Forcepoint

Log Export Variation Sheet

.

Revision A

Contents

- WEB on page 2
- ADMIN on page 6
- HEALTH on page 8
- CASBAPI on page 11
- ZTNA on page 15
- DLP on page 18
- CASBINLINE on page 20

WEB

The default fields to be exported for **Insights Collection** - **SWG** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1	syslogheader			NA		■ <114>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE swgweb ■ <110>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE swgweb
2	time	eventtime	time	eventtime	Time	
3	indexedtime	eventinsertedtime	eventinsertedtime	eventinsertedtime		

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
4	deviceguid	did	deviceid	did	Device ID	
5	ipaddress	dvi	localip	dvi	Local IP	
6	destinationip	dsi	destinationip	dsi	Destination IP	
7	uri	uri	uripath	uri	URI Path	
8	requestdomain	dom	domain	dom	Domain Name	
9	arguments	arg	requestargs	arg	Request Args	
10	requestmethod	rmd	httprequest method	rmd	HTTP Request Method	
11	protocol	ptl	application layerprotocol	ptl	Application Layer Protocol	
12	firstname	ufn	userfirstname	ufn	User First Name	
13	lastname	uln	userlastname	uln	User Last Name	
14	email	upn	username	upn	Username	
15	usergroup	gid	groupids	gid	Group IDs	
16	action	act	action	act	Action	
17	devicehostname	dhn	hostname	dhn	Hostname	
18	setransactionid	nxd	requestid	nxd	Request Id	
19	size	rbt	bytesreceived	rbt	Bytes Received	
20	uploadedbytes	sbt	bytessent	sbt	Bytes Sent	
21	useragent	uag	useragent	uag	User Agent	
22			urlcategory	tsc	URL Category	
23			urlreputation	tss	URL Reputation	
24			urlreputationvalue	trsk	URL Reputation Value	
25	lat	lat	latitude	lat	Latitude	
26	long	lon	longitude	lon	Longitude	
27	city	cty	city	cty	City	
28	country	cry	country	cry	Country	
29	countrycode	crc	countrycode	crc	Country Code	
30	region	reg	region	reg	Region	
31	regioncode	rgc	regioncode	rgc	Region Code	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
32	customlocation	csl	customlocation name	csl	Custom Location Name	
33	customcategories	cct	customcategory	cct	Custom Category	
34	referrer	ref	referrerheader	ref	Referrer Header	
35	application	apn	applicationname	apn	Application Name	
36	requestport	prt	requestport	prt	Request Port	
37	url	url	url	url	URL	
38	policyid	dpi	policyid	dpi	Policy ID	

The fields which are not exported by default for **SSE Log Type** - **swgweb** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1			proxytype	pxy	Proxy Type	
2			gatewayip	gwi	Gateway IP	
3			privateip	pvi	Private IP	
4			enterpriseapps corevalue	brsk	Enterprise App Score Value	
5			groups	gdn	Groups	
6			downloadpolicy action	dla	Download Policy Action	
7			localizedcountry	lct	Localized Country	
8			device	dos	Device	
9			traffictype	ttp	Traffic Type	
10			customersitename	snm	Customer Site Name	
11			connectiontype	con	Connection Type	
12			ikeid	ike	IKE ID	
13			ntlmid	nid	NTLM ID	
14			authentication method	aum	Authentication Method	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
15			authentication policyid	uai	Authentication Policy ID	
16			binaryexefilename	bin	Binary exe filename	
17			shorteneddomain	tdn	Shortened Domain	
18			destinationurl	durl	Destination URL	
19			webreputationvalue	rsk	Web Reputation Value	
20			responsestatuscode forclassify request	crs	Response Status Code For Classify Request	
21			filedownload markers	fdm	File Download Markers	
22			fileuploadmarkers	fum	File Upload Markers	
23			userid	lui	User ID	
24			webclassificationa1 attribute	wra	Web Classification A1 attribute	
25			bytesreceived	rbt	Bytes Received	
26			bytessent	sbt	Bytes Sent	
27	webcategories	wrc	webbrowsing categories	wrc	Web Browsing Categories	
28	webreputation	wrr	webreputation	wrr	Web Reputation	
29	webcategoryclass	wcc	webbrowsingclass	wcc	Web Browsing Class	
30	bgcategories	bgc	enterpriseapp categories	bgc	Enterprise App Categories	
31	bgcloudscore	bgs	enterpriseappscore	bgs	Enterprise App Score	

