OpenText[™] Database Activity Monitoring

Software Version 24.4.0

User Guide

opentext

Document Release Date: October 2024 Software Release Date: October 2024

Legal notices

Copyright 2023 - 2024 Open Text

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

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

Documentation updates

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

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

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that OpenText offers.

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

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

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

Contents

Introduction	
Abbreviations	
DAM Users and Roles	
DAM Architecture	
Logging in to DAM	
DAM Usage	10
Menu and Controls	10
Home	
Cluster Status	
Health and Disk	
Index Size	
Database Info	13
Top Activity	
Events	
Ongoing Alerts	
Search	
Search Panel	
Date Range Section	
Range	16
Export and Save Actions	
Field Chooser	
Historical Alert Processor	
Breakdowns	
Existing Assets	
Queries	
Reports	21
Schedule Properties	
DAM Query Examples	
String Queries	
Specific Field-Based Queries	
Regular Expression Queries	
Regexp String Queries	
Regexp Queries on Specific Fields	

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

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

Introduction

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

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

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

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

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

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

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

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

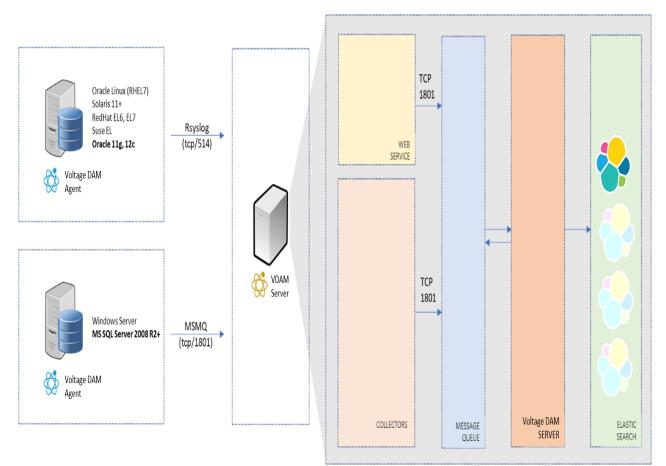
Abbreviations	Definition
DAM	Database Activity Monitoring
DSIM	DAM Installation Manager
DSPL	DAM Socket TAP Module
DSTAP	DAM TAP Module
LDAP	Lightweight Directory Access Protocol
OpenVAS	Open Vulnerability Assessment Scanner
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol

Abbreviations

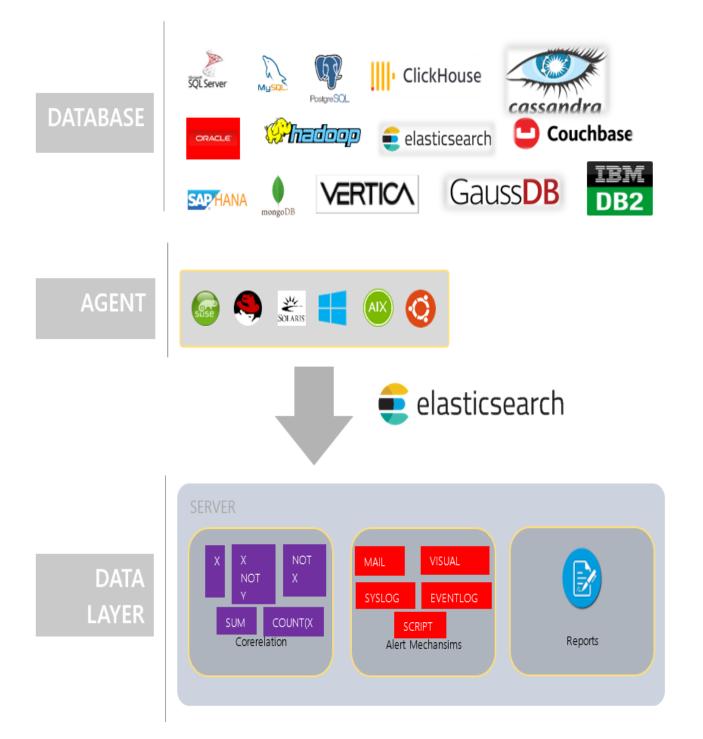
DAM Users and Roles

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

DAM Architecture



Windows Server 2012 R2+ Physical/Virtual Machine



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.

opente	Kt [™] │ Database Activity Monitoring
	Berver Name
	User Name
	Password
	Remember me
	Sign in

3. Click Sign In.

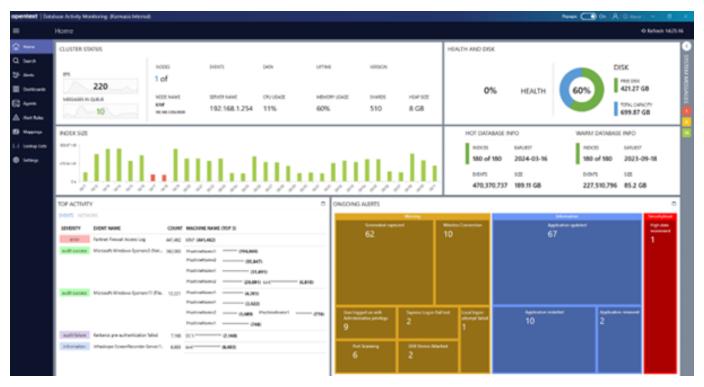
NOTE: The Server Name field can be filled in 3 ways: localhost, Server IP, or Server hostname.

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

DAM Usage

Menu and Controls

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

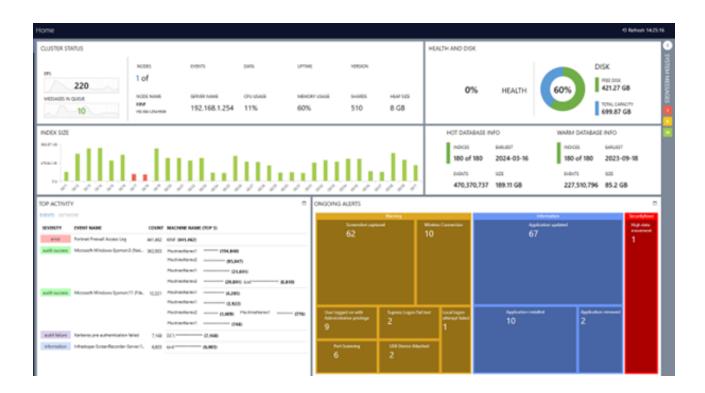


Menus	Function
Home	Used to display the home screen of DAM.
Search	Used to search events and export search results as x1s or pdf.
Alerts	Used to view alerts in detail.
Dashboards	Used to view and edit dashboards.
Agents	Used to show Agents, Policies and Options tabs, and Refresh, New Agent, Edit, Delete,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

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.
Popups: Off	Used to turn pop-up contents on or off.
<u>ዶ</u>	Used to reach user details. Includes Logged On Users , My Profile and Logout submenus.
(i) About	Used to show Copyright, Version, Disclaimer and License information
4	Used to check updates
• Refresh 10:53:39	Used to refresh.
SYSTEM MESSAGES 39 C	Used to show System Errors (red), Warnings (yellow) and Messages (green). Details and content can be viewed with the () icon. The numbers in the colored boxes indicate the number of errors, warnings, and messages.

Home

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



Cluster Status

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

CLUSTER STATUS						
elasticsearch7_kinf EPS	NODES	EVENTS 697.9M	DATA 275.01 GB	UPTIME 143 hours	VERSION 7.16.3	
<u>^ 14</u>	1	057.5141	275.01 GB	145 110015	7.10.5	
MESSAGES IN QUEUE	NODE NAME	SERVER NAME	CPU USAGE	MEMORY USAGE	SHARDS	HEAP SIZE
5	KINF 192.168.1.254:9300	192.168.1.254	11%	58%	510	8 GB

- Nodes shows the number of shards in the database (determined based on the system size).
- Events shows the number of events in the database.
- Data shows the record size.
- Uptime shows the active time period of the system.
- Version shows database version number.
- Node Name shows the node name.
- Server Name shows the server's name.
- **CPU Usage** shows the CPU usage percentage.
- **Memory Usage** shows the memory usage percentage. The max value, is also given with the Memory Usage, shows the amount of memory allocated for ElasticSearch. In Figure 5, the max

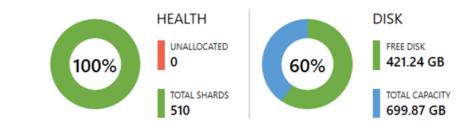
value for ElasticSearch is given as 3 GB max.

- Shards shows the number of the small unit where records are stored.
- Heap Size shows the amount of allocated RAM to the Elasticsearch mode.
- EPS shows the events per second.
- Messages in Queue shows the real-time incoming log count.

Health and Disk

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





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

Index Size

This panel shows how many computers are sending logs, how many computers have DAM agent installed in Active Directory, and how many computers have not connected to the system for a long time . Index Size is the database index, it graphically shows the amount of logs written to the database. If the log amount is the expected (average) number, the bar is shown green, if it is more than or lower than expected, the bar is shown red.



