EPP 8.5 SIEM Payload key/identifiers

Type: External

Objective: The key/identifiers of SIEM reports will provide user information about the values displayed on the generated report.

Description: An event list is generated when an administrator views the event logs on the configured SIEM server. These data formats are supported by LEEF (Log Event Extended Format) and CEF (Common Event Format) only.

SIEM Payload key/identifiers

The table below lists the key/identifier values been displayed in the event log.

Sr.No.	Module	Key	Value
1	Virus Protection	VP1	Access denied
2		VP0	None
3		VP2	Failed to deny access
4		VP3	Repaired
5		VP6	Delete failed
6		VP5	Deleted
7		VP4	Repair failed
8		VP7	Quarantined
9		VP8	Quarantine failed
10		VP9	File is repaired
11		VP10	File is skipped
12		VP11	Skipped
13		VP12	File is deleted
14		VP13	File is marked for deletion
15		VP14	File is marked for cleanup
16		VP15	File is clean
17		VP17	Scanner
18		VP16	File is quarantined
19		VP18	Virus Protection
20		VP19	Email Protection
21		VP20	Startup Scan
22		VP21	Office Protection
23		VP22	Scheduler
24		VP23	Quick Update
25		VP24	Memory Scan
26		VP25	Anti Ransomware
27		VP26	Allow
28	AntiMalware	AM2	Clean
29		AM1	Skip
30		AM3	Mark For Deletion
31		AM5	Password Recovery Tool
32		AM9	Rogue Security Software

33		AM7	Adware Bundler
34		AM14	Toolbar
35		AM6	Keylogger
36		AM8	English
37		AM15	Potentially Unwanted Program
38		AM18	Adware
39		AM17	P2P Program
40		AM16	Remote Control
41		AM19	Potentially Dangerous Tool
42		AM20	Trojan
43		AM13	Commercial Remote Control Tool
44		AM10	Remote Control Tool
45		AM11	Potentially Unwanted App
46		AM4	Rogue Security Program
47		AM12	PUPS
48	Web Security/ GAC/YAC	WS1	Blocked
49		WS2	Attacker's IP blocked
50		WS3	System Disconnected from Network
51		WS6	Password
52		WS501	YouTube
53		WS7	Account Creation
54		WS5	Login
55		WS4	Allowed
56	Device Control	DC1	Blocked
57		DC2	Write Access Denied
58		DC3	USB Storage Device
59		DC4	Scanner & Imaging Devices
60		DC5	Smart Phone
61		DC6	Windows Portable Device
62		DC8	Internal Card Reader
63		DC7	Windows Portable Device
64		DC10	FireWire Bus
65		DC9	PCMCIA Device
66		DC11	ZIP Drive
67		DC13	Internal Floppy Drive
68		DC14	Card Reader Device (MTD)
69		DC12	CD/DVD
70		DC15	Card Reader Device (SCSI)
71		DC17	Mobile Phones (Sony Ericsson, etc)
72		DC19	Bluetooth
73		DC24	iPhone
74		DC18	Local Printers
75		DC21	BlackBerry
76		DC22	Webcam
77		DC26	iPod
78		DC23	Serial Port
79		DC25	iPad
80		DC27	SATA controller

81		DC31	Network Share
82		DC28	Teensy Board
83		DC32	USB Interface
84		DC30	Thunderbolt
85		DC16	Windows Portable Device
86		DC20	WiFi
87		DC29	Unknown Device
88		Manufacturer Name	manufacture name will shows as Vendor name and Product name in SIEM reports
89	IntrusionPrevention	WC5	Advertisements and Pop-Ups
90		WC6	Alcohol and Tobacco
91		WC7	Anonymizers
92		WC11	Chat
93		WC7	Anonymizers
94		WC11	Chat
95		WC10	Computers and Technology
96		WC9	Business
97		WC8	Arts
98		WC13	Criminal Activity
99		WC14	Dating and Personals
100		WC12	Child Abuse Images
101		WC15	Download Sites
102		WC17	Entertainment
103		WC18	Fashion and Beauty
104		WC19	Finance
105		WC16	Education
106		WC20	Forums and Newsgroups
107		WC21	Gambling
108		WC22	Games
109		WC23	General
110		WC24	Government
111		WC25	Greeting cards
112		WC28	Health and Medicine
113		WC27	Hate and Intolerance
114		WC26	Hacking
115		WC29	Illegal Drug
116		WC31	Image Sharing
117		WC30	Illegal Software
118		WC34	Job Search
119		WC33	Instant Messaging
120		WC36	Network Errors
121		WC32	Information Security
122		WC37	News
123		WC35	Leisure and Recreation
124		WC38	Non-profits and NGOs
125		WC40	Offensive
126		WC41	Parked domains
127		WC42	Peer-to-Peer
128		WC39	Nudity

