FortiWeb Log Reference

VERSION 7.2.2

TABLE OF CONTENTS

Introduction

This document is a detailed reference of all of your FortiWeb appliance's possible log messages. It is organized primarily by the log type:

- Event
- Attack
- Traffic

To look up the meaning of a specific log message, go to the section that matches its **Type** (`type`) field, then look for the table that matches its **ID** (`log_id`).

This document also explains the general structure of FortiWeb log messages, and the meanings of common fields (see How to interpret FortiWeb logs on page 14).

Scope

This document provides administrators information about log messages that can be recorded by a FortiWeb appliance.

This document does **not** cover how to configure logging. It assumes you have already configured it, and need to know how to interpret the log messages. For instructions on how to configure logging, see the *FortiWeb Administration Guide* or *FortiWeb CLI Reference*.

How to interpret FortiWeb logs

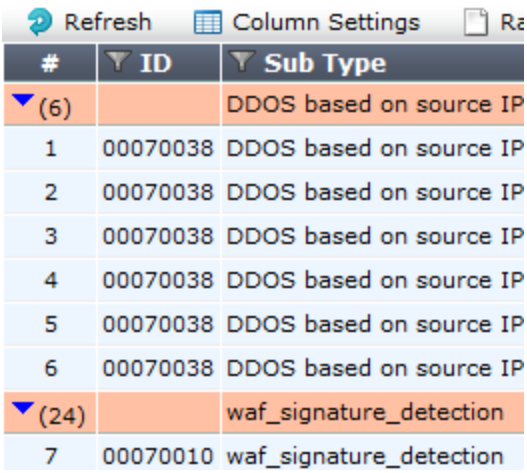
This section explains the composition of FortiWeb log messages.

In some cases, to avoid flooding attack logs with entries, FortiWeb collects multiple attack log messages into a single message. See Attack on page 450.

Header & body fields

Each log message is comprised of several field-value pairs. The names may vary slightly between **Raw** versus **Formatted** views in the web UI.

ID (`log_id`) header field and its value



All log messages' fields belong to one of two parts:

- **Header** — Contains the time and date the log originated, a log identifier, a message identifier, the administrative domain (ADOM), the type of log, the severity level (priority) and where the log message originated. **These fields exist in all logs.**
- **Body** — Describes the reason why the log was created, plus any actions that the FortiWeb appliance took to respond to it. **These fields vary by log type.**

Log message header and body

For example, this is a raw-format event log message. Body fields are in **bold**.

date=2013-10-07 time=11:30:53 log_id=10000017 msg_id=000000001117 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information **trigger_policy="" user=admin ui=GUI action=login status=success msg="User admin login successfully from GUI (172.20.120.47)"**

This attack log message contains the same header fields, but its body fields are different.

date=2016-02-19 time=11:23:45 log_id=20000010 msg_id=000139289631 device_id=FV-1KD3A15800072 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=attack subtype="waf_signature_detection" pri=alert **trigger_policy="" severity_level=Medium proto=tcp service=HTTP action=Alert policy="123" src=172.22.6.234 src_port=60554 dst=10.0.9.13 dst_port=80 HTTP_method=get HTTP_ url="/preview.php?file==../" HTTP_host="10.0.9.123" HTTP_agent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:43.0) Gecko/20100101 Firefox/43.0" HTTP_session_id=3B9864AEKNQSLLODNTILCG37M2FZ6A88 msg=" [Signatures name: 123] [main class name: Generic Attacks(Extended)] [sub class name: Directory Traversal]: 060150002" signature_subclass="Directory Traversal" signature_id="060150002" srccountry="Reserved" content_switch_name="none" server_pool_name="123" false_positive_mitigation="none" log_type=LOG_ TYPE_SCORE_SUM event_score=3 score_message="[score_type: total_score] [score_scope: TCP Session] [score_threshold: 5] [score_sum: 7]" entry_sequence="000139289630"**

Similarly, traffic log body fields are different.

date=2014-06-26 time=00:43:37 log_id=30000000 msg_id=000001351251 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=traffic subtype="HTTP" pri=notice **proto=tcp service=HTTP status=success reason=none policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80 HTTP_request_time=0 HTTP_response_time=0 HTTP_request_bytes=444 HTTP_response_bytes=401 HTTP_ method=get HTTP_url="/" HTTP_host="10.0.8.22" HTTP_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " HTTP_retcode=200 msg="HTTP GET request from 10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_ name="testa" server_pool_name="Auto-ServerFarm"**

The following table describes each possible header or body field, according to its name as it appears in the **Formatted** or **Raw** view.