ADMIN

The default fields to be exported for **Insights Collection** - **ADMIN** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1	syslogheader			NA		
2	time	eventtime	eventtime	eventtime	Event Time	
3	user	udn	userfullname	udn	User Full Name	
4	email	upn	username	upn	Username	
5	device	dos	devicename	dos	Device Name	
6	application	apn	applicationname	apn	Application Name	
7	ipaddress	dip	publicip	dip	Public IP	
8	location	cty || reg || rgc || crc		NA		Transformation not supported
9	activity	tgs	allactivities	tgs	All Activities	
10	action	atgs	action	atgs	Action	
11	useragent	uag	useragent	uag	User Agent	
12	request			NA		
13	transactionid	apd	transactionid	apd	Transaction ID	
14	emailfrom			NA		
15	emailto			NA		
16	emailsubject			NA		
17	emailcc			NA		
18	emailbcc			NA		
19	emailsenttime			NA		
20	filename	fnm	filename	fnm	File Name	
21	dlppattern			NA		
22	pagetitle			NA		
23	url	uri	requesturi	uri	Request URI	
24	details	msg	details	msg	Details	
25			city	cty	City	
26			region	reg	Region	
27			regioncode	rgc	Region Code	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
28			countrycode	crc	Country Code	

The fields which are not exported by default for **SSE Log Type** - **admin** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1			deviceid	did	Device ID	
2			country	cry	Country	
3			customregion	creg	Custom Region	
4			activity	acd	Activity	
5			userfirstname	ufn	User First Name	
6			userlastname	uln	User Last Name	
7			fileextension	ext	File Extension	
8			documenttype	ftp	Document Type	
9			accessmethod	acm	Access Method	
10			operatingsystem	hos	Operating System	
11			latitude	lat	Latitude	
12			longitude	lon	Longitude	
13			locationaccuracy	acc	Location Accuracy	
14			sforganizationid	org	SF Organization ID	
15			instancename	inm	Instance Name	
16			cloudapplicationid	aid	Cloud Application ID	
17			userid	lui	User ID	
18			groupids	gid	Group IDs	
19			group	gdn	Group	
20			userdisplaygroup	udg	User Display Group	
21			awsnodename internal	nod		
22			policyid	dpi	Policy ID	
23			notifyid	ntd	Notify ID	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
24			logkey	lgk	Log Key	
25			logtype	typ	Log Type	
26			model	mdl	Model	
27			bgid	bid	BG ID	
28			iaastype	ityp	IAAS Type	
29			violatingresources	vlr	Violating Resources	
30			lastscanned	lsc	Last Scanned	
31			filesize	fsz	File Size	
32			eventinsertedtime	eventinsertedtime		

HEALTH

The default fields to be exported for **Insights Collection** - **HEALTH** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1	syslogheader					■ <114>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE healthapi ■ <110>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE healthapi ■ <114>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE healthsystem ■ <110>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE healthsystem
2	time	eventtime	eventtime	eventtime	Event Time	
3	user	udn	userfullname	udn	User Full Name	
4	email	upn	username	upn	Username	
5	usergroup	gdn	group	gdn	Group	
6	device	dos	devicename	dos	Device Name	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
7	application	apn	applicationname	apn	Application Name	
8	activity	tgs	allactivities	tgs	All Activities	
9	url	uri	requesturi	uri	Request URI	
10	responsecode	rsc	responsecode	rsc	Response Code	
11	transactionid	apd	transactionid	apd	Transaction ID	
12	deviceguid	did	deviceid	did	Device ID	
13	ipaddress	dip	publicip	dip	Public IP	
14	location	cty || reg || rgc || crc		NA		
15	requestmethod	rmd	httprequest method	rmd	HTTP Request Method	
16	useragent	uag	useragent	uag	User Agent	
17	filename	fnm	filename	fnm	File Name	
18	fileid	fid	fileid	fid	File ID	
19	status	stt	status	stt	Status	
20			city	cty	City	
21			region	reg	Region	
22			regioncode	rgc	Region Code	
23			countrycode	crc	Country Code	
24			logtype	lgt	Log Type	

