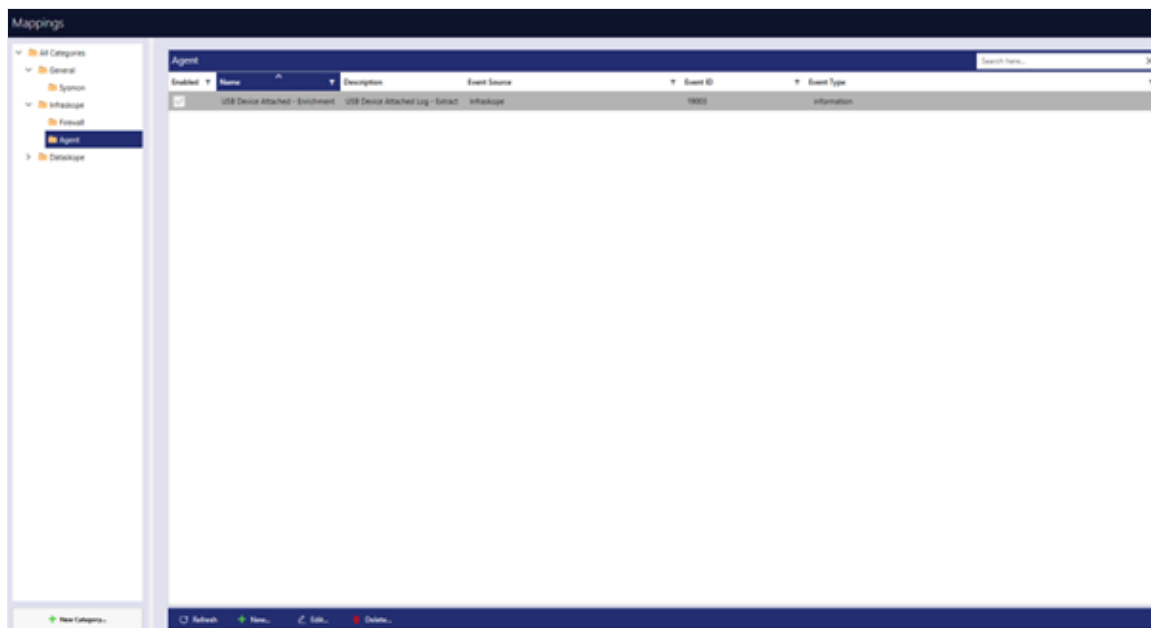
## 1.5.6.1.3. Multi-hit Rule

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 field containing 'New Multi-hit Rule'.
- Criteria:** A large empty text area for defining the criteria.
- Correlation Key:** A text field with the placeholder 'Enter correlation key'.
- Description:** A text field with the placeholder 'Enter description'.
- Group By Key:** A text field with the placeholder 'Enter group by key'.
- Interval:** A text field containing '00:00:30' with a clock icon for time selection.
- Match Condition:** A text field containing the SQL expression 'COUNT() >= 100'.
- Event ID Source Table:** A table with columns 'Event ID' and 'Source'.
- Parameter Name Table:** A table with columns 'Parameter' and 'Name'.
- Buttons:** 'OK' and 'CANCEL' buttons at the bottom right.

## 1.5.7. 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.

## 1.5.7.1. 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:  Event Source  Event Type

Input  Code  Output

```
1 //Special characters (.,,.,.) are not allowed in field names
2 //InfraskopeServer will automatically drop events if returned false
3 bool Map(ElasticContext ev)
4 {
5     return true;
6 }
```

☒ Enabled

SAVE CLOSE

## 1.5.8. Lookup Lists

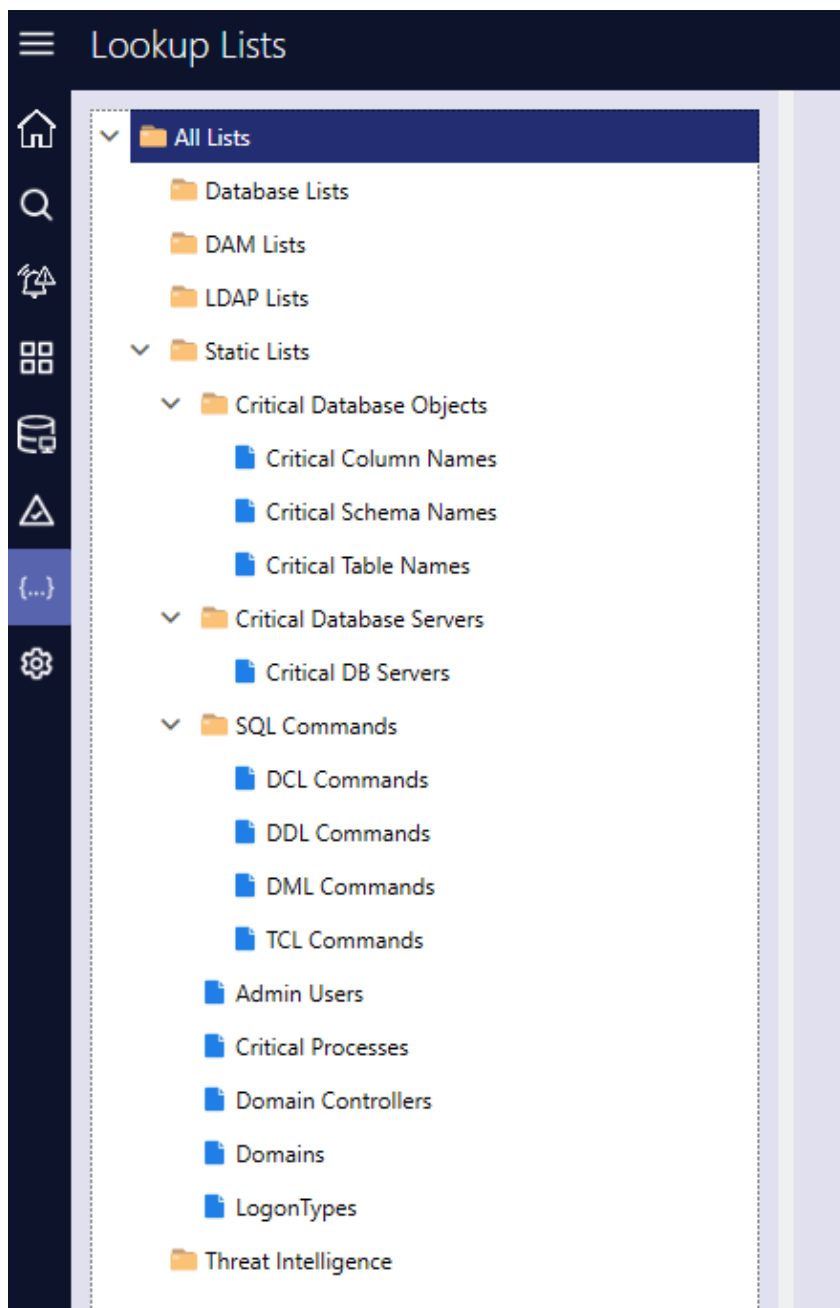
Lists that are used to modify the outputs of goals and are specifically tailored to the situation. These lists customize the outputs of goals, thereby increasing the accuracy of the outputs.