Log message fields

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
Header					
Date (`date`)	The year, month, and day when the log message was	+	+	+	`date=2013-10-08`

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
	recorded.				
Time (time)	The hour (according to a 24-hour clock, where 15:00 is 3:00 PM), minute, and second that the log message was recorded.	+	+	+	time=15:38:01
ID (log_id)	See Log ID numbers on page 24.	+	+	+	log_id=00041101
MSG ID (msg_id)	See Message IDs on page 26.	+	+	+	msg_id=000000000153
Device ID (device_id)	The identifier, typically the serial number, of the appliance which originally recorded the log.	+	+	+	device_id=FV-1KD2B34567890
ADOM (vd)	The administrative domain (ADOM) in which the log message was recorded	+	+	+	vd=”root”
Time Zone (timezone)	The name, geographical region, and Greenwich Mean Time (GMT) adjustment of the time zone in which the appliance is located.	+	+	+	timezone="(GMT-5:00)Eastern Time(US & Canada)"
Type (type)	See Types on page 24.	+	+	+	type=event
Sub Type (subtype)	See Subtypes on page 25.	+	+	+	subtype=admin
Level (pri)	See Priority level on page 25.	+	+	+	pri=alert
Body					
Protocol (proto)	tcp	–	+	+	proto=tcp

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
	The protocol used by web traffic. By definition, for FortiWeb, this is always TCP.				
Service (`service`)	`HTTP` or `HTTPS` The name of the application-layer protocol used by the traffic. By definition, for FortiWeb, this is always HTTP or HTTPS.	–	+	+	`service=HTTP`
Source (`src`)	The IP address of the traffic's origin. The source varies by the direction: • In HTTP requests, this is the web browser or other client. • In HTTP responses, this is the physical server.	–	+	+	`scr=10.0.0.0`
Source Port (`src_port`)	The port number of the traffic's origin.	–	+	+	`src_port=3471`
Destination (`dst`)	The IP address of the traffic's destination. The source varies by the direction: • In HTTP requests, this is the physical server. • In HTTP responses, this is the web browser or other client.	–	+	+	`dst=10.0.0.1`
Destination Port (`dst_port`)	The port number of the traffic's destination.	–	+	+	`dst_port=8080`

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
Policy (`policy`)	The name of the server policy governing the traffic which caused the log message.	–	+	+	`policy="policy1"`
User (`user`)	The daemon or name of the administrator account that performed the action that caused the log message.	+	–	–	`user=admin`
User Interface (`ui`)	The type of management interface used by the administrative session which caused the log message. Either: • `GUI` • `sshd` • `telnet` • `console` • `none` Unless the user is a daemon (which don't have a user interface), logins from `none` indicate that an administrator used the JavaScript **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login. Logins from `console` indicate use of CLI via the local serial console port.	+	–	–	`ui=GUI`
Action (`action`)	The action associated with the log message or policy violation, such as: `login` or	+	+	–	`action=Alert`

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
	Alert				
Status (status)	The result of the action.	+	–	+	status=failure
Reason (reason)	The reason for the status, if any.	+	–	+	reason=name_invalid
Return Code (HTTP_retcode)	The HTTP return code. If FortiWeb is configured to redirect, this is the rewritten code, **not** the original one from the server.	–	–	+	HTTP_retcode=200
Request Time (HTTP_request_time)	The amount of time it took FortiWeb to process the client request, in milliseconds (ms).	–	–	+	HTTP_request_time=10
Response Time (HTTP_response_time)	The amount of processing time for the response in milliseconds (ms). This can be a useful measure of performance issues, especially if processing involves regular expressing matching.	–	–	+	HTTP_response_time=10
Request Bytes (HTTP_request_bytes)	The size of the request in bytes.	–	–	+	HTTP_request_bytes=2
Response Bytes (HTTP_response_bytes)	The size of the individual response in bytes (B). For chunked responses, this is for each reply; it does **not** aggregate all related chunks.	–	–	+	HTTP_response_bytes=136
Method (HTTP_method)	The method, such as GET or POST, used by the HTTP request.	–	+	+	HTTP_method=get