The fields which are not exported by default for **SSE Log Type - healthsystem (lgt=SystemHealth)** and **SSE Log Type - healthapi (lgt = APIHealth)** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1			activity	acd	Activity	
2			details	msg	Details	
3			userfirstname	ufn	User First Name	
4			userlastname	uln	User Last Name	
5			customregion	creg	Custom Region	
6			country	cry	Country	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
7			operatingsystem	hos	Operating System	
8			latitude	lat	Latitude	
9			longitude	lon	Longitude	
10			locationaccuracy	acc	Location Accuracy	
11			userid	lui	User ID	
12			userdisplaygroup	udg	User Display Group	
13			groupids	gid	Group IDs	
14			logkey	lgk	Log Key	
15			cloudapplicationid	aid	Cloud Application ID	
16			awsnodename internal	nod		
17			eventinsertedtime	eventinsertedtime		

CASBAPI

The default fields to be exported for **Insights Collection** - **CASBAPI** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1	syslogheader					■ <114>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE cloudaudit ■ <110>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE cloudaudit
2	filename	fnm	filename	fnm	File Name	
3	time	eventtime	eventtime	eventtime	Event Time	
4	size	fsz	filesize	fsz	File Size	
5	owner	own	owner	own	Owner	
6	application	apn	application	apn	Application	
7	status	stt	status	stt	Status	
8	action	act	action	act	Action	
9	folder	fld	path	fld	Path	
10	fileid	fid	fileid	fid	File ID	
11	patterns	dptn	dlppatternswith contextdata	dptn	DLP Patterns with Context Data	
12	filelink	link	link	link	Link	
13	sharedwith	shd	sharedwith	shd	Shared With	
14	originalstatus	ofStatus	originalfilestatus	ofStatus	Original File Status	
15	original sharedwith	ofShared	originalfile sharedwith	ofShared	Original File Shared With	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
16	quarantine filename	qfFileName	actionfilename	afName	Action File Name	
17	quarantinefileid	qfid	actionfileid	afid	Action File Id	
18	notification filename	nfFileName	notification filename	nfFileName	Notification File Name	
19	notificationfileid	nfid	notificationfileid	nfid	Notification File ID	
20	activity	acd	activitydetail	acd	Activity Detail	
21	copies	afName +afOwner +afStatus+afPath +afLink				
22	policyid	dpi	policyid	dpi	Policy ID	
23	enterprisename	tmn	teams	tmn	Teams	
24	createdtime	crt	createdsent	crt	Created Sent	
25	modifiedtime	mod	objectmodified	mod	Object Modified	
26	actoripaddress	aip	actorip	aip	Actor IP	
27	actor	atr	actoremail	atr	Actor Email	
28			actionfileowner	afOwner	Action File Owner	
29			actionfilestatus	afStatus	Action File Status	
30			actionfilelink	afLink	Action File Link	
31			actionfilepath	afPath	Action File Path	
32			previouslabel	plbl		
			search	srch		

The fields which are not exported by default for **SSE Log Type** - **cloudaudit** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1			activity	acv	Activity	
2			dlppatterns	dlp	DLP Patterns	
3			groups	gdn	Groups	
4			hash	hsh	Hash	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
5			classifylabels	csl	Classify Labels	
6			label	lbl	Label	
7			scanincluded groups	sci	Scan Included Groups	
8			scanexcluded groups	sce	Scan Excluded Groups	
9			scanincluded sites	scis	Scan Included Sites	
10			scanexcluded sites	sces	Scan Excluded Sites	
11			scanincluded buckets	scib	Scan Included Buckets	
12			scanexcluded buckets	sceb	Scan Excluded Buckets	
13			scandatapatterns	scdp	Scan Data Patterns	
14			threatindicator	thi	Threat Indicator	
15			zipfileinfo	zip	Zip File Info	
16			sitename	snm	Site Name	
17			emailbcc	bce	Email BCC	
18			emailcc	cce	Email CC	
19			emailto	toe	Email To	
20			emailfrom	fre	Email From	
21			logkey	lgk	Log Key	
22			applicationcode	app	Application Code	
23			apiconfigid	aci	API Config ID	
24			salesforce organizationid	org	Salesforce Organization ID	
25			groupids	gid	Group IDs	
26			eventtype	typ	Event Type	
27			actionfile destinationapp	afDestApp	Action File Destination App	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
28			actionfile appinstance	afAppInst	Action File App Instance	
29			notification fileowner	nfOwner	Notification File Owner	
30			notification filestatus	nfStatus	Notification File Status	
31			notification filepath	nfPath	Notification File Path	
32			exposures	estt	Exposures	
33			datacontext	ptn	Data Context	
34			userdisplaygroup	udg	User Display Group	
35			notificationid	ntfyid	Notification ID	
36			allactivities	tgs	All Activities	
37			eventinsertedtime	eventinsertedtime		