### **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.
- DAM List: Used to add lists to DAM policies.
- Database List: Used to customize database outputs.
- LDAP List: Used to customize LDAP outputs.



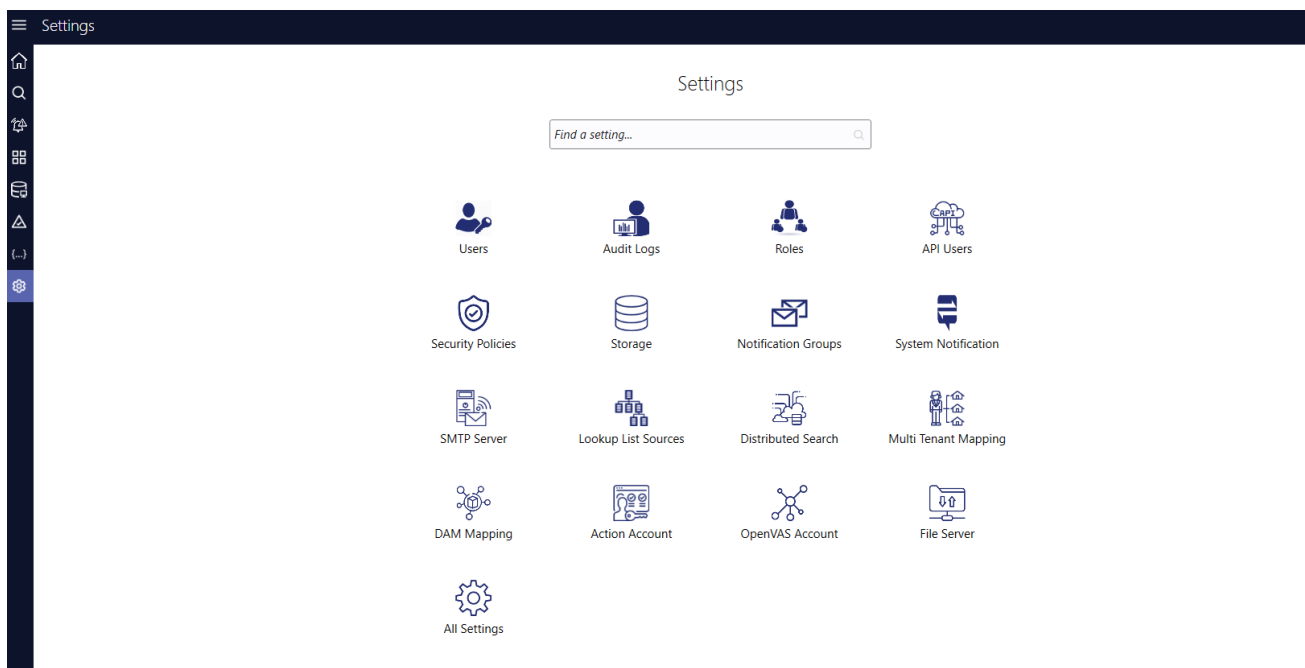
Clicking the Save button after each change to the list disables the automatic submission process, giving users the option to submit their modifications directly.











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

**Note**








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

## 1.5.9. Settings



Ref.	Controls	Function
	Users	Used to create, update, and delete users.
	Audit Logs	Used to view audit logs.
	Roles	Used to create, update, and delete roles.
	API Users	Used to create, update, and delete API Users.
	Security Policies	Used to change security policy 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.
	Lookup List Sources	Used to change Lookup List Source settings.



	Action Account	Used to reach account information by DAM agents.
	Distributed Platform	Used to create, update, and delete distributed platform settings.
	Multi-Tenant Mapping	Used to create, update, and delete multi-tenant mappings.
	DAM Mapping	Used to create, update, and delete VDAM Mappings
	OpenVAS Account	Used to OpenVAS API connection management.
	File Server	Used to create or delete file server.
	All Settings	Used to create, update, and delete DAM registry settings.

## 1.5.9.1. User Settings

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

The screenshot shows the 'Users' management page in the OpenText Database Activity Monitoring application. The interface includes a dark sidebar with navigation icons and labels: Home, Users, User Activities, and Roles. The main content area is titled 'Users' and contains a description: 'Manage user accounts by viewing, editing, and organizing roles, login permissions, and user activity details'. Below the description are action buttons: Refresh, New..., Edit..., and Delete... A table lists the existing users with columns for Login Enabled, Name, User Name, Roles, Email, Last Password Change Time, and Last Login Time. The table contains one entry for 'Log Admin'.

Login Enabled	Name	User Name	Roles	Email	Last Password Change Time	Last Login Time
<input checked="" type="checkbox"/>	Log Admin	logadmin	Admin	logadmin@ReplaceMe.local	-	2024-12-17 02:46:08

# 1.5.9.1.1. Adding New User

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

The image displays three sequential screenshots of the 'New User' configuration window, illustrating the different tabs available for user setup.

- General Tab (Left):** This tab contains fields for 'User Information' (Name, Email, Mobile Phone, SMS Number), 'Account Information' (User Name, Active checkbox, Expiry on, Use Database checkbox), 'Authentication' (Set Random Password, Password, Confirm Password, Should change password on next login checkbox), and 'User Inactivity' (Inactivity Logout checkbox). It includes 'SAVE' and 'CANCEL' buttons at the bottom.
- Roles Tab (Middle):** This tab shows a list of roles with checkboxes for selection. The roles listed are Admin, Users, Database, TestDefault, Database Group, Sales, J2SE, Web API, TestUtil, Read-Only User, Company1, Company2, Company3, Admin Role Test, Test, BDM TEST - ADMIN ROLE, and BDM TEST - USER ROLE. It includes 'SAVE' and 'CANCEL' buttons at the bottom.
- Notification Groups Tab (Right):** This tab shows a list of notification groups with checkboxes for selection. The groups listed are DefaultOps, Security Ops, User, Task, MRPD Ops, Test, Dev, Dev2, BDM TEST, and Schedule Test Group. It includes 'SAVE' and 'CANCEL' buttons at the bottom.