Database Info

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

HOT DATABASE INFO			WARM DATABASE INFO		
	INDICES	EARLIEST	INDICES	earliest	
	180 of 180	2024-03-16	180 of 180	2023-09-18	
	events	size	events	size	
	470,388,139	189.12 GB	227,510,796	85.2 GB	

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

Top Activity

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

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

1	OP ACTIVITY	(•
1	EVENTS NETWO	DRK		
	SEVERITY	EVENT NAME	COUNT	MACHINE NAME (TOP 5)
	error	Fortinet Firewall Access Log	441,462	KINF (441,462)
	audit success	Microsoft-Windows-Sysmon:3 (Net	362,003	MachineName1 (194,848)
				MachineName2 (95,847)
				MachineName1 (31,691)
				MachineName2 (29,891) kinf. (6,810)
	audit success	Microsoft-Windows-Sysmon:11 (File.,	12,221	MachineName1 (4,285)
				MachineName1 (3,922)
				MachineName2 (1,689) MachineName1 (776)
				MachineName1 (748)
	audit failure	Kerberos pre-authentication failed	7,168	DC1.****** (7,168)
	information	Infraskope-ScreenRecorder-Server:1.	6,803	kinf.****** (6,803)

Events

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

Ongoing Alerts

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

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

ONGOING ALERTS					
Warn	ing		Informatio	n	SecurityIssue
Screenshot captured 62	User logged on with Administrative privilege 9	Port Scanning 6	Application updated 67	Application installed	High data movement 1
	Supress Logon Fail test 2	US8 Device Attached 2			
Wireless Connection 10	Local logon a 1	ttempt failed		Application removed 2	

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

Search

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

Search Panel

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

SEARCH		
Search here or filter predefined queries and reports	Search	

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

A beix application group	Rep.	pr; - All Events III							
at 5m Y 🔍 🔿 🔿							last last	Properties 1	Steport Scheduler
				1.			1 647	RANGE OUL OD	25= 00x
								2004-09-11 14/31/532-49	2014-09-11 14:36:532-43
uccowns		SURCE RESULTS					1	RED-CHOOSER	•
erhere.	ж	TeneCouted	Name Y	Reports Y	MachineName	Summary		Alterhee.	ж
Seconda (A)	0 x *	201-09-11 1426502-02	Fortinet Rinewall Access &	entr	694	192,196,1,3> 84,8,8,50 ((inited States) v/s		> Standard Fields	
with source	8,005	2024-08-11 14/36/502-03	Fortinal Fernal Acons G	-	614	$152.162.13 \rightarrow 82.4.453 \ (Sechael States) \ n's$			
		204-09-11 1438-502-03	Forthet Frenal Access 5	enter	694	182,168,1,3 \rightarrow 8,844,453 (Sinted Totes) v/s			
ese.	4.199	2024-08-11 14:36:532-43	Fortinet Frenal Acces 5	-	614	182,168,1,3> 8,84,453 (Johnel States) v/s			
with Solver	324	204-09-11 14;06:502-03	Forthet Reviel Access to	entr	614	182,166,1,3 -> 8,8,8,8,50 ((avted Date)) v/a			
(Complete)	142	2024-08-11 14:36:502-03	Fortinet Frenal Acces L	-	614	162.168.1.127 -> 108.171.127.188.5228 (3%			
Machine/Lame (6)	•		Fortinet Firewall Access to		614	1823083.3 -> 884.453 (~)a			
antargi PC kamasi Ziscal	7,200		Factions French Access L		614	TELNET.3 -> ELAASS (Solvel State) 1/4			
			Fortnet Frewall Access 5		64	192 368 1.3 8.8 8.8 50 (Swited States) v/a			
			Faction Frend Access L		64	TREASENCE + BARRIER (Locket States) 1/2			
LE COMPLE PERMIT AND			Fortnet Frewall Access 5		69	192 368 1.3 8.8.8.8.50 (United States) v/a			
C1.kamadi.2.ksci	330		Fortinet Frend Access Li Fortinet Frendel Access Li		124	182.168.1.3> 8.8.4.4.53 (United States) =/+ 182.168.1.3> 8.8.8.8.53 (Livited States) =/+			
Minner Kannesziool	250		Fortinet Frendl Access to		00	162 162 13+ 8.8.8.50 g via			
itter	326		Fortiget Frendel Access L		100	102 108 1.3 -> 8.8.4.4.53 0/a			
Name (K)			Factionst Freewall Access (c		64	TREASE IS -> REAASD (initial listed of			
	_		Fortinet Formed Access to		614	192 198 1.3 + 8.8.4.450 () m/s			

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.

/12	W13	W14	W15	W16	W17	W18	W19	W20	W21	W22	W23	W24	W25	W26	W27	W28	W29	W30	W31	W32	W33	W34	W35	W36
		Ар	r il, 202	4		м	ay, 202	94			June,	2024			July	y, 2024			4	August	, 2024			Sept
														al L	.1									
					- 1	dal I	table.	dlha				dth.			llh.									
					h	IIIII	dillin				- 111	dilili												
									1							Ш.								
									h	hili						lh.	ւիսե	ult.	հե	ult	dla	hur.	h	ath.,
				.060					luti.	.hth.						lh.	վեն	ad t.	hth.	.tilt.	dhi.	hu.	h	allı.
	Custor			.llio.					llılı.	.hth.						llı.	altılı	udt.	hth.	.tilt.	ıllıt.	hu.	hu	allı.
0	Custor	n	4.00.1					End	lult.	.1111.		14-26-4				lh.	altılı	udt.	hth.	.IIII.	dha.	hu.	hu	attı.
0	Custor	n	24-09-1	1 1431	.53			End	Date:	. . 2024	-09-11	14:36:5	13	1		lh.	altılı	an lı .	hth.	.tilt	dha.	hu.	hu	allı.
0	Custor	n	24-09-1	. II I 1 1431	53			End	Date:	2024	-09-11	14:36:5	3	:		llı.	olth	u lt.	hth.	.IIII	dha.	lm.	hu	allı.
Sta	Custor	e 202		1 14:31	53	Last			Date:			14:365 Today	3		III This W	I h.	oltih	itt il .	hth.	.1111.	ot D8	lm.	Warm	

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

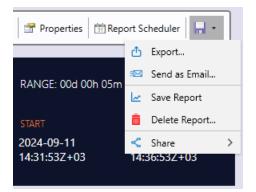
Range

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

RANGE: 00d 00h 05	5m 00s
START	END
2024-09-11	2024-09-11
14:31:53Z+03	14:36:53Z+03

Export and Save Actions

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



Field Chooser

SCARCH RESULTS					10	FIELD CHOOSER	
TimeOreated	Name Y	Reywords T	MachineName 7	Summary		Fiber here)
2024-09-11 14:06:532+00	Fortinal Frenall Access to	error	KINF .	192.568.5.3> 8.8.8.8.53 (Johnel States) n/a	î	Standard Fields	
2024-09-11 1436:532-08	Fortinet Rirewall Access U	enor	KINF	192.168.1.3> 8.8.4.4.53 (United States) n/a			
2024-09-11 14:36:532+08	Fortinat Finewall Access to	ertor	kind	192.168.1.3> 8.8.4.4.53 (United States) n/s			
2034-09-11 14:06:532+09	Fortinet Rinewall Access to	eror	KINF	192.168.1.3 → 8.8.4.4.53 (United Stated In/a			
2024-09-11 14:06:532-03	Fortinat Frenall Access &	arror	KINF .	192,568.5.3> 8.8.8.8.53 (Johnel States) rs/a			
2024-09-11 14:06:532-05	Fortinet Rirewall Access to	enor	KINI	192.168.1.127 → 108.177.127.188.5228 (Jan			
2024-09-11 14:06:532+03	Fortinat Finewall Access to	error	KIN	192.168.1.3> 8.8.4.453 () n/a			
2024-09-11 1436:532+08	Fortinet Rirevall Access &	eror	KINF	192.168.1.3 → 8.8.4.4.53 (United States) n/a			
2024-09-11 1436-532-00	Fortinat Finewall Access to	error	KINF .	192,568.1.3> 8.8.8.8.53 (Johned States) n/a			
2024-09-11 1436:532-00	Portinet Rirewall Access U	enor	KINI	192,168.1.3 → 8.8.8.8.33 (United States) N/a			
2024-09-11 14:06:532+00	Fortinal Formall Access to	error	KINF	192.568.5.3> 8.8.8.8.53 (United States) n/a			
2024-09-11 1436:532+08	Fortinet Rirewall Access &	enor	KIN#	192.168.1.3 → 8.8.4.4.53 (Juited States) n/a			
2024-09-11 14:36:532+08	Fortinat Finewall Access &	ertor	KINF	192.168.1.3> 8.8.8.853 () =/a			
2024-09-11 14:06:532+00	Fortinet Rirewall Access to	erox	KIN#	192.168.1.3 → 8.8.4.4.53 (United States) w/a			
2024-09-11 14:06:532+00	Fortinal Frenall Access &	error	KINF .	192.168.1.3 → 8.8.4.4.53 () +/#			
2024-09-11 14:06:532=08	Fortinet Rirewall Access U	eror	KINF	192.168.1.3 → 8.8.4.453 (United State) rula			
2024-09-11 14:36:532+08	Fortinat Finemall Access to	erter	kind	192.168.1.3 → 8.8.4.453 () n/a			
					Page 1 of 136	E Brasistown fait III (Crist Re