ZTNA

The default fields to be exported for **Insights Collection - ZTNA** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1	syslogheader					■ <114>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE ztna ■ <110>1 2025-07-30T09:49:00.000000Z api.bitglass.com NILVALUE NILVALUE ztna
2	time	eventTime	time	eventTime	Time	
3	policyid	dpi	policyid	dpi	Policy ID	
4	email	upn	username	upn	Username	
5	action	act	action	act	Action	
6	ztnatransactionid	nxd	ztnatransactionid	nxd	ZTNA Transaction ID	
7	service	ptl	service	ptl	Service	
8	protocol	ptc	protocol	ptc	Protocol	
9	ztnatype	ztyp	logtype	ztyp	Log Type	
10	application	apn	applicationname	apn	Application Name	
11	ipaddress	gwi	gatewayip	gwi	Gateway IP	
12	city	cty	city	cty	City	
13	region	reg	region	reg	Region	
14	country	cry	country	cry	Country	
15	countrycode	crc	countrycode	crc	Country Code	
16	regioncode	rgc	regioncode	rgc	Region Code	
17	device	dos	device	dos	Device Name	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
18	devicehostname	dhn	devicehostname	dhn	Device Hostname	
19	machineuser	mus	machineuser	mus	Machine User	
20	deviceguid	did	deviceguid	did	Device GUID	
21	requestdomain	dom	domain	dom	Domain	
22	uri	uri	uripath	uri	URI Path	
23	url	url	url	url	URL	
24	arguments	arg	requestargs	arg	Request Args	
25	servicehostname	svh	servicehostname	svh	Service Hostname	
26	destinationip	dsi	destinationip	dsi	Destination IP	
27	requestport	prt	port	prt	Port	
28	responsecode	err	agentresponse code	err	Agent Response Code	
29	datacenter	dtc	datacenter	dtc	Data Center	
30	connector	cnn	connectorname	cnn	Connector Name	
31	availabilityzone	zaz	availabilityzone	zaz	Availability Zone	
32	userid	lui	userid	lui	User ID	
33	usergroup	gid	groupids	gid	Group IDs	
34	localipaddress	dvi	localip	dvi	Local IP	
35	privateipaddress	pvi	privateip	pvi	Private IP	
36	lat	lat	latitude	lat	Latitude	
37	long	lon	longitude	lon	Longitude	
38	firstname	ufn	userfirstname	ufn	User First Name	
39	lastname	uln	userlastname	uln	User Last Name	
40	proxytype	pxy	proxytype	pxy	Proxy Type	
41	traffictype	ttp	traffictype	ttp	Traffic Type	
42	sitename	snm	sitename	snm	Site Name	
43	customsite location	csl	customlocation name	csl	Custom Location Name	
44	connectiontype	con	connectiontype	con	Connection Type	
45	uploadedbytes	sbt	bytessent	sbt	Bytes Sent	

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
46	size	rbt	bytesreceived	rbt	Bytes Received	

The fields which are not exported by default for **SSE Log Type** - **ztna** are given below.

	Current Export API		New Export API			Notes
SNo	Exported Name	Column Name	Splunk/Script Exported Name	Column Name	QRadar Exported Name	
1			usergroups	gdn	User Groups	
2			streamsession end	ssc	Stream Session End	
3			streamsession start	sss	Stream Session Start	
4			ikeid	ike	IKE ID	
5			eventinsertedtime	eventinsertedtime		

DLP

The default fields to be exported for **Insights Collection** - **DLP** are given below.

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
1	eventtime	eventTime	Event Time
2	eventinsertedtime	eventinsertedtime	
3	transactionid	apd	Transaction ID
4	requestid	nxd	Request Id
5	proxytype	stp	Proxy Type
6	applicationname	apn	Application Name
7	dlpaction	dlpact	DLP Action
8	action	atgs	Action
9	filename	fnm	File Name
10	username	upn	Username
11	userfullname	udn	User Full Name

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
12	allpatterns	csl	All Patterns
13	allkeywords	kwd	All Keywords
14	allactivities	tgs	All Activities
15	malwarethreat	trt	Malware Threat
16	uri	uri	URI
17	documenttype	ftp	Document Type
18	fileextension	ext	File Extension
19	filesha256hash	sh256	File SHA256 Hash
20	filesha1hash	sh1	File SHA1 Hash
21	filemd5hash	md5	File MD5 Hash
22	group	gdn	Group
23	deviceid	did	Device ID
24	device	dos	Device
25	useragent	uag	User Agent
26	dlpsourceip	dip	DLP Source IP
27	city	cty	City
28	countrycode	crc	Country Code
29	region	reg	Region
30	regioncode	rgc	Region Code
31	salesforce organizationid	sorg	Salesforce Organization ID
32	policyid	dpi	Policy ID

The fields which are not exported by default for **SSE Log Type** - **NA** are given below.