## 1.5.9.2. Audit Logs 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.

**Audit Logs**  
Monitor and analyze user activities and access logs

2025-07-08 00:00:00 2025-07-08 23:59:59 Search here... ☒ User Logs ☐ API 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
2025-07-08 04:39:29	WIN-8PIDOL34216	Administrator	::1	Log Admin	User Activities
2025-07-08 04:39:27	WIN-8PIDOL34216	Administrator	::1	Log Admin	Operations
2025-07-08 04:39:24	WIN-8PIDOL34216	Administrator	::1	Log Admin	Event Descripti
2025-07-08 04:39:24	WIN-8PIDOL34216	Administrator	::1	Log Admin	Queries
2025-07-08 04:39:23	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunction
2025-07-08 04:39:21	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunction
2025-07-08 04:39:21	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunctions
2025-07-08 04:39:21	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunctions
2025-07-08 04:39:20	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunctions
2025-07-08 04:39:20	WIN-8PIDOL34216	Administrator	::1	Log Admin	Mappings
2025-07-08 04:39:20	WIN-8PIDOL34216	Administrator	::1	Log Admin	AuditDB
2025-07-08 04:39:19	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunctions
2025-07-08 04:39:19	WIN-8PIDOL34216	Administrator	::1	Log Admin	Intelli Search
2025-07-08 04:39:19	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunctions
2025-07-08 04:39:19	WIN-8PIDOL34216	Administrator	::1	Log Admin	Cross Platform Se
2025-07-08 04:39:19	WIN-8PIDOL34216	Administrator	::1	Log Admin	ElasticFunction

Page 1 of 1 | 45 Total

**ACTIVITY DETAILS**

```
{
  "Service": "Login",
  "Action": "Logon",
  "Parameters": {
    "UserName": "logadmin",
    "ServerName": "WIN-8PIDOL34216",
    "LogonTime": "2025-07-08T03:45:50.1102154-07:00",
    "Status": "Success"
  }
}
```

Session ID: **a1d40a6-181c-4fcb-ad8f-0ba5245f6339** [Minimize](#)





Computer Name: **WIN-8PIDOL34216** OS User Name: **Administrator**

IP Address: **::1** Operator: **Log Admin**

Service: **Login** Action: **Logon**

## 1.5.9.3. 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.

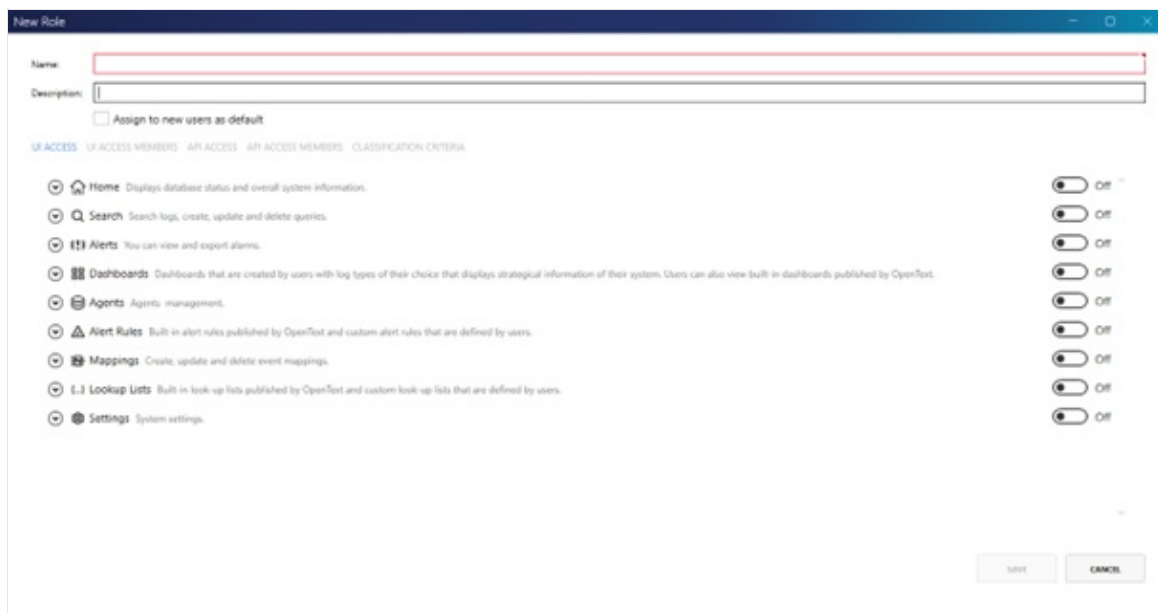
Roles			
 Refresh  New...  Edit...  Delete...			
Default	Outside Connection	Role Name	Description
<input type="checkbox"/>	<input type="checkbox"/>	Admin	This role has access to all features.
<input type="checkbox"/>	<input type="checkbox"/>	Admin Role Test	
<input type="checkbox"/>	<input type="checkbox"/>	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