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:

FI	ELD CHOOSER			¶	FIE	LD C	HOOSER			ņ
F	iter here			×	Fil	ter h	ere			×
¥	Standard Fields			-	>	Stan	dard Fields			4
	Category	Σ	≡		~	Dyni	amic Fields			
	Channel	Σ	≡			1	sourceaddress	Σ	≡	
	DataLabel	Σ	≡			2	srcip	Σ	≡	
	EventID	Σ	≡			3	dstip	Σ	≡	
	EventSource	Σ	≡			4	srcport	Σ	≡	
	Hash	Σ	≡			5	dstport	Σ	≡	
	Keywords	Σ	Ξ			6	action	Σ	≡	
	Level	Σ	≣			7	type	Σ	≡	
	MachineName	Σ	Ξ			8	subtype	Σ	≡	
	Name	Σ	Ξ			9	proto	Σ	≡	
	Severity	Σ	≡			10	dstcountry	Σ	≡	
	Summary	Σ	Ξ			11	srcmac	Σ	≡	
	TimeCreated	Σ	Ξ			12	facility	Σ	≡	
	TimeInserted	Σ	≡			13	severity	Σ	≡	
	UserName	Σ	≡			14	date	Σ	≡	
>	Dynamic Fields					15	time	Σ	≡	
>	Other Fields					16	devname	Σ	≡	
				~		17	devid	Σ	≡	Ŧ
	Σ Breakdown field	≣G	rid fie	ble			Σ Breakdown field	≣g	rid fie	ble

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
ዋ	Used to hide the Field Chooser panel.
Filter here X	Used to filter the fields.
ΣΣ	Used to add the filter to the Breakdowns list.
	Used to add the filter to the search results table as a column.

EARCH RESULTS						1
fimeCreated	Name T	Keywords T	Mach	ineName	т	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/4
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/4
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/4
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/
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/
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/
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
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF			192.168.1.119> 8.8.4.4:53 (United States)
2024-09-11 14:36:53Z+03	Microsoft-Wine 🖉 Edit	Summary		rgi-PC.karmasi	s2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)
2024-09-11 14:36:53Z+03	Microsoft-Winc 🗹 Chec	k Integrity	>	argi-PC.karmasi	s2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)
2024-09-11 14:36:53Z+03	Microsoft-Winc 🛆 Send	to Alert Processo	or >	argi-PC.karmasi	s2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)
2024-09-11 14:36:53Z+03	Microsoft-Winc + Add	Drop Rule		argi-PC.karmasi	s2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)
2024-09-11 14:36:53Z+03	Microsoft-Winc 🛆 Crea	te Alert Rule		argi-PC.karmasi	s2.lo	KARMASIS2\can.kargi -> 192.168.1.134 (-)
H	Sind	Related	>			Page 1 of 136

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

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

Historical Alert Processor

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

TimeCreated	Name T	Keywords T	MachineName T	Summary
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Li	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 Le	error	KINF	192.168.1.3> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortinet Firewall A	neck Integrity	> 66 For All Even	1.3> 8.8.4.4:53 (United States) n/a
2024-09-11 14:36:53Z+03	Fortingt Firewall A	end to Alert Proce		1.2
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Le	error	KINF	192.168.1.3> 8.8.8.8:53 (United States) n/
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 Li	error	KINF	192.168.1.134> 3.254.236.24:443 (United
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Le	error	KINF	192.168.1.3> 57.144.126.192:443 (France)
2024-09-11 14:36:53Z+03	Fortinet Firewall Access L	error	KINF	192.168.1.134> 3.254.236.24:443 (United S
2024-09-11 14:36:53Z+03	Fortinet Firewall Access Li	error	KINF	192.168.1.119> 8.8.4.4:53 (United States)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysm	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysm	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.78 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysm	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysm	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 10.10.10.1 (-)
2024-09-11 14:36:53Z+03	Microsoft-Windows-Sysm	audit success	CanKargi-PC.karmasis2.lo	KARMASIS2\can.kargi -> 192.168.1.134 (-)

Breakdowns

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

BREAKDOWINS		4
Filter here		×
✓ Keywords (4)	¢ ×	Î
audit success	8,866	L
error	4,199	L
audit failure	324	L
information	162	
✓ MachineName (6)	¢ ×	
CanKargi-PC.karmasis2.local	7,200	L
KINE 2 3	16 4,192	L
ELIF-DEMIRTAS-PC.karmasis2.lo	<u>cal</u> 1,245	L
DC1.karmasis2.local	330	L
EylulSonmez-PC.karmasis2.local	258	
Other	326	
✓ Name (6)	o x	
Microsoft-Windows-Sysmon:3 (Network Co	1
Fortinet Firewall Access Log		~

Existing Assets

Queries

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

Search		
# Hone A basic application group w		
SEARCH		
Search here or filter predefined queries and reports		Search
EXISTING ASSETS		
QUERES (\$74) REPORTS (\$2)		
NAME TAG	a quary	
O A basic application-group was changed	EventD-4764 AND EventSource: Microsoft Windows Security Audiling'	
O DADABASE BADKUP ERROR.	EventEvursa:"SglEvver-Audit" AND EventD1568 AND category"BAD0JP AND revuit:"SclEvere-Audit" AND EventD1568 AND category"BAD0JP	
A basic application group was created	EventD-018 AND EventSource"Microsoft Windows Security Auditing"	
A basic application group was deleted	EvenED-4785 AND EvenEducitie "Minister" Windows-Security-Auditing"	
A certificate request extension changed	EventDAI73 AND EventSource*Mindows-Security-Auditing*	
A Certificate Services template was updated	EventD-AB9 AND EventSource: "Microsoft Windows-Security-Auditing"	
A change was made to iPsec settings	(senED504) AND (sentSource?Microsoft Windows Security Auditing?	
A change was made to the Windows Firewall exception list	EventD-HHB AND EventSource: Microsoft Windows Security Auditing*	
A computer account was changed	EventD-K142 AND EventSource: "Microsoft Windows-Security-Auditing"	
A computer account was created	EventDxD4D41AND (ventSource'hliorosch Windows Security-Auditing'	
A computer account was deleted	DentDAT43 AND EventSource "Microsoft Windows Security Auditing"	
A configuration entry changed in Certificate Services	DeetC-4811 AND EvertSource "Microsoft Windows Servicity Auditing"	
A configuration entry changed in the OCSP Responder Sanica	Deet03123 AND (seetDoutse "Microsoft Windows-Security Auditing"	*

Reports

.....

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

arch					
have A best	application group w Report - All Events	•			
	SEARCH				
	Search here or filter predefined queries and rep	075			Search
	EXISTING ASSETS				
	OLERES (\$74) REPORTS (\$2)				
	Filter reports here				Scheduled only
	NAME	CATEGORY	On the second se	SOHDAUS	1
	* A basic application group was changed		EventD-4764 AND EventSource "Microsoft- Windows Security Auditing"		
	* All twents	All Event	n		
	* Custon Al Dients	Allbert	1		
	* All Application Activity Logs	App Tracker	(EventOx6010) OR (EventID:6011)		
	* All Application Usage Logs	App Tracker	EventD 6012		
	All Text Editors Usage Logs.	App Tracker	EventD-6012 AND (processmellinolegad") OR processmellisublimet" OR processmellintam" OR processmellinkorosith Wordpad")		
	* Application Activation	App Tracher	EventiO 6010 AND EventSource "inhackope"		
	* Application Activities With Admin Privileges	App Tracker	EventD 6010 AND windowtitle "Administrator"		
	* Inactive User - Scheduled Report	App Tracker	EventD:6012 AND processname:"LockApp.exe"		
	R Microsoft Office Usage Logs	App Tracker	EventD 8012 AND (processname*Morrosh) Wood* OR processname*Morrosh Exo#* OR processname*Morrosh* Oxfood** OR processname*Morrosh* RowerPoint** OR processname*Morrosh*Access*	2	
	* Web Browser Activity	App Tracker	EventED:8011		*

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.