129		WC43	Personal Sites
130		WC44	Politics
131		WC46	Profanity
132		WC45	Pornography/Sexually Explicit
133		WC47	Real Estate
134		WC48	Religion
135		WC49	Restaurants and Dining
136		WC51	Search Engines and Portals
137		WC50	School Cheating
138		WC52	Sex Education
139		WC54	Social Networking
140		WC53	Shopping
141		WC55	Spam Sites
142		WC56	Sports
143		WC58	Translators
144		WC60	Travel
145		WC57	Streaming Media and Downloads
146		WC63	Web-based Email
147		WC62	Weapons
148		WC61	Violence
149		WC59	Transportation
150		WC5-tltp	Sites related to advertising graphics or banners and pop-ups.
151		WC6-tltp	Sites related to sell alcohol- or tobacco-related products or services.
152		WC11-tltp	Sites related to web-based exchange of realtime messages.
153		WC7-tltp	Site helping to surf anonymously, sometimes to circumvent web filtering.
154		WC13-tltp	Sites promoting criminal activities and violence.
155		WC12-tltp	Sites that portray or discuss children in sexual or other abusive acts.
156		WC14-tltp	Sites related to interpersonal relationships such as dating and marriage.
157		WC15-tltp	Sites sharing downloadable software, freeware, shareware, etc.
158		WC17-tltp	Sites related to television, movies, music and video.
159		WC8-tltp	Sites related to artistic content or relating to artistic institutions.
160		WC19-tltp	Sites related to banking, finance, payment or investment.
161		WC18-tltp	Sites concerning fashion, jewellery, glamour, beauty, cosmetics, etc.
162		WC21-tltp	Sites related to online gambling, lottery, casinos, betting agencies, etc.
163		WC20-tltp	Sites for sharing information in the form of newsgroups, forums, etc.
164		WC16-tltp	Sites containing educational information, encyclopaedias, etc.

165		WC22-tltp	Sites containing online and downloadable games.
166		WC23-tltp	Sites that do not clearly fall into other
167			categories.
168		WC10-tltp	Sites related to computer software, hardware, services, news, etc.
169		WC9-tltp	Sites containing financial and business related information.
170		WC25-tltp	Sites that allow people to send and receive greeting cards and postcards.
171		WC24-tltp	Sites run by governmental organizations, departments, or agencies.
172		WC27-tltp	Sites related to Hate and Intolerance.
173		WC26-tltp	Sites that advise about hacking for illegal cyber activities.
174		WC31-tltp	Sites that host digital photographs and images.
175		WC32-tltp	Sites that provide legitimate information about data protection.
176		WC29-tltp	Sites promoting illegal drugs, alcohol, tobacco, etc
177		WC30-tltp	Sites that illegally distribute software or copyrighted materials.
178		WC35-tltp	Sites relating to recreational activities and hobbies.
179		WC34-tltp	Sites containing job listings, career information etc.
180		WC36-tltp	Sites that do not resolve to any IP address.
181		WC28-tltp	Sites containing information related to health, healthcare services, etc.
182		WC33-tltp	Sites related to instant messaging.
183		WC37-tltp	Sites covering news and current events.
184		WC38-tltp	Sites devoted to clubs, communities, unions, and non-profit organizations.
185		WC41-tltp	Sites that are inactive, typically reserved for later use.
186		WC42-tltp	Sites which supports peer-to-peer communication.
187		WC40-tltp	Sites containing offensive content.
188		WC44-tltp	Sites that promote political parties or political advocacy.
189		WC45-tltp	Sites that contain explicit sexual content.
190		WC39-tltp	Sites that contain full or partial nudity that are not necessarily overtly sexual in intent.
191		WC43-tltp	Sites about or hosted by personal individuals, including those hosted on commercial sites.
192		WC46-tltp	Sites with tasteless content such as bathroom humor or profanity.
193		WC47-tltp	Sites related to commercial and residential real estate services.
194		WC49-tltp	Sites that list, review, advertise food, dining or catering services.