## 1.5.9.3.1. Adding a New Role

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

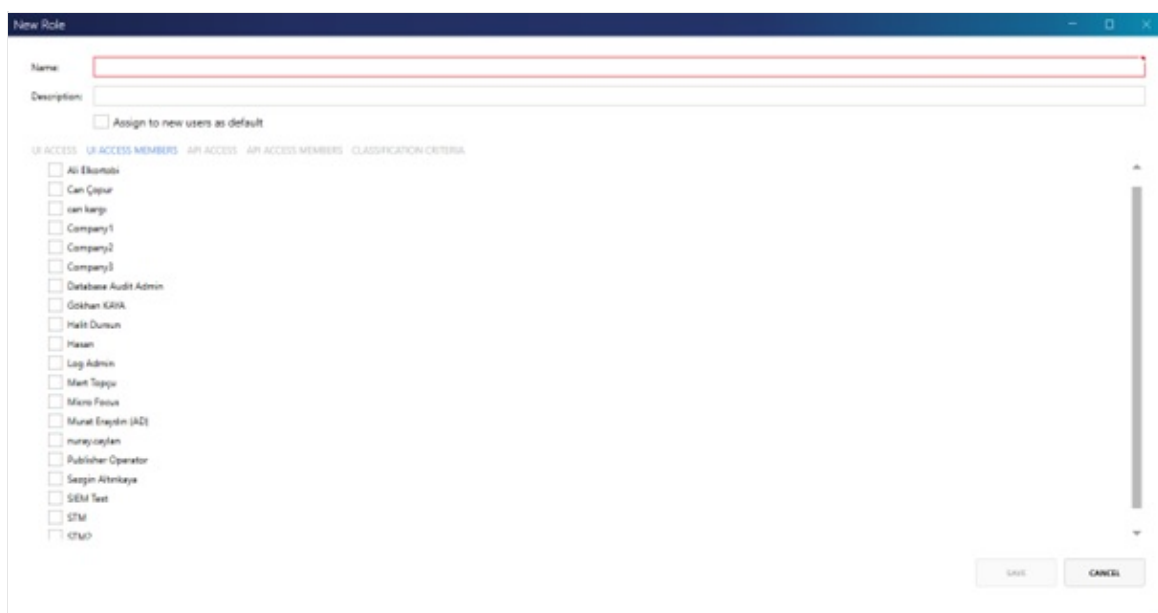
To add a New role, click New button on the **Roles Settings**.

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.



The screenshot shows the 'New Role' dialog box with the 'UI ACCESS' tab selected. The 'Name' field is highlighted with a red border. Below it is the 'Description' field and a checkbox for 'Assign to new users as default'. The 'UI ACCESS' tab is active, showing a list of system components with toggle switches to the right. The components and their toggle states are: Home (On), Search (On), Alerts (On), Dashboards (On), Agents (On), Alert Rules (On), Mappings (On), Lookup Lists (On), and Settings (On). The 'SAVE' and 'CANCEL' buttons are at the bottom right.

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



The screenshot shows the 'New Role' dialog box with the 'UI ACCESS MEMBERS' tab selected. The 'Name' field is highlighted with a red border. Below it is the 'Description' field and a checkbox for 'Assign to new users as default'. The 'UI ACCESS MEMBERS' tab is active, showing a list of users with checkboxes to the left. The users listed are: Ali Ekrem, Can Çipni, can kargi, Company1, Company2, Company3, Database Audit Admin, Gözhan KARAK, Hakkı Dursun, Hasan, Laga Admin, Mark Topçu, Merve Fırat, Murat Enaydin (ADE), mureyca/ten, Publisher Operator, Sezgin Altinkaya, SETH Test, STH, and STH2. The 'SAVE' and 'CANCEL' buttons are at the bottom right.

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

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

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

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

New Role

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 Filters +

✖ Must NOT Filters +

☐ Raw Query String

Company Name:

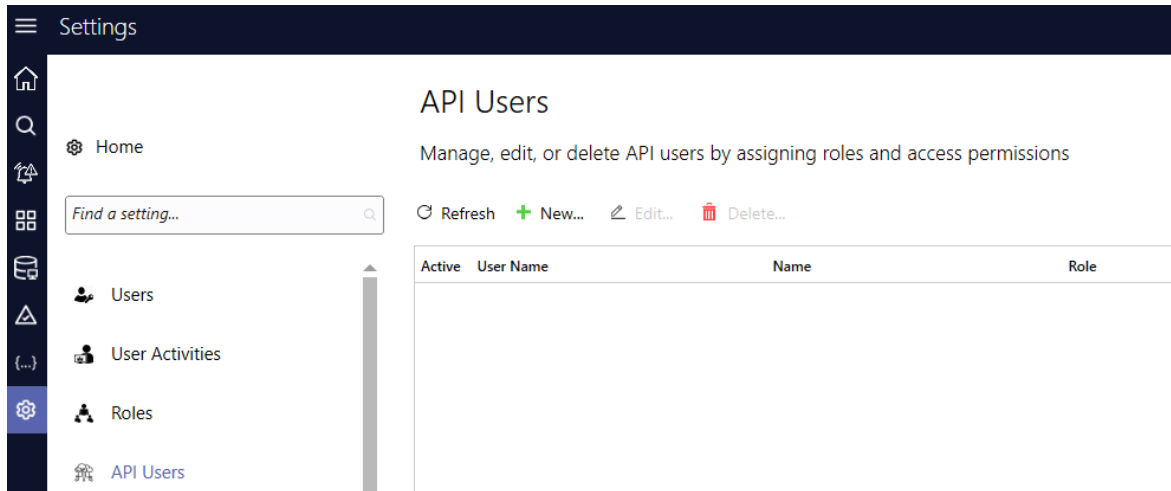
SAVE

CANCEL



## 1.5.9.4. API Users Settings

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



### 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.

The 'New User' dialog box is shown. It has a title bar 'New User' with close and maximize buttons. The form is divided into two sections: 'Account Information' and 'Authentication'. In the 'Account Information' section, there are input fields for 'Name:' and 'User Name:', a 'Role:' dropdown menu, and two checkboxes: 'Active' (unchecked) and 'Expires on' (checked). The 'Expires on' checkbox is followed by a date input field with the placeholder 'Enter date' and a calendar icon. The 'Authentication' section has a 'Password:' label and a password input field with a key icon and a copy icon. At the bottom are 'SAVE' and 'CANCEL' buttons.

**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.

## 1.5.9.5. Security Policies Settings

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

The screenshot shows the 'Settings' application interface. On the left is a dark sidebar with a menu containing icons and labels: Home, Users, Audit Logs, Roles, API Users, Security Policies (highlighted in blue), Storage, Notification Groups, System Notification, SMTP Server, Lookup List Sources, Distributed Search, and Multi Tenant Mapping. Above the menu is a search bar labeled 'Find a setting...'. The main content area has a dark header bar with a hamburger menu icon and the word 'Settings'. Below this, the 'Security Policies' section is titled, followed by the subtitle 'Configure password policies and session management to protect user accounts'. The settings are organized into three sections: 'Password Complexity' with four checked checkboxes (Require digit, Require lowercase, Require special characters, Require uppercase) and a 'Minimum length' input field set to 8; 'Password Expiration' with a checked 'Enforce password expiration' checkbox, an 'Interval (in months)' dropdown set to 3, and an unchecked 'Enforce password history' checkbox; and 'Session Management' with an unchecked 'Disable concurrent sessions' checkbox. A vertical scrollbar is visible on the left side of the main content area.