chedule Properties		- o ×
 Enable Schedule 	ŧ	
GENERAL TRIGGER		
Content:	🕑 Data 📃 Summary	
File Name:	File Name	
Format:	Csv	~
Page Size:	A4	
-	Portrait	
Page Orientation:	Convert time to local Show column headers	*
CSV Options:	Convert time to local Show country neaders Clear double quotes inside value	
Deliminator:	◯ Tab ◯ Semicolon ● Comma ◯ Space ◯ Other	
Email File Share	FTP Share	
 Enable 		
	to generated alert	
Subscribers:		Notification groups only
Judichoerk	Apply classification rules for subscribers	Houndation groups only
	mppy classification in subscribes	
		SAVE CANCEL
Schedule Properties		- o x
 Enable Schedu 	e	
GENERAL TRIGGER		
Content:		
File Name:	🗸 Data 🔄 Summary	
	Data Summary File Name	
Format:	File Name	v
Format: Page Size:	File Nome Cav	•
Page Size:	File Name Cav	• •
	File Name Cav A4 Portrait	v v
Page Size:	File Nome Cov A4 Portrait Covert time to local Show column headers	v v v
Page Size: Page Orientation:	File Name Cav A4 Portrait Image: Convert time to local Image: Con	♥ ♥ ♥
Page Size: Page Orientation: CSV Options: Deliminator:	File Name Cav A4 Portrait ✓ Convert time to local ✓ Show column headers ✓ Enclose value in double quotes ✓ Clear double quotes inside value Tab Semicolon € Comma Space Other	♥ ♥ ♥
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share	File Name Cav A4 Portrait ✓ Convert time to local ✓ Show column headers ✓ Enclose value in double quotes ✓ Clear double quotes inside value Tab Semicolon € Comma Space Other	♥ ♥ ♥
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share I Enable	File Name Cav A4 Portrait Image: Convert time to local Image: Convert timage: Con	 ✓ ✓ ✓
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share V Enable Share Path:	File Name Cav Ad Portrait Image: Convert time to local Image: Convert timage: Con	
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share I Enable	File Name Cav A4 Portrait Image: Convert time to local Image: Convert timage: Con	
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share V Enable Share Path:	File Name Cav Ad Portrait Image: Convert time to local Image: Convert timage: Con	U BROWSE
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share Emable Share Path: Domain Name:	File Name Cav Ad Portrait Image: Convert time to local Image: Convert timage: Con	BROWSE
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share Enable Share Path: Domain Name:	File Name Cav Ad Portrait Image: Convert time to local Image: Convert timage: Con	
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share Enable Share Path: Domain Name:	File Name Cav Ad Portrait Image: Convert time to local Image: Convert timage: Con	
Page Size: Page Orientation: CSV Options: Deliminator: Email File Share Enable Share Path: Domain Name:	File Name Cav Ad Portrait Image: Convert time to local Image: Convert timage: Con	

edule Properties								
Enable Schedul	e							
ENERAL TRIGGER								
Content:	🗸 Data 🛛	Summary						
File Name:	File Nome							
Format:	Csv						~	
Page Size:	A4						~	
Page Orientation:	Portrait						~	
CSV Options:		t time to local	Show colur					
Deliminator		value in double quot		le quotes inside value				
Email File Share			omma () space					
File sending w		d		File sending with S	FTP enabled			
192.168.1.129				✓ Select file server				
						SAVE	CANCEL	
_						SAVE	CANCEL	- 1
Enable Sche	dule R					SAVE		- 1
Enable Sche SENERAL TROOF	dule	00.00.00		0		SAVE	Runs a day. G	e 00:00 e
Enable Sche SENERAL TROOF Daily Weekby	dule R		ific Time 00.00	0 00 © 00000 ©		SAVE	Runs a day. G	enerates
Enable Sche GENERAL TROOF	dule R		ific Time 0000			SAVE	Runs a day. G	enerates
Enable Sche SENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	enerates
Enable Sche SENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	enerates
Enable Sche SENERAL TROOF	dule R		ife Time 00.00			SAVE	Runs a day. G	enerates
Enable Sche ENERAL TROOF	dule R		ific Time 0000			SAVE	Runs a day. G	- I
Enable Sche SENERAL TROOF	dule R		ific Time 0000			SAVE	Runs a day. G	enerates
Enable Sche SENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	enerates
Enable Sche SENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	- I
Enable Sche SENERAL TROOF	dule R		ific Time 0000			SAVE	Runs a day. G	- I
Enable Sche SENERAL TROOF	dule R		ific Time 0000			SAVE	Runs a day. G	- I
Enable Sche SENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	- I
Weekly	dule R		ife Time 00.00			SAVE	Runs a day. G	- I
Enable Sche ENERAL TROOF	dule R		ife Time 00.00			SAVE	Runs a day. G	enerates
Enable Sche ENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	enerates
Enable Sche ENERAL TROOF	dule R		ific Time 00.00			SAVE	Runs a day. G	- I

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	at meet the specified conditions. The "AND" operator

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: producnme~ (Correct spelling is productname) EventSource: productme~ EventSource: proutname~ EventSource: prouctnae~
To perform searches with restrictions on a single field:	EventSource: 'productname OR OSname' EventSource: 'productname OSname' (Works in the same way with OR)
To perform a search using a specified range:	TimeCreated: '[Date to Date]' TimeCreated: [* TO 2017-12-01] (Returns all dates before the specified date)
Search with sorting	EventID: >10 EventID: >=10 EventID: >= 500 AND EventID: <=1000 EventID: [500 TO 1000]

Regular Expression Queries

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:	<pre>/(P p)ro(ductname file)/ This regular expression pattern will match the word "Pro" followed by either "ductname" or "file". The "(P p)" part allows for variations in the capitalization of the letter "P"</pre>
	<pre>/(p P)ro./ This regular expression pattern will match any word that starts with "pro" or "Pro" followed by any characters. The "(p P)" part allows for variations in the capitalization of the letter "P",</pre>

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

Regexp Queries on Specific Fields

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

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

Alerts

Verts								
2824-05-11 08:00:00		2524-04-11 23:09:04	I Sect					
2009-09-11 00:00:00		and the second second		ALC: N				
Severity	5646	Aust Tane	Competer Name		Name	Suppress Count	Massaga	
• Maring	hev	2824-09-111452-12	003		The account looked out			
Warring	New	2824-05-11 14/0/14	MatriceBarred		Screenshot captured		Screenhot is captured on Henroekened in HM.	
 Security/sece 	New	2624-09-11 1416-048	Maderallated		Kiph data mavement		Tau many time coginal to USB device	
 Warring 	New	2824-25-11 1415:59	Hadrow Barnell		USB Device Attached			
 Warring 	New	2824-09-11 1412-01	Hasto ellared		108 Device Attached			
 Marring 	Nev	2824-09-11 1408/17	Matterelland)		Screenshot captured		Screenshot is captured on	
 Warring 	have	2824-09-11 1e06/17	Mathine Barrel		Screenshot captured		Screenbult's captured an Michael Annaba, 100	
 Warring 	harv	2824-09-11 1409-25	Mathematica		Screenshot ceptured		Scientifict's optimitian . Historickinstra, 500	
 Warring 	New	2624-09-11 1400/15	Maderelland		Screenshot captured		Screenbult's captured an History Kendly XX.	
• Warring	hev	2824-09-11 1400/12	Manhored Revent		Screenshot captured		Screenhot a captured on Pantorelaned in XXX	
 Warring 	have	2824-09-11 1408/12	Marthrolline)		Screenshot captured		Scientist's captured on Historikanad in 100	
 Warring 	here	2824-09-11 12 59-51	(7st).		Screenshot captured		Scientific application. Pacticipation, 500	
 Warring 	New	2624-09-11 12:58:07			Screenshot captured		Screenhot is captured on Historicania/19/88.	
• Harring	hev	2824-09-11 12-58-17	Hartrollams]		Screenahot captured		Several-of a ceptored on Machinekanud by KK.	
								Rep: 1 of 2 175 %
ine Generated	form D	* Searce	Y Category Y	free lign - 7	Machine Name		* Event Details	
2014-09-11 14:50:07	4740	Mexanit Windows S	iesa Uber-Assourt	Add sources	0C1 *****		(See 6) VINC	
							Next* Y are present and index any Next*Y (S1): Next*Y (S1): Next*Y (S1): Next*Y (S1): Next*Y (S1): Next*Y (S1): Next*Y (Next*Y): Next*Y (Next*Y):	

- Severity shows the event type.
- State shows the action status of the event.
- Alert Time shows the date and time of the event occurrence.
- Computer Name shows the machine name where the event occurred.
- Name shows the event description.
- Suppress Count shows the number of suppressed events.
- Message shows the description.

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

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

	Severity	State	Alert Time	Computer Name			Name
•	Warning	New	2024-09-11 14-52-12		JE AN		User account locked out
•	Warning	New	2024-09-11 1 A Alert	Resolution State >	비를 All	>	New
•	SecurityIssue	New	2024-09-11 14:16:03			٦	Acknowledged
٠	Warning	New	2024-09-11 14:15:59				Assigned To Helpdesk
٠	Warning	New	2024-09-11 14:12:01				Outsourced
•	Warning	New	2024-09-11 14:06:17				Resolved

Change Resolution State Menu:

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

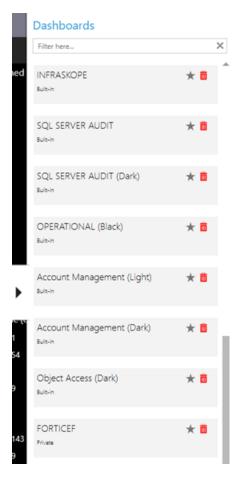
Dashboard

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

5								/ In Children	9 Relia 145728
VPN Tracking	increase the stand	Top Countries	ineral bea	Top Real IP Addresses	inerer beleg	Top Users	investing.	Top Assigned Private Ph	International National
Survey class	165	United States	276232	1111	98.172	use1	361	forward	66.82
carried	64		21,174	8844	26.452	um2	153	local	26,627
depres	64	Tarkey	14342	13.1072222340	6.209	uwr3	N3	endpoint	
funnel-down	25	United Graphon	16261	154171.14201	5.047	991079			
turnel-up	24	Rusian Federation	5.424	1111	5.002	used			
of east error		Nethelands	5,404	150171.1039	4,907	NA			
si det		Cernary	4349	150.171.16.39	2344				
of new can		Autola	460	192175484	2.629				
		France	3.412	158171.16340	2563				
		Inland	2,345	206.065.201	2,198				
		Caroda	1.629	216239.34.10	2.090				
		Sweden	1.469	35.18622424	1.997				
		Hong Cong	1,205	100171.102	110				
Internet Traffic (inbound)	movel fields	Internet Taffic Jostboar	e) meature	Top Dest Ports	tional faile	Local Taffic (robound)	Next Tale	Local Traffic (subound)	ners Me
19210813	16,71 68	213.74.174.128	15.15.68	53	206813	10212154200	3273 MB	192,108,1.81	96.11 MB
1921683119	7.46.68	\$211510841	12.01.68	443	132497	10212104201	61.04 MB	192.1681.254	86.79.68
192108-1154	578 68	154.14L12.37	5.95 GB	67	54.036	PR2.168.1.150	27.44 648	258.146.19	\$1.9 MB
192168.1190	52168	\$2,56,180,153	2.83.68	1048	19,309	31,223,16,155	30.71 MB	192,168,1.89	0.95 MB
192,168,1127	E I GB	217.1467.001	141 CB	637	12,777	134071341	15.90 MB	164.13	17.41 MB
1921081111	4.27 GB	4724132134	1.34 GB	80	1.798	1021681.97	10.41 MB	192.1683.3	11.83 MB
1921681115	4.16.68	1561465279	131.68		4.039	4422810824	\$35.89 (8)	45.05.0610	7.5 MB
192108140	3.84 68	\$2114,115,160	1,29 (8	\$23	1464	19216813	33431-0	192.1661.99	736.27 KB
192168-1110	331 68	30.196.100.151	L36 CB	1228	2,324	199.45.154.146	76.15 48	192,966,145,160	47.54 KB
192.168.1.77	3.19 G8	4031.0044	11.75 MB	138	2.322	N2.142.125.35	16.11.68	192, 166,0, 195	48.37 13
192168.1190	1.06 GB	\$2.115.107.85	752.15 MB	5938	1,097	164.9021035	62.40 (0	192,168,148,189	3423-08
192108.1116	133 68	213.227.168.540	11.79.66	5478	1.96	66.163.152.97	10.01 13	25534531	32.59 (3
15216816	151.68	185,166,143,38	419.18 MB	640		1921683.021	40.7148	192.1681.84	0.5 0

Sliding Dashboard Panel

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



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

boards			-	falk C AdSceen 4 fateb 10000 Stee * A
NNOON				
			ILEACOME Investigned In TOP MACHE Berry Be	ref 40,60 re2 256,547 re6 50,707 read 40,071
Generic USB Device Usage veluade veluade MtConfig USBSTOR WashEDRowerSD rturs2264	sear sax USB Devices Used 4 SanOok Crozer Fit USB Device 2 2 2 3 1 1	www.rww Data Movement by Usernar 2	nd www.vew Screensbucks E7:01:148 Uner1 Uner2 Uner6 Uner17 Uner22	by Utamane www.www. 97 22 6 19 33
Most violad and sites (apprache)		www.inkedin.com	403 Windows Vers 194 Cuthook - * 99 Windows Sen 195 Windows Sen 196 Oally Spic - N 197 Arkens Web 196 Karmasis Res 196 192 No. 193 87	Applications (spotraciles) www.r.lwa aulia Lack Sonwin 05.36.54 aylian Kilk Bosani 03.54.51

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

Edit Dashboard

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

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

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

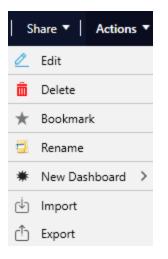
The **Themes** tab offers various **Theme Designs**. It also provides separate customization opportunities for **Background**, **Widget Caption**, **Widget Area**, **Widget Border** and **Chart Formatting**.

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

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

File	Desig	yn The	emes	Option	s										
Sav	e	Delete	Rena	ame f	Bookmark										
File Desi	gn Them	es Options													
💜 Forma	t Painter	123,456 Value	Pie	Bar	Column Time		map Map	Data Grid	-	L Image			Align	5 Undo	Redo
Clipbo	bard					Insert	Widget						Layout	Histo	ory
File Design	Themes Op	tions													
Light (Green, Aa		Light (Blue/White) Aa	Dark (Yellow/ Aa	Black) Aa	rk (Yellow/Black) a	Dashboard Background	Segoe UI V <u>A</u> V A V Widget	18 ¥	Segoe UI V A V A V Widget	14 🗸	Vidget	Palette: Axes color:	Windows8	¥	Save as Theme
			Themes			~	Caption		Area		Border		Formatting		
File	Desig	in The	emes	Options	5										
30 se	ecs		~												
	Refres	h Interva	əl												

Actions



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

Creating a New Dashboard

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

To create a new dashboard,

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

3. Choose a theme for the new dashboard and press the **OK** button.

New Dashboard				:
Please provide a new nar	ne for the new dashboard:			,
Description for the new d	lashboard:			
Select a theme for the ne	w dashboard:			
Light (Green/Gray) Aa	Light (Blue/White) Aa	Dark (Yellow/Black) Aa	Dark (Yellow/Black) Aa	
Dark (Khaki/Gray) Aa	Dark (Khaki/Gray) Aa	Dark (Green/Black) Aa	Dark (Green/Black) Aa	
			ок	CANCEL

Agents

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

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

• Group your agents for monitoring purposes with the categorization feature.

6045					OC TABLE	Refrech
Crouped by 6					-	New Agent
OSTAP Status	T DSM Status T	Hod Name	T Deteluir T	DSM Version 7		Edit
A oracle (1)						Delete
* Alve	 Running 	win19-pr(19-2	0.004	2436470		Actions *
 10.388/68.02 	5					
 Alve 	 Running 	Deficiel/040-18514	SOCIEPIOR	2434489		
 Alter 	 Ranning 	ev.	SQUEEKER	21.073		

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 Wiz	zard	×
Connect	tion	
Enter the conn	nection information to connect to the agent	8765
Protocol:	TLS 1.2	~
Certificate Use old defa	fault certificate 🔵 Use new default certificate 🔵 Upload certificate	
Client Certificat	te:	Browse
Password:		
	Use old certificate Use new certificate	
	CANCEL	NEXT >

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

New Agent Wizard

Listener Settings

Select the databases you want to collect logs

pcap.devices	*
oracle.enabled	
oracle.server_port	1521
mysql.enabled	
mysql.server_port	3306
postgre.enabled	
postgre.server_port	5432
mssql.enabled	
mssql.server_port	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 Set	Listener Settings					
Select the databases	you want to collect logs					
elastic.enabled						
elastic.server_port	9200					
netezza.enabled						
netezza.server_port	5480					
gauss.enabled						
gauss.server_port	1888					
sybase.enabled			- E			
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:

00:	T
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	

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

When clicked on Finish button, agent is created.

CANCEL

< BACK

×

×

۰

NEXT >

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

Agents Tab

ents Open								
Policies 0	Options							TASKS
(ENTS						DETAILS	•	Refrech
Dougel by	Cataline					· without	19-2 Î	New Agent
DS7VP Rules	T DSM Status	Y Hot Name	· Section ·	DSM Wester Y		CS Name	Windows Server 2019 Standard	Calif
• ende (7)							Detution	Delete
· Alter	· Auroing	win19-ord19-2	oracie	24384723		Tex.	· · · · · · · · · · · · · · · · · · ·	
10.507/01.0	a					OS Release		Actions *
•	· Ranning	047454049-78374	100389-08	243.44828		CS Version	104.17763	Open Terminal
•	· furning	KM/	SQUERVER	243.54793		CPU Contib	4	
						Physical Rams	4.08	
						Strage Location	CitoganDatedata/optiqued	
						Tutal Capacity	20.4 (8	
						Aver Spece	217.08	
						Debug Mode		
						DIPL		
							u .	
						Last Contacted	2024-09-11 12:40:42	
						COSIM (Running	
						CETAP (Alter)	
						· Realtime D	agnostica () Sant () Report	
						CPU theps	0.00%	
						Resident Memory	114.14 MB	
						Virtual Memory:	29.56 MB	
						Messages Dropped Messages Sent		
						Recises Captured	230568	
						Reckets Dropped	0	
					Page 1 of 1	Reclarts Queue Cox	- 0 V	

Controls	Function
DETAILS	Used to reach details of the selected agent. Real-time Diagnostics tool available here allows user to view the agent's activities and performance in real-time.
Refresh	Used to refresh the agents tab.
New Agent	Used to add new agent. For more details, see Adding a New Agent.
Edit	Used to edit the selected agent.
Delete	Used to delete the selected agent.
Actions	Used to reach various actions related to the agents. Includes Export and Send as Email.
Open Terminal	Used to open terminal.