195		WC48-tltp	Sites related to faith, spirituality, religious beliefs, worship places.
196		WC50-tltp	Sites promoting unethical practices such as cheating or plagiarism.
197		WC52-tltp	Sites relating to sex education.
198		WC54-tltp	Sites that enable social networking.
199		WC53-tltp	Sites for online shopping, catalogs, auctions, classified ads.
200		WC55-tltp	Sites that have been promoted through spam techniques.
201		WC51-tltp	Sites enabling the searching of the Web, newsgroups, images, etc.
202		WC56-tltp	Sites relating to sports teams, fan clubs, scores and sports news.
203		WC57-tltp	Sites allowed Streaming Media and Downloads.
204		WC58-tltp	Sites that translate Web pages or phrases from one language to another.
205		WC59-tltp	Sites that provide information about motor vehicles such as cars, motorcycles and the like.
206		WC60-tltp	Sites related to travel and tourism and online booking of travel services.
207		WC61-tltp	Sites that contain images or text against humans, animals etc.
208		WC63-tltp	Sites that enable users to send and receive email through a web-accessible email account.
209		WC62-tltp	Sites that depict, sell, review or describe guns and weapons, including for sport.
210		WC1	Unknown
211		WC3	Phishing
212		WC0	Custom
213		WC4	Private IP Addresses
214		WC2	Malicious/Infected
215		WC64	Cyber Security Awareness and Training Simulation Sites
216	Firewall	FW6	Inbound-Outnound
217		FW2	TCP
218		FW8	High
219		FW7	Block All
220		FW9	Medium
221		FW10	Low
222		FW11	Client connected to unsecured Wi-Fi network
223		FW12	Unsecured Wi-Fi network of the client is accessed
224		FW3	ICMP
225		FW1	UDP
226		FW4	Inbound
227		FW5	Outbound
228	DLP	dlp4	Applications
229		dlp3	Removable Devices

230		dlp6	Clipboard
231		dlp5	Network share
232		dlp11	User Defined Dictionary
233		dlp7	Print Screen
234		dlp8	Printer Activity
235		dlp10	Confidential Data
236		DLP1	Blocked
237		DLP2	Skipped
238		DLP3	Removable Devices
239		DLP4	Applications/Online Services
240		DLP5	Network Share
241		DLP7	Print Screen
242		DLP8	Printer
243		DLP6	Clipboard
244		DLP10	Confidential Data
245		DLP16	Discover
246		DLP17	JCB
247		DLP18	MasterCard
248		DLP19	Visa
249		DLP20	Driving License
250		DLP21	E-mail ID
251		DLP22	IBAN
252		DLP23	Phone Number
253		DLP24	SSN
254		DLP25	Health Insurance
255		DLP26	Passport
256		DLP27	ID
257		DLP28	Pan Card
258		DLP29	Business Registration Number
259		DLP30	Corporation Registration Number
260		DLP31	Bank Account Number
261		DLP32	Individual My Number
262		DLP33	Corporate My Number
263		DLP34	On Demand Scan
264		DLP15	Diners
265		DLP35	Schedule Scan
266		DLP36	Credit/Debit Card
267		DLP37	Personal
268		DLP38	PIN Code
269		DLP39	Vehicle Registration Number
270		DLP40	Aadhar Number
271		DLP9	File
272		DLP11	User Defined Dictionary
273		DLP13	Printer
274		DLP14	Amex
275		DLP12	Print Screen
276		dlp-file-type-cat-2	Office Files
277		dlp-file-type-cat-3	Programming Files
278		dlp-file-type-cat-1	Graphic Files

279		dlp-file-type-cat-4	Other Files
280		dlp-file-type-cat-5	Custom Extensions
281		DLP41	Drug Enforcement Agency (DEA) Number
282		DLP42	Australia Tax File Number
283		DLP43	Australian Business Number
284		DLP44	Australia Medical Account Number
285	Application control on access	appctrl-cat-0	Unknown
286		appctrl-cat-1	Other
287		appctrl-cat-3	Backup Software
288		appctrl-cat-2	Archive Tools
289		appctrl-cat-6	Educational Software
290		appctrl-cat-12	Media Players
291		appctrl-cat-13	Miscellaneous
292		appctrl-cat-14	Office Software
293		appctrl-cat-15	Security Software
294		appctrl-cat-16	Synchronization Software
295		appctrl-cat-17	Tuning Software
296		appctrl-cat-18	USB Modems
297		appctrl-cat-19	Video Chat Applications
298		appctrl-cat-20	Web Browsers
299		appctrl-cat-21	Developer Tools
300		appctrl-cat-22	Encryption Steganography Tools
301		appctrl-cat-23	Authorizing Tools
302		appctrl-cat-24	Barcode Software
303		appctrl-cat-11	Instant Messaging Clients
304		appctrl-cat-25	Designing Software
305		appctrl-cat-26	Proxy
306		appctrl-cat-27	Toolbars
307		appctrl-cat-28	Network Tools
308		appctrl-cat-7	Email Clients
309		appctrl-cat-8	File Sharing Applications
310		appctrl-cat-9	Games
311		appctrl-cat-10	Image Editing Tools
312		appctrl-cat-4	CD/DVD Applications
313		appctrl-cat-5	Download Managers
314	Application control on demand	appctrl-cat-100	Unknown
315		unauthorized-app	Unauthorized applications
316		unauthorized	Unauthorized
317		lbl-authorized	Authorized
318		lbl-authorized-app	Authorized applications
319		lbl-authorized-wi-fi-connections	Authorized Wi-Fi Connections
320		lbl-authorized-wi-fi-connections-rdobtn1	Allow for all Wi-Fi access points
321		lbl-authorized-wi-fi-connections-rdobtn2	Allow only for authorized Wi-Fi access points