Settings

Home

Find a setting...

Users

Audit Logs

Roles

API Users

Security Policies

Storage

Notification Groups

System Notification

SMTP Server

Lookup List Sources

Distributed Search

Multi Tenant Mapping

### Security Policies

Configure password policies and session management to protect user accounts

#### Password Complexity

- ☒ Require digit
- ☒ Require lowercase
- ☒ Require special characters
- ☒ Require uppercase

Minimum length

8

#### Password Expiration

Users must change their password after the specified time interval

- ☒ Enforce password expiration

Interval (in months)

3

When enabled, users cannot reuse their last N passwords

- ☐ Enforce password history

Password history length

3

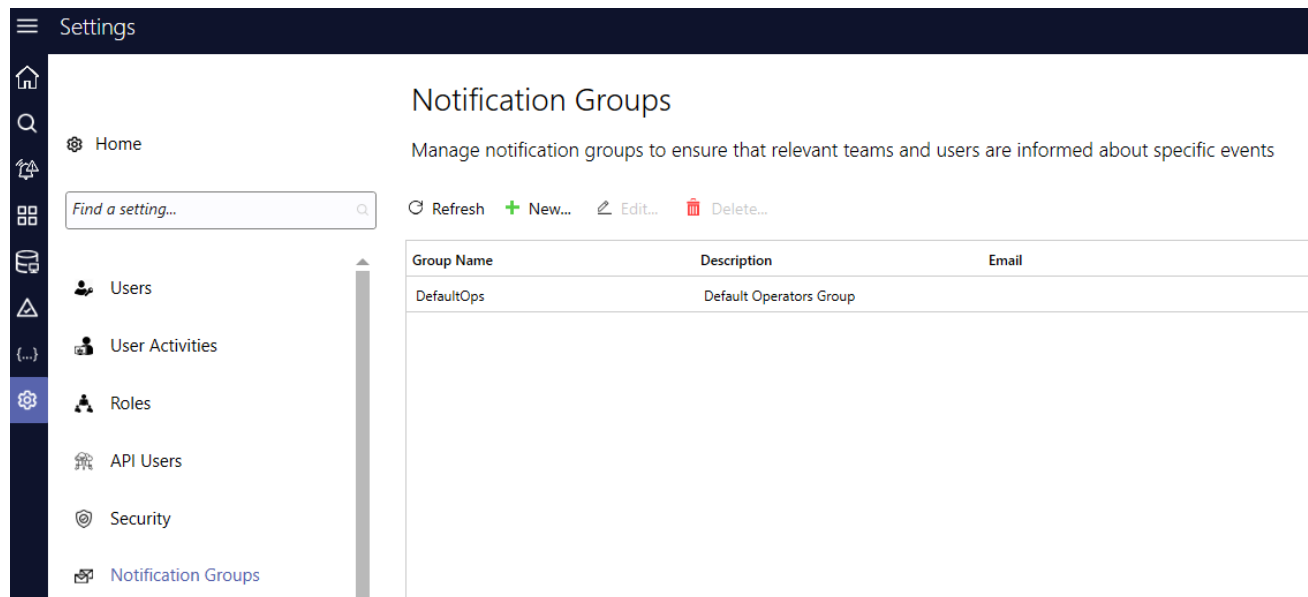
#### Session Management

Prevent the same user from being signed in on multiple devices simultaneously

- ☐ Disable concurrent sessions

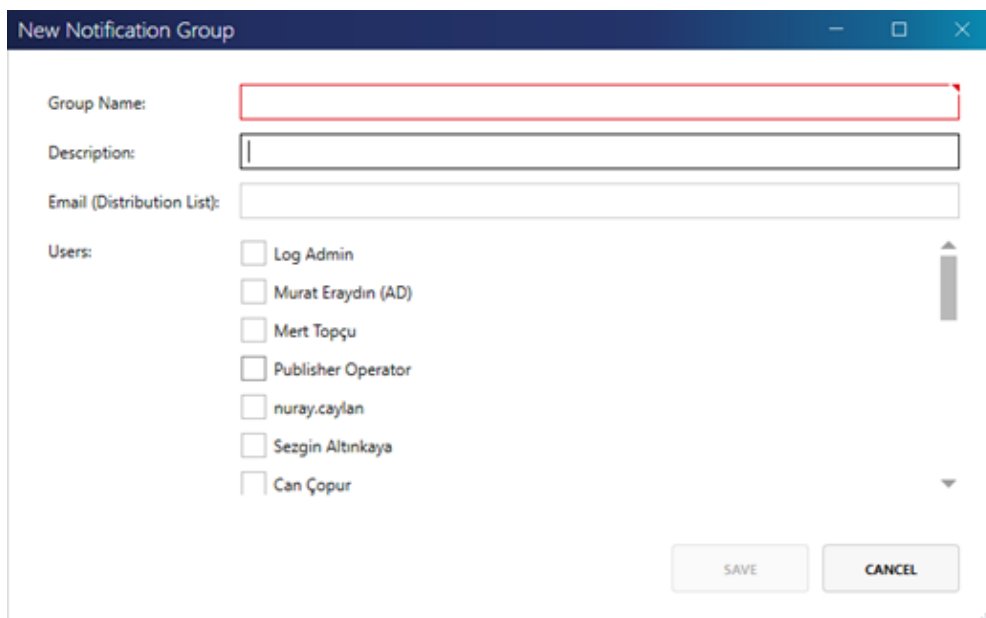
## 1.5.9.6. Notification Group Settings

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



## Adding a New Notification Group

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



## 1.5.9.7. Storage Settings

### Main Storage Settings

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

### Storage Security Settings

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

#### Storage

Manage data capacity, schedule backup and archiving processes, and notify administrators

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

Manage data capacity, schedule backup and archiving processes, and notify administrators

SETTINGS SECURITY **IMPORT ARCHIVE** RESTORE FROM BACKUP CURATOR SETTINGS

2024-12-14		2024-12-14		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

Manage data capacity, schedule backup and archiving processes, and notify administrators

SETTINGS SECURITY IMPORT ARCHIVE **RESTORE FROM BACKUP** CURATOR SETTINGS

🔄 Refresh

[Create & Restore All](#)

No missing or corrupted index found.