Policies

gents Po	Actes Options			
insuped by		Detabers A	Decorption	
Name		Debber	Desception	-
- 19				- 1
	virtual-machine Default		Default configuration	-
	citual machine Default (2)		Delasit configuration	-
	virtual-machine Debuit (3)		Default configuration	-
	citual machine Default (4)		Default configuration	-
	rmachine Default (2)		Default configuration	-
couchies				
	ope Default Policy for Couchbase Ser		This policy is read-only, and it captures and stores all the operations on Coudhase server. You can activate the example rules by deleting '#" character at the beginning of the rule orteria.	_
lama	wheet Default (3)	couldese	Default configuration	
monge	10			
di-test	-machine Default	manga	Default configuration	_
vounty	Assit Default (2)	mongo	Default configuration	_
sharts	next Default (3)	mungo	Default configuration	
starts	nest Default (4)	mongo	Debut configuration	
mysel (0			
41-102	machine Default (8)	mysol	Default configuration	
operates	enh CD			
Denk	ope Default Policy for Operdearch Se	operocarch	This policy is need only, and it captures and stores all the operations on OperGranch server. You can activate the example rules by deleting 'V' character at the beginning of the rule oftens.	
-	CE Carlanti	operation	Default configuration	
oracle (8			
++72,5	ent Default	onada	Default configuration	
oracler	sig-server Default	orade	Default configuration	
where	next Default	onacle	Default configuration	
	worth-2 Oethuit	arade	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	CAN	ICEL	

Options

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

Agents OpenVAS				
Agents Policies Options				
Default Certificate	Default Certificate			
Used for agents of version 3.2.0.4084 an	d higher			
Agent Security Certificate (.crt) *				
dsim_server.ort file selected.		Remove		
Agent Key File (.key) *				
dsim_server.key file selected.		Remove		
Client Certificate *				
dsim_client.pfx file selected.		Remove		
Password *				
	5478	CANCEL		

Alert Rules

						List of soles containing
Real Time A	åerts				Search here.	
Alers Ended Y S	everity Name		Update Date	Contains in Keyword	*	
Anaparant I	Marring Policy of	clation	20129-11-02 21/29/29			
	Barring Hardwa	* Configuration Changed	2020-11-02 21-08/01			
	Marring Low did	i space	2023-00-22 11:00:30			
	Harring 14 Max	an faileith	2018-01-0813-40-44			
	Marring Tala La	lies Keline Kullanm	2022-09-13 10:42:45			
atorg Dista	Barring Hardwa	w Configuration Changed (instal	2023-01-28 0022-33			
	Barring New Par	fern halt	2024-08-07 1513-49			
	Barring Nave Pat		2024-08-19 14:06:10			
Rect						
alatity						
69.						
red on Users						
figerce						
Case Allerts						
SET WALL RE PUBLISHED						
Asward						
let .						
eq.						
oy .						

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

Column Details

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

Adding New Alert Rule

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

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

Pattern Editor			– 🗆 🗙	
New Patter	n			
Name: New Patte	em			
Severity: Warning	✓ Category: Real	Time Alerts 🗸 🗸	✓ Enabled	
All rules must or	ccur within 00.00.05 ③ Act	vity: 00.00.00 (5) to 23.59.59 (5)		
Suppress all sub	sequent matches for 00:00:00	Suppress by event params Event params to in	clude	
Rules Actions				
Name	Туре	Description	Add Rule 🗠	
			Generic Rule Respond to a single event	
			Missed Rule Respond to an event that does n within given interval	iot happen
			Multi-hit Rule Respond to an event that will oc N times within given interval	cur more than
			OK CANCEL	

Generic Rule

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

Rule Editor					-		×
New Rule	3						
Name:	New Rule			Event ID Source			
			?				
Criteria:				Parameter Name			
Criteria							
Correlation Key	Enter correlation key						
Description:	Enter description						
				ок		CANCEL	
Rule Editor				- o x			
New Rule							
Name	New Rule	Event ID Sour	ce				
	H.C.	riteria Helper					
		Simple Queries					
				 Event Source here' \$678] AND param6 like %axoo%' 			
		Lookup Lists Usa		2 series when because the personal			
Criteria:				- "Event Source here" AND param 1 NOT IN (0	lookupilst	ame]	
		EventID = 1234 AN	D Source	- Event Source here' AND ListContains (looku	plistname'	paravi2) =	true
	-						
Correlation Keyr	Enter correlation key						
Description	Enter description						
				OK CANCEL			

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.

Rule Editor			- o x
New Miss	ed Rule		
Name: Criteria:	New Missed Rule	?	Event ID Source
Correlation Key: Description:	Enter correlation key Enter description		
From:	00:00:00 C To: 00:00:00 C Interval: 00:01:00 C		OK CANCEL

Multi-hit Rule

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

Rule Editor					-		×
New Multi	-hit Rule						
Name: Criteria:	New Multi-hit Rule	?	Event ID Source	e			
	Enter correlation key Enter description						
Group By Key: Interval: Match Condition:	Enter group by key 00:00:30 COUNT(0 >= 100			ОК		CANCEL	

Mappings

Mappings			
 All Categories Energial 	Agent		Search here. X
a typenon	Enabled Y Name * Y Decorption Event Source	T found D T found Type	•
v 🗎 infraskope	USB Device Attached - Environment USB Device Attached Log - Entract Infraskope	19000 information	
In Frenal			
a Agent			
> In Detailage			
+ New Category	() Subsub + Hana, & Sala, B Dalama,		

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

Column Details

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

Add New Mappings

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

- 1. Enter Mapping Name.
- 2. Enter **Description**.
- 3. Fill in the **Criteria**, **Events Source** and **Event Type** sections.
- 4. Complete the **Input**, **Code** and **Output** sections as appropriate.

						-	
Name:							
Description	Description						
Criteria:	0	Event Source	4	Event Type			G
Input Cl		7	Code 🕨		Output		7
			<pre>1//Special characters (i,*,i,*) are not allowed in { //Infravous/server will automatically drop events in soon Rep(fisitiContext ev) { return true; return true; } </pre>	field names			
 Enabled 							
					SAVE	a	058

Lookup Lists

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

Purpose of use

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

List Types

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

Lookup Lists		
v hous	Advision Advision Advision der sino Nerse Advision Advision anset contraction Nerse Advision Advision anset contraction Nerse Nerse Nerse Advision anset contraction Nerse Nerse Nerse Nerse anset contractin <t< th=""></t<>	
Database Links		
- Perlet	Name	
> 🖿 wet	All loss	admins Sample usage parent in (Badming)
deteringe_bet2		
6elevinge,text3		
Di LDAP Liets	Value Column	10he
👻 🎦 Static Line	Yolas T	
Except 1	Administrative	
Star Lance		
3 See Category		
Admin (hum)		
Critical Processes	Muturk1	
Domain Controllers	Citik here to ad	d raw how
Domaine		
Exclude Appx		
Laganlypen		
pomonourseller liet (dynamic)		
Sect fails		
Institute		
 opriogentalisenips list (dynamic) 		
In these intelligence		
		4 ter
() fature		

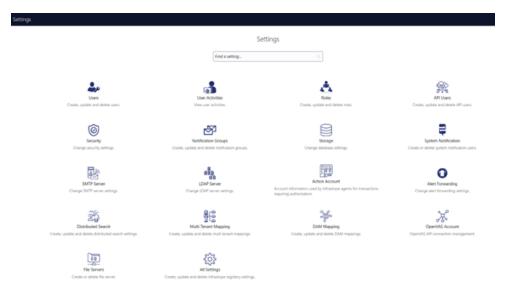
Clicking the Save button after each change to the list disables the automatic submission process, giving users the option to submit their modifications directly.

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

	Lookup Lists				
1	v Matten			To send the updates you wade to the borkup list in Databage to the agent, great the Cannel Softan.	
	> Desteux Lins	DAMeet		List Type: Datasia	ape .
	v ba	Name .	Designed		
	E DAM, and Extension, and	Alex	14	Sergie usep permit in (Brid)	
	Enteringen_text	Description	Enter a short description		
	b sort	Nature Columns	Volue		
	> In Tradic Lines	User T			
	> h Twat instigence	Appent?			
		itan2			
		Child here to a	Ad new York		

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

Settings



Ref.	Controls	Function
&	Users	Used to create, update, and delete users.
	User Activities	Used to view user activities.
A	Roles	Used to create, update, and delete roles.
	API Users	Used to create, update, and delete API Users.
0	Security	Used to change security settings.
₫	Notification Groups	Used to create, update, and delete notification groups.
	Storage	Used to change database settings.
Ę	System Notification	Used to create and delete system notification users.
	SMTP Server	Used to change SMTP server settings.

60 60	LDAP Server	Used to change LDAP server settings.
	Action Account	Used to reach account information by DAM agents.
•	Alert Forwarding	Used to change alert forwarding settings.
	Distributed Platform	Used to create, update, and delete distributed platform settings.
	Multi-Tenant Mapping	Used to create, update, and delete multi-tenant mappings.
O Refresh + New	VDAM Maping	Used to create, update and delete VDAM Mappings
Enabled Name Description		
dataskope mapping 3 dataskope test 12		
×	OpenVAS Account	Used to OpenVAS API connection management.
	File Servers	Used to create or delete file server.
	All Settings	Used to create, update, and delete DAM registry settings.