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
1	notifications appliedid	ntfyid	Notifications Applied ID
2	userdisplaygroup	udg	User Display Group
3	filetransactionid	fapd	File Transaction ID

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
4	filesize	fsz	File Size
5	activity	acd	Activity
6	actionpattern	acsl	Action Pattern
7	userfirstname	ufn	User First Name
8	userlastname	uln	User Last Name
9	actionkeywords	akwd	Action Keywords
10	domain	dom	Domain
11	url	url	URL
12	country	cry	Country
13	customregion	creg	Custom Region
14	latitude	lat	Latitude
15	longitude	lon	Longitude
16	alert	alert	Alert
17	notifications applied	ntd	Notifications Applied
18	dlpmatchlocation	dml	DLP Match Location
19	manageddevice	mng	Managed Device
20	managed application	mngapp	Managed Application
21	cloudapplicationid	aid	Cloud Application ID
22	userid	lui	User ID
23	groupids	gid	Group IDs

CASBINLINE

The default fields to be exported for **Insights Collection** - **CASBInline** are given below.

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
1	eventtime	eventTime	Event Time

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
2	username	upn	Username
3	devicename	dos	Device Name
4	action	atgs	Action
5	details	msg	Details
6	filename	fnm	File Name
7	applicationname	apn	Application Name
8	publicip	dip	Public IP
9	city	cty	City
10	region	reg	Region
11	countrycode	crc	Country Code
12	transactionid	apd	Transaction ID
13	allactivities	tgs	All Activities
14	userfullname	udn	User Full Name
15	deviceid	did	Device ID
16	fileextension	ext	File Extension
17	emailfrom	fre	Email From
18	emailto	toe	Email To
19	emailsubject	esj	Email Subject
20	emailbcc	bce	Email BCC
21	emailcc	cce	Email CC
22	pagetitle	ptl	Page Title
23	requesturi	uri	Request URI
24	useragent	uag	User Agent
25	regioncode	rgc	Region Code
26	sforganizationid	org	SF Organization ID
27	instancename	inm	Instance Name
28	cloudapplicationid	aid	Cloud Application ID
29	group	gdn	Group
30	policyid	dpi	Policy ID

All fields for **SSE Log Type** - **NA** are given below.

	New Export API		
SNo	Splunk/Script Exported Name	Column Name	QRadar Exported Name
1	notificationid	ntfyid	Notification ID
2	filesize	fsz	File Size
3	activity	acd	Activity
4	country	cry	Country
5	customregion	creg	Custom Region
6	userfirstname	ufn	User First Name
7	userlastname	uln	User Last Name
8	documenttype	ftp	Document Type
9	emailmessageid	fid	Email Message ID
10	emailsenttime	est	Email Sent Time
11	actiondetails	act	Action Details
12	accessmethod	acm	Access Method
13	httprequest method	rmd	HTTP Request Method
14	operatingsystem	hos	Operating System
15	latitude	lat	Latitude
16	longitude	lon	Longitude
17	locationaccuracy	acc	Location Accuracy
18	threatindicator	csl	Threat Indicator
19	userid	lui	User ID
20	groupids	gid	Group IDs
21	userdisplaygroup	udg	User Display Group
22	awsnodename internal	nod	
23	justification	jst	Justification

Contents

- Cloud Web Security on page 23

Cloud Web Security

All available fields from the collections for Cloud Web Security are given below. Currently, only the **Web** schema is available for SIEM export.