# Storage Curator Settings

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

## Storage

Manage data capacity, schedule backup and archiving processes, and notify administrators

[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="2"/>     |
| Resolve alerts        | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="1"/>     |
| Delete session logs   | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="1,825"/> |
| Delete agents         | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="30"/>    |
| Delete resource usage | <input checked="" type="checkbox"/> | older than (days) | <input type="text" value="365"/>   |

### Other operations

- |   |                                     |
|---|-------------------------------------|
| Import intelli search parameters                | <input checked="" type="checkbox"/> |
| Include inactive machines in the summary report | <input type="checkbox"/>            |
| Send summary information                        | <input checked="" type="checkbox"/> |

SAVE

CANCEL

RUN CURATOR

## 1.5.9.8. System Notification Settings

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

The screenshot shows the 'Settings' page in the OpenText Database Activity Monitoring interface. The left sidebar contains a navigation menu with icons and labels for Home, Users, User Activities, Roles, API Users, Security, and Notification Groups. The 'Settings' page title is at the top. The main content area is titled 'System Notification' and includes a description: 'System notifications are sent to the specified email addresses. You can add, edit, or delete addresses'. Below this is a section titled 'E-mail Addresses' with a summary: 'Summary information of the system will be delivered to these e-mail addresses.' and action buttons: 'Refresh', '+ New...', and 'Delete...'. The 'E-mail Addresses' section is currently empty, showing a large grey rectangular area.



## 1.5.9.9. SMTP Server Settings

This setting can be utilized to configure mail service settings.

The screenshot shows the 'SMTP Server' settings page. On the left is a dark sidebar with a 'Settings' header and a list of navigation items: Home, Users, User Activities, Roles, API Users, Security, Notification Groups, Storage, System Notification, and SMTP Server (which is highlighted). Above the list is a search bar labeled 'Find a setting...'. The main content area has a title 'SMTP Server' and a subtitle 'Manage email delivery by configuring SMTP server settings'. Below this is the 'SMTP Settings' section with three fields: 'SMTP Server' (empty), 'SMTP Port' (587) with an 'SSL Enabled' checkbox, and 'SMTP From Address' (empty). The 'Authentication Settings' section follows, with an 'Authentication Required' checkbox, 'User Name' and 'Password' fields, and three buttons at the bottom: 'SAVE', 'CANCEL', and 'SEND TEST E-MAIL'.

Settings

Home

Find a setting...

Users

User Activities

Roles

API Users

Security

Notification Groups

Storage

System Notification

SMTP Server

### SMTP Server

Manage email delivery by configuring SMTP server settings

#### SMTP Settings

SMTP Server:

SMTP Port:  ☐ SSL Enabled

SMTP From Address:

#### Authentication Settings

☐ Authentication Required

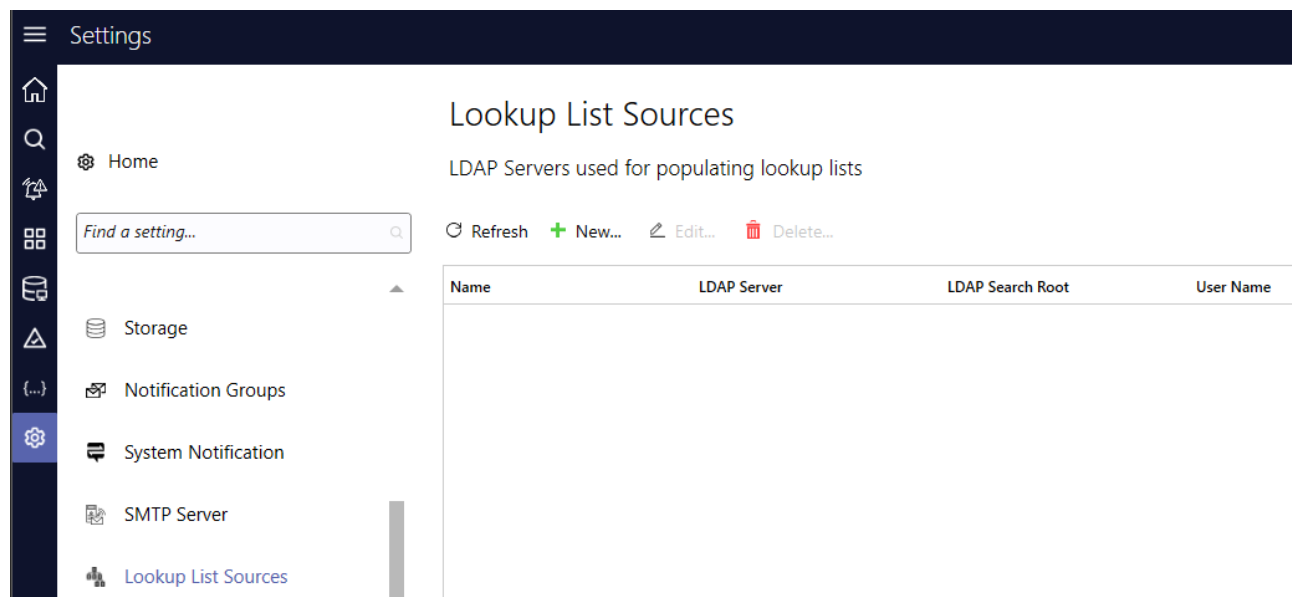
User Name:

Password:

## 1.5.9.10. Lookup List Source Settings

The server information related to users' LDAP services can be entered on this screen. Users can define multiple LDAP server sources here. This allows users to connect to several LDAP servers simultaneously. Relevant queries can be executed, and this will automatically add the results to the Lookup Lists.

This approach simplifies the aggregation and maintenance of data from various sources under a single framework. By executing the relevant queries, the Lookup Lists are automatically populated with the results retrieved from the LDAP Server.



## Adding new LDAP Server Sources

To add a New LDAP Server Source, click **New** button on the **Lookup List Sources Settings**.