User Settings

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

Users

🔿 Refresh 🕂 New... 🐔 Edit... 🍵 Delete...

Login Enabled	Name	User Name	Roles	Email	Last Password Change Time	Last Login Time
~	Log Admin	logadmin	Admin	halit.dursun@karmasis.com	2023-09-29 22:29:26	2024-09-11 14:49:40
×	Murat Eraydin (AD)	meraydin@karmasis2Jocal	Users, Admin	murat.eraydin@karmasis.com	2022-06-22 19:25:31	
1	Mert Topçu	mert.topcu@karmasis2/ocal	Admin	mert.topcu@karmasis.com	2022-06-22 19/25/31	2023-08-03 14:01:59
1	Publisher Operator	publisher	Admin	fulyauluturk@karmasis.com	2022-06-22 19/25:31	2022-10-04 13:32:19
\checkmark	nuray.caylan	Nuray Çaylan	Admin	nuray caylan@karmasis.com	2022-06-22 19:25:31	- C
\sim	Sezgin Alterkeya	saltinkaya@karmasis2.local	Admin	seginaltinksys@karnasis.com	2022-06-22 19/25/31	2023-02-13 14:30:22
×	Can Çopur	can.copur@karmasis2.local	Admin, Dataskope	can copur@karmasis.com	2022-06-22 19:25:31	2023-12-20 10:24:57
<u>×</u>	Database Audit Admin	dbadmin	Dataskope	dbadmin@kamasis.com	2022-06-22 19:25:31	
×	Micro Focus	microfocus	Admin	karmasisapi@karmasis.com	2022-06-22 19:25:31	
	Ali Ekortobi	ekortobi	Dataskope Group	al.ekortobi@microfocus.com	2022-06-22 19:25:31	2019-12-17 10:44:33
~	SIEM Test	siemtest	TestSIEM	sion@karmasis.com	2022-06-22 19:25:31	2020-06-17 12:31:34
\checkmark	STM	stm	Read-Only User	stm@karmasis.com	2022-06-22 19/25/31	2020-07-08 11:01:29
\checkmark	STM2	stm2	test_default	stm@karmasis.com	2022-06-22 19:25:31	2020-07-08 10:36:05
\checkmark	Company1	company1	Company1	company1@karmasis.com	2022-06-22 19/25/31	2021-02-25 14:03:01
1	Company2	company2	Company2	company2@karmasis.com	2022-06-22 19:25:31	2021-02-25 14:06:51
1	Company3	company3	Company3	company3@karmasis.com	2022-06-22 19:25:31	2021-02-25 14:12:38
×	Gokhan KANA	goldran.kaya	Admin	ttgolchankaya@gmail.com	2022-08-16 15:00:01	
×	Hasan	hasan.keskin	Users, test_debuilt, EGM TEST - AD	hasan.keskin@karmasis.com	2023-01-18 10/03/56	2023-01-18 10:04:53
\checkmark	Halit Dursun	halit.dursun@karmasin2.local	Admin	haitdursun@gmail.com		2023-11-01 11:12:48
×	can kargi	ckargi	Users, test_default, Admin	can kargi@karmasis.com	2024-02-26 00:00:00	

Adding New User

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

i User	- D X New User	- O X New User	- 0
NEW ROLE NOTIFICATION GROUPS	GRANAL ROUS NOTIFICATION GROUPS	GINERAL ROUS NOTIFICATION GROUPS	
User Information	Admin	Cvfsult0*5	
Nane	✓ Uses	Security Opti	
	Cutashope	iduri	
Inal	✓ tetteftett	Tylenik	
ible hore	Datashope Group	MSMD Ope	
NS Number	See	%st	
	147.005	Dev .	
count Information	Tites API	Des2	
se Name	Twefdbir	60w 100* Schedule Tech Group	
Alter .	Read-Only User	Science intraction	
Expires on	Company1		
Uner Defaitsuch	Congeny2		
	Company3		
luthentication	Admin Role Text		
et Random Resevord	564 BOM TEST - ADMIN ROLE		
and the second	UDW TEST - ADMIN ROLE		
perfere Passered	EGM TEST - USER RECE		
Should change password on work login			
lser inactivity			
Inactivity logical			
Land	CANETA	Last Carros	Sect. Gentle

User Activities Settings

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

User Activities

Diag a column header	and drop it have to group by	that column					ACTIVITY DETAIL	5			
line Generated	Computer Name	T OS User Name	T IP Address T	Operator 7	Module T	Action	(
2024-09-11 16:53:51	KFMOTT000	burnakuruk	192.168.1.3	Log Admin	Publisher	GelCulturer 1	"Service": "Public "Action": "SetCo "Method": "SET"				
2024-09-11 16:51:47	KFMOT7009	bustakucuk	192,166.1.3	Log Admin	Uses	GetOperators)				
2024-09-11 16:51:13	GZGETUNCER-PC	coget	192.168.1.132	Log Admin	Publisher	GetCustomer					
2524-09-11 16:50 12	KFMOT7009	buseakucuk	192,168.1.3	Log Admin	Operations	GetCuratorSettings					
2024-09-11 16:46:17	KFMOTT003	burnakuruk	192,168,1.3	Log Admin	Basticfunctions	Alarta					
2524-09-11 16:46:03	KFMC/T1003	bustakucuk	192,166.1.3	Log Admin	EasticFunctions	Search					
2024-09-11 16:46:03	KFMDIT1003	burnakucuk	192,168,1,3	Log Admin	EasticFunctions	Search					
2024-09-11 16:46:03	KFMDIT1003	bustakucuk	192,166.1.3	Log Admin	Eastichunctions	Search					
2024-09-11 16:46:02	KFMDIT000	burnituruk	192.168.1.3	Log Admin	DasticFunctions	Alarta					
2024-09-11 16:45:47	KFMO#1003	bustakucuk	192.168.1.3	Log Admin	Easticfunctions	Alerts					
2024-09-11 16:45:33	KFMDIT003	burnituruit	192.168.1.3	Log Admin	Dasticfunctions	Search					
2024-09-11 16:45:33	KFMOT7003	busikkucuk	192,168.1.3	Log Admin	Bastichunctions	Search					
2024-09-11 16:45:33	KFNOTT000	burnituruit	192,168.1.3	Log Admin	DasticFunctions	Search					
2024-09-11 1645-32	KFMOT7003	busekucuk	192,168.1.3	Log Admin	Eastichunctions	Alets					
2024-09-11 16:49:17	KFMDIT000	burnituruk	192,168,1.3	Log Admin	DasticFunctions	Alarts					
2024-09-11 16:45:03	KPNOT1009	busekucuk	192.168.1.3	Log Admin	Eastichunctions	Search					
2024-09-11 16:45:02	KFMDIT003	burnalisesk	192,168,1.3	Log Admin	Basticfunctions	Alarta					
2024-09-11 16:44.47	KFMC#1008	busekucuk	192,146.1.3	Log Admin	Eastichunctions	Alens					
2024-09-11 16:44:33	KFMOIT003	burnakuruk	192,168,1.3	Log Admin	DasticFunctions	Search					
2024-09-11 16:44:33	KFMC/T1003	busekucuk	192,168.1.3	Log Admin	Eastichunctions	Search	Section (D)	54814829-6312-4035-867			Meiniz
2024-09-11 16:44:33	KPM011003	burnituruk	192,168,1.3	Log Admin	DasticFunctions	Search	Computer Name		OS User Name		
2024-09-1116-4432	KFMOT7003	besteleycolt	192,146.1.3	Log Admin	Eastchunctions	Alets	IP Address	192,168.1.3	Operator	Log Admin	

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

Default	Outside Connection	Role Name	Description
		Admin	This role has access to all features.
		Admin Role Test	
		Company1	
		Company2	
		Company3	
		Dataskope	
		Dataskope Group	
		EGM TEST - ADMIN ROLE	
		EGM TEST - USER ROLE	
		INTERN	Stajyer Grubu
		Read-Only User	
		Sales	
		Test	Halit test1
\checkmark		test_default	
		TestSIEM	
\checkmark		Users	Read only user with full logs access.
		Web API	Used for connections outside the Infraskope

Adding a New Role

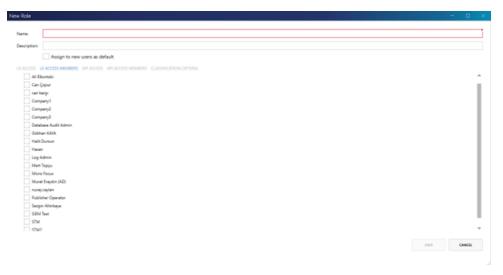
This is used to customize the access scope as desired when adding a new role.