322	Ransomeware	lbl-arwbkp	Backup for Ransomware Protection
323		lbl-ARWB1	Backup process success
324		lbl-ARWB2	Backup process fail
325		lbl-ARWB3	Invalid arguments passed
326		lbl-ARWB4	Size exceeds the mentioned limit
327		lbl-ARWB5	Insert operation failed
328		lbl-ARWB6	Backup location is valid
329		lbl-ARWB7	Unknown error
330		lbl-ARWB8	Backup database is corrupted
331		lbl-ARWB9	Database file not found
332		lbl-ARWB10	Backup process is interrupted
333		lbl-ARWB11	Backup path is invalid / access denied
334		lbl-ARWB12	Network path is invalid
335		lbl-ARWB13	Network login failed
336		lbl-ARWB14	Backup copy at network location failed
337		lbl-ARWB15	Network interrupted while copying backup
338	Vulnerability Scan	lbl-VS1	Low
339		lbl-VS2	Medium
340		lbl-VS3	High
341	ETH	lbl-endpoint-dt	Endpoint Scan Date & Time
342		lbl-search-name	Search Name*
343		lbl-hash-type	Hash Type
344		lbl-hash-code	Hash Code
345		lbl-action	Action
346		Scantype1	On Demand
347		Scantype2	Schedule
348		Query Type 1	MD5
349		Query Type 2	SHA1
350		Query Type 3	MD5_SHA1
351		Query Type 4	SHA256
352		Query Type 5	MD5_SHA256
353		Query Type 6	SHA1_SHA256
354		Query Type 7	MD5_SHA1_SHA256
355	Patch Scan	lbl-patch-category-1	Critical Updates
356		lbl-patch-category-2	Definition Updates
357		lbl-patch-category-3	Drivers
358		lbl-patch-category-4	Feature Packs
359		lbl-patch-category-5	Security Updates
360		lbl-patch-category-6	Service Pack
361		lbl-patch-category-7	Tools
362		lbl-patch-category-8	Update Rollups
363		lbl-patch-category-9	Updates

364		lbl-patch-category-10	Upgrades
365		lbl-patch-category-11	Application
366	File Activity Monitoring	lbl-FAMD1	Local Drive
367		lbl-FAMD2	Removable Drive
368		lbl-FAME1	Modified/Copied
369		lbl-FAME2	Deleted
370		lbl-FAME4	Extension Changed
371	Encryption		
372		Encryption/Volume / Endpoint Status : 1	Encrypted
373		Encryption/Volume / Endpoint Status : 2	Not Encrypted
374		Encryption/Volume / Endpoint Status : 3	Partial Encrypted
375		Encryption/Volume / Endpoint Status : 4	Not Supported
376		Report Type:1	Activity
377		Report Type:2	Status
378		Report Type:3	Recovery
379		Activity Type:1	Info
380		Activity Type:2	Error
381		Volume Type: 0	Operating System
382		Volume Type: 1	Data
383		Volume Type: 2	Removable
384		Volume Encryption Method:0	None
385		Volume Encryption Method:1	AES_128_WITH_DIFFUSER
386		Volume Encryption Method:2	AES_256_WITH_DIFFUSER
387		Volume Encryption Method:3	AES_128
388		Volume Encryption Method:4	AES_256
389		Volume Encryption Method:5	HARDWARE_ENCRYPTION
390		Volume Encryption Method:6	XTS_AES_128
391		Volume Encryption Method:7	XTS_AES_256