New LDAP Server ×

Name:

LDAPServer

LDAP Server:

dc.company.com

LDAP Search Root:

dc=company,dc=com

User Name:

company\username

Password:

••••••••

TEST CONNECTION

SAVE

CANCEL

## 1.5.9.11. Action Account Settings

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

The screenshot shows the 'Action Account' configuration screen. On the left is a dark sidebar with a 'Settings' header and a list of navigation items: Home, Users, User Activities, Roles, and API Users. The 'Settings' header has a search bar with the placeholder text 'Find a setting...'. The main content area is titled 'Action Account' and contains the instruction 'Configure the service account that will perform the system's automated operations by filling in the required fields'. Below this instruction are three input fields: 'Domain Name:', 'User Name:', and 'Password:'. Each field has a red border, indicating it is required. At the bottom of the form are three buttons: 'SAVE', 'CANCEL', and 'TEST CONNECTION'.

Settings

Home

Find a setting...

Users

User Activities

Roles

API Users

### Action Account

Configure the service account that will perform the system's automated operations by filling in the required fields

Domain Name:

User Name:

Password:

SAVE CANCEL TEST CONNECTION

## 1.5.9.12. Distributed Search Settings

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

The screenshot displays the 'Settings' page for 'Distributed Search'. The left sidebar contains a navigation menu with options: Home, Storage, System Notification, SMTP Server, LDAP Servers, Action Account, Alert Forwarding, Distributed Search (selected), and Multi Tenant Mapping. The main content area is titled 'Distributed Search' and includes a subtitle: 'Configure distributed search settings to enable an efficient and centralized search experience across different data sources'.

The settings form includes the following fields and controls:

- ☐ Enable Cross Cluster Search
- Cluster Manage Url:
- ☐ Authentication
  - User Name:
  - Password:
- TEST CONNECTION button
- SAVE button
- CANCEL button

Below the settings form is a 'Seeds' section with a toolbar containing 'Refresh', '+ New...', 'Edit...', and 'Delete...' buttons. Below the toolbar is a table with the following columns: Name, Cluster Name, ES URLs, Cross Cluster Search Status, IP Address, Port, Include in Cross Cluster Search, and Include in Manage APIs. The table is currently empty.

## 1.5.9.13. Multi-Tenant Mapping Settings

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

The screenshot shows the 'Settings' application interface. On the left is a dark sidebar with navigation icons for Home, Search, Settings, Storage, System Notification, and SMTP Server. The main content area is titled 'Multi Tenant Mapping' and includes a subtitle: 'Mapping rules are applied in the DAM Server and executed in order during event processing'. Below the subtitle are action buttons: 'Refresh', '+ New...', 'Edit...', and 'Delete...'. A table with columns 'Enabled', 'Name', and 'Description' is present but empty.

Enabled	Name	Description
---------	------	-------------

## 1.5.9.14. DAM Mapping Settings

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

The screenshot shows the 'Settings' application window with the 'DAM Mapping' configuration page. On the left is a dark sidebar with navigation icons and labels: Home, Storage, System Notification, and SMTP Server. The main content area has a title 'DAM Mapping' and a subtitle 'Mapping rules are applied in the DAM Collector and executed in order during event processing'. Below the subtitle are action buttons: Refresh, New..., Edit..., and Delete... A table with columns 'Enabled', 'Name', and 'Description' is shown, but it is currently empty.

Enabled	Name	Description
---------	------	-------------

## 1.5.9.15. OpenVAS Account Settings

To connect an OpenVAS account, credentials should be entered.

The screenshot shows the 'Settings' application window. On the left is a dark sidebar with a menu containing icons for Home, Storage, System Notification, SMTP Server, LDAP Servers, and Action Account. The 'Settings' title bar is at the top. The main content area is titled 'OpenVAS Account' and includes a subtitle: 'Configure the OpenVAS API connection details to establish integration with the system and manage security scans'. Below this, there are three input fields: 'API Address:', 'User Name:', and 'Password:'. The 'API Address' and 'User Name' fields have red borders, indicating they are required or have validation errors. Below the input fields is a checkbox labeled 'Enable OpenVAS API connection'. At the bottom of the form are three buttons: 'TEST CONNECTION', 'SAVE', and 'CANCEL'.

Settings

OpenVAS Account

Configure the OpenVAS API connection details to establish integration with the system and manage security scans

Find a setting...

API Address:

User Name:

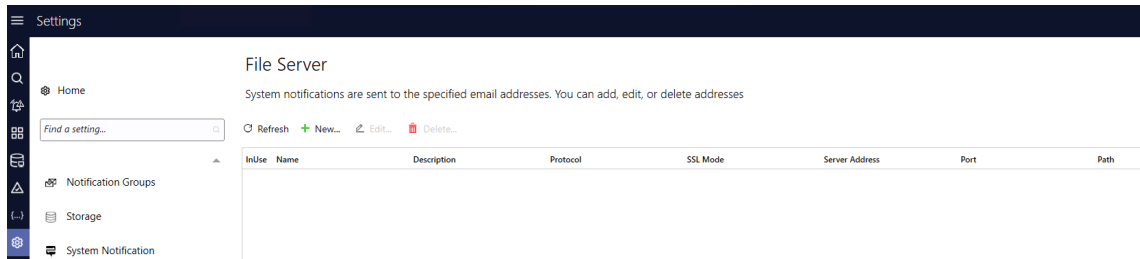
Password:

☐ Enable OpenVAS API connection

TEST CONNECTION SAVE CANCEL

## 1.5.9.16. File Server Settings

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



### Adding a New 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



## 1.5.9.17. All Settings

Accessing and modifying all settings on this screen is possible.

**Settings**

**All Settings**

View and edit all configuration settings across the application as needed

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

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

Name	Value
Section: AgentHealthCheck (2)	
Section: AlertRules (1)	
Section: DailyJobs (10)	
Section: DataMaskExpressions (1)	
Section: Dataskope (1)	
Section: dataskopcollectors (1)	
Section: ESServer (8)	
Section: InfraskopeSiemPlus (1)	
Section: Reports (1)	
Section: Security (2)	
Section: Server (27)	
Section: ServerRoles (1)	
Section: Syslog (9)	
Section: Throttler (2)	

## Adding a New Setting

Setting Editor

Section:

Name:

New name

Value:

New value

☐ Is Password

Password:

Confirm Password:

SAVE

CANCEL

## LDAP Settings

Settings

Home

Find a setting...

Storage

Notification Groups

System Notification

SMTP Server

Lookup List Sources

Distributed Search

Multi Tenant Mapping

DAM Mapping

Action Account

OpenVAS Account

File Server

All Settings

All Settings

View and edit all configuration settings across the application as needed

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

Refresh

New...