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

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

ni -	
stription:	
Assign to new users as default	
ACCESS UFACCESS MEMBERS APEACESS MEMBERS CLASSFICATION CRITERIA	
	• or
Q Search Search logs, create, update and delete queries.	• or
the Alerts You can view and export alarms.	• or
S B Dashboards Dashboards that are created by users with log types of their choice that displays strategical information of their system. Users can also view built in dashboards published by OpenTest.	• or
Ge Agents Agents management.	• or
A Vert Rules Built in alert notes published by OpenText and custom alert notes that are defined by users.	• or
B Mappings Create, update and delete event mappings.	• or
§ 1.3 Lookup Lists: Built in look-up fast published by OpenText and custom look-up lists that are defined by users.	• or
Settings System settings.	• or

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



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

SAVE CANCEL

An and a second s	- 0
lgfon	
Assign to new users as default	
CESS UFACCESS MEMBERS APLACCESS APLACCESS MEMBERS CLASSIFICATION CRITERIA	
jg: Search By Events	• • •

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

New Role		- 0 X
Name		
Description		
Assign to new users as default		
UFACCESS OF ACCESS MINIBERS APLACCESS APLACESS MINIBER CLAUSIFICATION OFFERA		
alf-user		
_ test		
tenApUter		
	3498	CANCEL

- 8. In CLASSIFICATION CRITERIA, check Activate Classification if necessary.
- 9. Select Field Queries or Raw Query String and complete the relevant details.

w Role		- 0 >
Name		
Description		
Assign to new users as default		
U ACCESS. ULACCESS MEMBERS: APLACCESS. APLACCESS MEMBERS: CLASSIFICATION OFTENIA		
Activate Classification		
Field Queries		
× Must Files +	X Must NOT Filters +	
Raw Query String		
Company Names		
		SAVE CANCEL

API Users Settings

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

API Users

Active	User Name	Name	Role
~	api-user	api-user	
\checkmark	microfocus	Microfocus API	
~	test	test	Admin Role Test
\checkmark	TestApiUser	TestApiUser	
\checkmark	user-test	user-test	Admin Role Test

Adding a New API User

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

w User			-
Account Inform	nation		
Name:			
User Name:			
Role:			~
Active			
 Expires on 	Enter date		Ē
Authentication			
Password:			₽□
		SAVE	CANCEL

NOTE:

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

Security Settings

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

Security
Password Complexity
✓ Use default settings
Require digit
Require lowercase
Require non alphanumeric
Require uppercase
Required length
8
Password Change
Set password change interval for all users
SAVE CANCEL

Notification Group Settings

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

Notification Groups

🛅 Delete	
Description	Email
Default Operators Group.	
	idari@karmasis.com
Dev	
	halit.001@
	Default Operators Group.

Adding a New Notification Group

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

New Notification Group				
Group Name:				
Description:				
Email (Distribution List):				
Users:	Log Admin			î
	Murat Eraydın (AD)			
	Mert Topçu			
	Publisher Operator			
	nuray.caylan			
	Sezgin Altınkaya			
	Can Çopur			Ŧ
	SAVE	•	CANCEL	

Storage Settings

Main Storage Settings

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

Storage

 Statuses
 Statuses
 Oata Sources

 Number of Shuds:
 1
 Image: Activate name database
 Image: Activate name
 Image: Activate name
 Image: Activate name

Storage Security Settings

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

Storage

SETTINGS SECURITY IMPORT ARCHIVE RESTORE FROM BACKUP CURATOR SETTINGS

Elasticsearch Credentials

User Name:	elastic	
Old Password:		
New Password:		
Confirm Password:		
	SAVE	CANCEL

Import Archive Settings

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

Storage

SETTINGS	SECURITY	IMPORT ARCHIV	E RESTORE FROM BACKUP	CURATOR	SETTINGS	
2021-0	9-30		2023-09-17		RESTORE	REFRESH
Select dat	tes and click	restore to start im	port from archive process.			

Restore from Backup

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

Storage

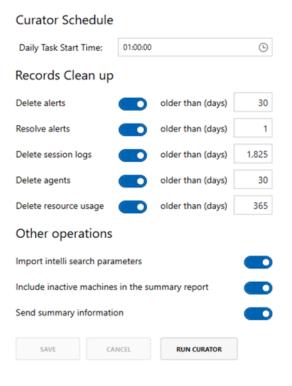
SETTINGS SECURITY IMPORTANCINE RESTORE FROM BACILIP CURITOR SETTINGS	
C Rahush	Create & Restore All
2023-07-26 Missing index. (Backup not found.)	Re-create Index
2023-07-27 Missing index. (Backup not found.)	Re-create Index
2023-09-01 Missing index. (Backup not found.)	Re-create Index
2023-09-02 Missing index. (Backup not found.)	Re-create Index

Storage Curator Settings

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

Storage

SETTINGS SECURITY IMPORT ARCHIVE RESTORE FROM BACKUP CURATOR SETTINGS



System Notification Settings

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

System Notification

E-mail Addresses

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

C Refresh	+ New	Î	Delete
halit.dursun@	karmasis.com		

SMTP Server Settings

This setting can be utilized to configure mail service settings.

SMTP Server

SMTP Settings

SMTP Server:	smtp.office365.com
SMTP Port:	587 SSL Enabled
SMTP From Address:	infraskope@karmasis.com

Authentication Settings

User Name:	infraskope@	karmasis.com
Password:	•••••	
SAVE	CANCEL	SEND TEST E-MAIL

LDAP Server Settings

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

LDAP Server

LDAP Server	
LDAP Server:	DC3.karmasis2.local
Example;	companydc.karma.intra/OU=CompanySUBOU,OU=CompanyOU,DC=karma,DC=intra IP / Host Sub OU (Optional) Parent OU (Optional) Domain Name
Authentication S	ettings
 Authentication Rec 	uired
User Name:	karmasis2\meraydin
Password:	•••••
SAVE	CANCEL

Action Account Settings

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

Action Account

Domain Name:	KARMASIS2	
User Name:	action	
Password:	•••••	•
SAVE	CANCEL	TEST CONNECTION

Alert Forwarding Settings

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

Alert Forwarding

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

 Enable Alert For 	orwarding				
Site Name (Active	Directory):	Test site code			
Parent Site Name (Active Directory):				
		Tes	t Alert Forwarding		
Forward Aler	ts On uesday 🗌 Wednes	sday 🗌 Thursda	y 🗌 Friday 🗌 S	Saturday Sunday	/
Hours Allowe	ed				
0AM	6AM	12PM	18PM	23PM	CHECK ALL
					CLEAR ALL
SAVE	CANCEL				

Distributed Search Settings

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

Distribut	ed 9	Search	h
Distribut	eu.	searci	1

🖌 Enable Cross Ouster	Search						
Cluster Manage Urb	Main Cluster URL						
Authentication							
UserName: elasti	ic .						
Passwordt							
TEST CONNECTION		SAVE CA	NCEL				
Seeds							
C Refresh + New	💪 Edit 🍵 Delete						
Name Cluster	Name ES	URLS	Cross Cluster Search Status	IP Address	Port	Include in Cross Cluster Search	Include in Manage APIs

Multi-Tenant Mapping Settings

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

Multi Tenant Mapping

Enabled	Name	Description
\checkmark	Dataskope Fieldname Normalization	
	Dataskope Field Name Normalization - Fo	or Microfocu:
~	Dataskope Enrichment - extract real user	from uid_cha
\checkmark	Oracle Zenginleştirme - Adalet Bak. v1	
	Oracle Audit - Clear Null Chars	
\checkmark	Oracle Zenginlestirme - Adalet v2	

DAM Mapping

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

DAM Mapping



OpenVAS Account Settings

To connect an OpenVAS account, credentials should be entered.

OpenVAS Account

API Address:	http://192.1	68.1.97:9393			
User Name:	admin				
Password:	•••••	•			
✓ Enable OpenVAS API connection					
TEST CONNECTION		SAVE	CANCEL		

File Server Settings

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

File Servers

C Ref	resh 🕈 New., 🖻 Edit.,	Delete					
InUse	Name	Description	Protocol	SSL Mode	Server Address	Port	Path
20	192,168,1.40		FTP	None	192.168.1.40	21	
	192,168,1.74		SETP	Nore	192.148.1.74	22	
	192,168,1.129 (hp)	fφ	FTP	None	192.168.1.129	21	/home/schedule-reports
	Curator FTP Server		SITP	Explot	192.168.1.254	21	

Figure 1: File Server Settings

t	Description:			
	Descriptions			
ţ	Protocol	SFTP		
5	SSL Mode:	None		
5	Server Address:			
1	Port:	22		
,	User Name:			
1	Password:			
;	Path:			

All Settings

Accessing and modifying all settings on this screen is possible.

All Settings

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

G	Refresh + New 🖉 Edit 🧰 Delete
	Name Value
•	Section: Admins (1)
•	Section: AlertRules (1)
•	Section: ClientMonitoring (3)
•	Section: DailyArchiver (1)
	Section: DailyJobs (4)
•	Section: DataMaskExpressions (7)
	Section: DataMaskSettings (2)
	Section: dataskopecollectors (5)
•	Section: ESServer (24)
	Section: Helpdesk (4)
•	Section: InfraskopeSiemPlus (1)
•	Section: Kafka (1)
•	Section: KafkaCluster (4)
	Section: Nessus (3)

Setting Editor

Section:				
Name:	New name			
Value:	New value			
Is Password				
Passwo	Password:			
Confirm Password:				

SAVE

CANCEL

×