Web

Point Product Code: WS | Collection: Web

SNo	Exported Name	Column Name
1	action	action
2	category	category
3	blockdirection	blockDirection
4	endpointtype	endpointType
5	endpointversion	endpointVersion
6	group	group
7	localizedcountry	vpopRegion
8	parentcategory	parentCategory
9	policyname	policyName
10	riskclass	riskClass
11	searchterm	searchTerm
12	user	user
13	workstation	workstation
14	domain	domain
15	domainsecondlevel	sld
16	domaintoplevel	tld
17	host	host
18	path	path
19	protocol	protocol

SNo	Exported Name	Column Name
20	query	query
21	cloudappname	casbAppName
22	cloudappcategory	casbAppCategory
23	cloudappforwarded	casbForwarded
24	cloudapprisklevel	casbAppRiskLevel
25	connectionip	sourceIp
26	connectionipcity	sourceIpCity
27	connectionipcountry	sourceIpCountry
28	connectionname	connectionName
29	dedicatedip	dedicatedIp
30	destinationip	destIp
31	destinationipcountry	destIpCountry
32	egressip	egressIp
33	sourceip	internalIp
34	analyticname	analyticName
35	severity	severity
36	threatname	threatDetail
37	threattype	threatType
38	filename	fileName
39	filetype	fileType
40	mimesubtype	rspMinorType
41	mimetype	rspMajorType
42	refererdomain	refererDomain
43	refererhost	refererHost
44	refererpath	refererPath
45	refererport	refererPort
46	refererquery	refererQuery
47	operatingsystem	uaOsName
48	operatingsystemtype	uaOsFamily
49	useragent	userAgent
50	useragenttype	uaType
51	authenticationmethod	authentication
52	classificationtype	categoryType

SNo	Exported Name	Column Name
53	datacentre	cluster
54	deviceregistrationid	deviceRegistrationId
55	filteringsource	clientType
56	httpstatuscode	httpStatus
57	port	port
58	requestmethod	method
59	tlsversiondownstream	downstreamTlsVersion
60	bytesreceived	bytesReceived
61	bytessent	bytesSent
62	serverresponsetime	originGetTime
63	totaltime	totalTime
64	bandwidth	bandwidth
65	fullmimetype	rspFullMimeType
66	filteringtime	proxyTime
67	blockedbydestipcountry	blockedByDestIPCountry

Contents

- Cloud DLP on page 26

Cloud DLP

The default fields to be exported for **Cloud DLP** are given below.

DLPIncidentsAll

Point Product Code: DS

SNo	Attribute Name	Exported Name
1	eventTime	time
2	alertId	alertid
3	channel	channel
4	createdTimestamp	createdtimestamp
5	user	user
6	violatedPolicies	violatedpolicies
7	destination	destination
8	action	action
9	analysedBy	analysedby
10	dataChannels	datachannels
11	violatedTriggers	violatedtriggers
12	userRiskLevel	userrisklevel
13	detectedBy	detectedby
14	justificationChoice	justificationchoice
15	justificationText	justificationtext
16	reportingProducts	reportingproducts
17	fileNames	filenames
18	alertEventId	alerteventid
19	rules	rules
20	inspectionId	inspectionid

SNo	Attribute Name	Exported Name
21	department	department
22	transactionSize	transactionsize
23	riskImpact	riskimpact
24	maximumMatches	maximummatches
25	updateTime	updatetime
26	stateTransition	statetransition
27	severity	severity
28	reason	reason
29	state	state
30	assignee	assignee
31	tags	tags
32	incidentStatus	incidentstatus
33	ignoredIncident	ignoredincident
34	releasedIncident	releasedincident
35	timeToResolve	timetoresolve

DLPIncidents

Point Product Code: DS

SNo	Attribute Name	Exported Name
1	eventTime	time
2	alertId	alertid
3	channel	channel
4	createdTimestamp	createdtimestamp
5	user	user
6	violatedPolicies	violatedpolicies
7	destination	destination
8	action	action
9	analysedBy	analysedby
10	dataChannels	datachannels
11	violatedTriggers	violatedtriggers
12	userRiskLevel	userrisklevel
13	detectedBy	detectedby

SNo	Attribute Name	Exported Name
14	justificationChoice	justificationchoice
15	justificationText	justificationtext
16	reportingProducts	reportingproducts
17	fileNames	filenames
18	alertEventId	alerteventid
19	rules	rules
20	inspectionId	inspectionid
21	department	department
22	transactionSize	transactionsize
23	riskImpact	riskimpact
24	maximumMatches	maximummatches
25	updateTime	updatetime
26	stateTransition	statetransition
27	severity	severity
28	reason	reason
29	state	state
30	assignee	assignee
31	tags	tags
32	incidentStatus	incidentstatus
33	ignoredIncident	ignoredincident
34	releasedIncident	releasedincident
35	timeToResolve	timetoresolve

© 2026 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 28 July 2026