Edit...

Delete...

Name	Value
HashMethod	XXH64
LDAPAuthRequired	0
LdapDirectoryType	ActiveDirectory
LdapDN	
Idappassword	*****
LdapServer	
LdapUser	
MappingVersion	0
NotifyKarmasisSupport	0
SignalRSecretKey	633d8825418444c3abe18911bc155de8
SignalRUrl	http://+:8181
SMTPAuthRequired	0
SMTPEnableSsl	0
SMTPFromAddress	
SMTPPort	587
SMTPServer	
SMTPUserName	

VariableName	Values	Definition
LDAPAuthRequired	true	Mandatory

VariableName	Values	Definition
LDAPDirectoryType	ActiveDirectory OR FreeIPA	It has two options.
LdapServer	ip OR ip:port	ip entry is mandatory. ip:port format can be used.
LdapDN	cn=example, dc=karmasis2, dc=local	This field is optional. Ldap search root parameters can be given.
LdapUser	username	Mandatory
ldappassword	password	Mandatory

The default ports for **LdapServer** are as follows:

Port	Protokol/Hizmet
389	LDAP (clear)
636	LDAP
3268	AD Global Catalog (clear)
3269	AD Global Catalog (secure)

## Syslog Forwarder

The SyslogForwarding feature is sending all events to a different syslog server. By default, the syslogserver is deactivated. It can be activated in the Syslog section.

**All Settings**

View and edit all configuration settings across the application as needed

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

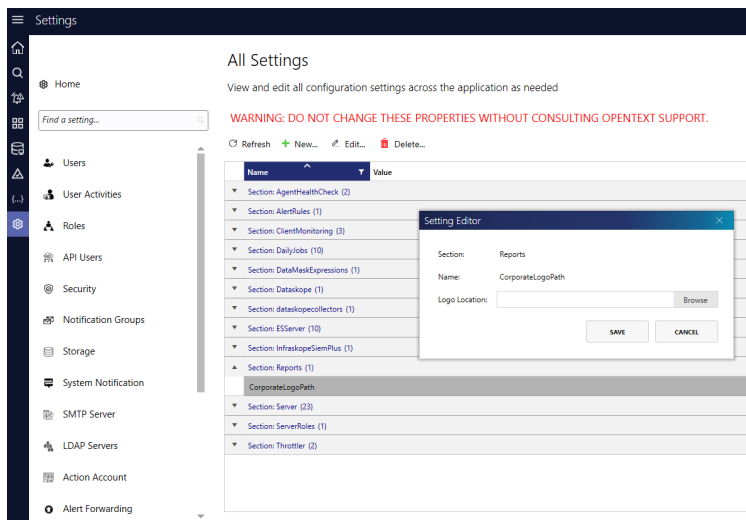
Refresh New... Edit... Delete...

Name	Value
Section: ESServer (8)	
Section: InfraskopeSiemPlus (1)	
Section: Reports (1)	
Section: Security (2)	
Section: Server (27)	
Section: ServerRoles (1)	
Section: Syslog (9)	
AppName	Dataskope
Host	127.0.0.1
MessageFormat	RFC5424
MessageFraming	octet-counting
MessageFramingTrailer	0x0A
Port	514
QueueSize	15000
SyslogForwarderEnabled	true
Timeout	-1
Section: Throttler (2)	

1. Set the **SyslogForwarderEnabled** value to **true**. Then, the messages will be sent in JSON format via UDP protocol to the specified target using **Host** and **Port** information.
2. Go to Services and restart **DAM Server**. The syslog server will be started.
3. The given values should not be changed:
  - QueueSize: 15000
  - Timeout: -1
  - Protocol: udp
4. The following values can be used for Message Format:
  - Rfc5424 (default)
  - Rfc3164 (BSD)
  - Legacy (legacy)
  - Plain
5. The syslog generated event can be processed by the server and viewed on the Console.

## Changing Company Logo

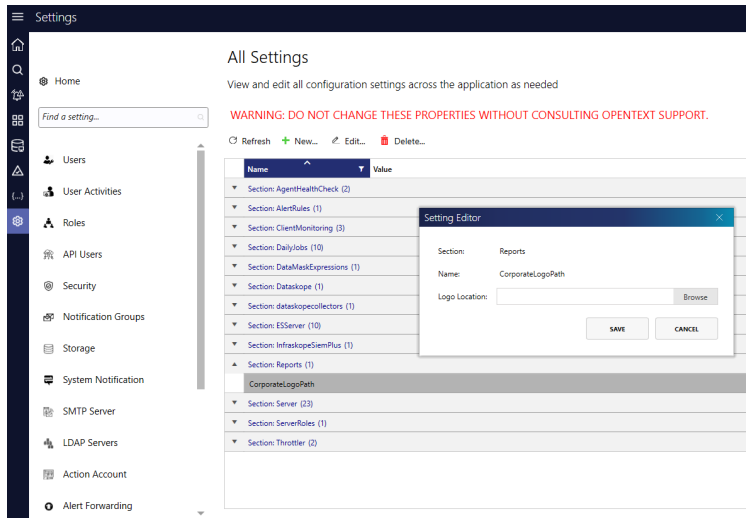
To change the company logo:



1. Click **CorporateLogoPath** under the **Section: Reports**.
2. Click **Browse** to the location to select the logo.
3. Click **Save**.

## 1.5.10. Changing Company Logo

To change the company logo:



1. Click **CorporateLogoPath** under the **Section: Reports**.
2. Click **Browse** to the location to select the logo.
3. Click **Save**.

## 1.6. Transferring Reports

A parametric and database-independent SQL script is used to allow the transfer of report ownership from a deleted/disabled user (`from_user`) to another existing user (`to_user`).

To run the script:

1. Navigate to the location **<install\_dir>\DSMedia\tools**.
2. Open Powershell and execute the following command:

```
sqlcmd -S localhost -d KarmasisControlPanel -U sa -P your_password -i  
ownership_reassignment.sql -v from_user="<deleted/disabled user>"  
to_user="<another existing user>"
```

where `<deleted/disabled user>` is `from_user` and `<another existing user>` is `to_user`

For example : `sqlcmd -S localhost -d KarmasisControlPanel -U sa -P your_password  
-i ownership_reassignment.sql -v from_user="logadmin" to_user="logadmin2"`



© Copyright 2025 Open Text

For more info, visit <https://docs.microfocus.com>

---