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
URL (`HTTP_url`)	The URL in the HTTP header of the original HTTP request, such as: `/images/buttons/hintOver.png` This does not include the service (HTTP://) nor host name (example.nl). If FortiWeb is configured to rewrite the URL, this is the original URL from the client, **not** the rewritten one.	–	+	+	`HTTP_url="/image/up.png"`
Host (`HTTP_host`)	The `Host:` field in the HTTP header of the HTTP request, such as: `www.example.com` or `10.0.0.1:8080` This is typically a fully qualified domain name (FQDN) or IP address and port number that resolves or routes to the virtual server on the FortiWeb appliance. This may be different from your internal DNS name (if any) for the web server, or, if you are using HTTP `Host:` rewrites, different from the virtual host on the web server. For example, this might be `www.example.co.jp` instead of `www1.local` or the virtual host that serves responses for all DNS names, `www.example.com`.	–	+	+	`HTTP_host="example.com"`

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
User Agent (HTTP_agent)	The name and version of the HTTP client, usually a web browser. This is reported by the client itself in the User-Agent: HTTP header. In attacks, it is often fake.	–	+	+	HTTP_agent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36"
FortiWeb Session ID (HTTP_session_id)	The session identifier for a client's related HTTP requests (if any). The ID may be unknown if the **Session Management** option is not enabled in the applied protection profile, and therefore FortiWeb has not injected a session cookie nor inferred a session ID from the protected web application.	–	+	–	HTTP_session_id=K8BXT3TNYUM710UEGWC8IQBTPX9PRWHB
Severity Level (severity_level)	The severity that the administrator configured in the rule or policy governing the traffic which caused the log message.	–	+	–	severity_level=High
Trigger Policy (trigger_policy)	The name of the notification servers used to record and/or deliver this log message (if any). The trigger policy value may be an empty string if no trigger policy was selected.	+	+	–	trigger_policy=notification-server-group1
Signature Subclass (signature_subclass)	The name of the signature subclass. If the current signature has no subclass, the main class is displayed.	–	+	–	"Cross Site Scripting"

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
Signature ID (`signature_id`)	The ID of the specific signature within the subclass that triggered the log message.	–	+	–	`"010000001"`
Source Country (`srccountry`)	The country that is the source of the traffic.	–	+	+	`"United States"`
Message (`msg`)	Details describing the reason why the log message was created. The message varies by the nature of the cause. The `msg` log field has the lowest priority in the disk log. When the total size of all the log fields exceeds the disk log size limit, FortiWeb truncates the msg field, which helps preserve other log information.	+	+	+	`msg="User admin changed dns from GUI (172.20.120.47)"`
HTTP Content Routing (`content_switch_name`)	The name of the associated HTTP content routing policy.	–	+	+	`content_switch_name= "HTTProutes1"`
Server Pool (`server_pool_name`)	The name of the server pool in the associated server policy.	–	+	+	`server_pool_name= "Auto-ServerFarm"`

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
False Positive Mitigation `false_positive_mitigation`	For violations of SQL injection signatures, specifies whether FortiWeb identified the attack using the signature and additional SQL syntax validation (`yes`) or the just the signature (`no`).	–	+	–	`false_positive_mitigation="yes"`

Threat Scoring
`log_type`
`event_score`
`score_message`
`entry_sequence`
	Information about the threat score, which FortiWeb generates based on multiple signature violations by a client, instead of a single signature violation.
	For details, see Attack log fields.
		–	+	–	`log_type=LOG_TYPE_SCORE_SUM event_score=3 score_message="[score_type: total_score] [score_scope: TCP Session] [score_threshold: 5] [score_sum: 7]" entry_sequence="000139289630"`

Detailed Information (N/A)	This column contains the entire log message in raw format. If your **Column Settings** show this column, the entire raw log message will be included in the row under this column, next to the formatted column view of the same log message. This way, if you want to view the entire raw log message, you can simply scroll the page, instead of switching the entire page back and forth from **Raw** to **Formatted** log views.	+	+	+	`date=2013-10-10 time=00:38:58 log_id=20000051 msg_id=000000000008...`

Field name (Raw view name in parentheses)	Description	Exists in log type			Example field-value pair (Raw view)
		Event	Attack	Traffic	
	This column appears only when using the **Formatted** log view. It does not actually exist as a field in the raw logs.				

Log ID numbers

The **ID** (`log_id`) is an 8-digit field located in the header, immediately following the time and date fields.

The `log_id` field is a number assigned to all permutations of the same message. It classifies a log message by the nature of the cause of the log message, such as administrator authentication failures or traffic. Other log messages that share the same cause will share the same `log_id`.

For example, creating an administrator account always has the log ID 00003401.

Types

Each log message contains a **Type** (`type`) field that indicates its category, and in which log file it is stored.

FortiWeb appliances can record the following categories of log messages:

Log types

Log type	Description
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.
Traffic	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.
Attack	Records attack and intrusion attempts.

Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. **Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.**

Subtypes

Each log message contains a **Sub Type** (`subtype`) field that further subdivides its category according to the feature involved with the cause of the log message.

For example:

- In event logs, some may have a `subtype` of `admin`, `system`, or other subtypes.
- In attack logs, they have main type and subtypes to reflect the classification of the attacks.
- In traffic logs, the `subtype` is always HTTP even if the service is HTTPS.

Priority level

Each log message contains a **Level** (`pri`) field that indicates the estimated severity of the event that caused the log message, such as `pri=warning`, and therefore how high a priority it is likely to be.

Level (`pri`) associations with the descriptions below are not always uniform. They also may not correspond with **your own** definitions of how severe each event is. If you require notification when a specific event occurs, either configure SNMP traps or alert email by administrator-defined Severity Level (`severity_level`) or ID (`log_id`), **not** by Level (`pri`).

Approximate log priority levels

Level (0 is highest)	Name	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required. **Used in attack logs.**
2	Critical	Functionality is affected.
3	Error	An error condition exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events. **Used in traffic logs, and in event logs for administrator logins, time changes, and normal daemon actions.**
6	Information	General information about system operations. **Used in event logs for configuration changes.**

For each location where the FortiWeb appliance can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. The FortiWeb appliance will store all log messages equal to or exceeding the log severity level you select.

For example, if you select **Error**, the FortiWeb appliance will store log messages whose log severity level is **Error**, **Critical**, **Alert**, and **Emergency**.

Avoid recording log messages using low log severity thresholds such as information or notification to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

Message IDs

The **MSG ID** (`msg_id`) field is an 12-digit number located in the header, incremented with each individual log message generated by the FortiWeb appliance. It is used only for numbering each entry in the database, and does not necessarily reflect its cause.

Each `msg_id` number is a unique identifier for that specific log entry. No other log messages, regardless of cause, share the same `msg_id`.

Event

Event log messages record subsystem events such as NTP-based time changes, reboots and RAID level changes. They also record configuration changes.

Unless noted as otherwise in each event log's description:

- **Level** (`pri`) field is `information`
- **User** (`user`) field is the name of the administrator account that caused the event
- **User Interface** (`ui`) field is according to User Interface on page 18

To go to a sample, additional information, and solution (if applicable) for an event log message, click the **ID** (`log_id`) field in the table.

Event logs by subtype & ID

ID (`log_id`)	Sub Type (`subtype`)
00001002	admin
00001012	admin
00001052	admin
00001062	admin
00002202	admin
00002801	admin
00002802	admin
00002811	admin
00003401	admin
00003402	admin
00003411	admin
00003801	admin
00003802	admin
00003811	admin
00004401	admin
00004402	admin
00004411	admin
00004902	admin
00006001	admin

ID (log_id)	Sub Type (subtype)
00006002	admin
00006011	admin
00006102	admin
00006202	admin
00006302	admin
00006501	admin
00006502	admin
00006511	admin
00006541	admin
00006542	admin
00006551	admin
00007302	admin
00007402	admin
00008101	admin
00008102	admin
00008111	admin
00008602	admin
00008701	admin
00008702	admin
00008711	admin
00008801	admin
00008811	admin
00008901	admin
00008911	admin
00009001	admin
00009011	admin
00009101	admin
00009111	admin
00009201	admin
00009211	admin

ID (log_id)	Sub Type (subtype)
00009301	admin
00009311	admin
00009401	admin
00009402	admin
00009411	admin
00009501	admin
00009502	admin
00009511	admin
00009702	admin
00010001	admin
00010002	admin
00010011	admin
00010201	admin
00010202	admin
00010211	admin
00010401	admin
00010402	admin
00010411	admin
00010501	admin
00010502	admin
00010511	admin
00010601	admin
00010602	admin
00010611	admin
00010701	admin
00010711	admin
00011521	admin
00011522	admin
00011531	admin
00011671	admin

ID (log_id)	Sub Type (subtype)
00011672	admin
00011681	admin
00019001	admin
00019011	admin
00019102	admin
00019202	admin
00020088	admin
00020201	admin
00020202	admin
00020211	admin
00020301	admin
00020302	admin
00020311	admin
00020701	admin
00020702	admin
00020711	admin
00020801	admin
00020802	admin
00020811	admin
00020901	admin
00020902	admin
00020911	admin
00021002	admin
00021102	admin
00021140	admin
00021202	admin
00021302	admin
00021402	admin
00022997	admin
00030001	admin

ID (log_id)	Sub Type (subtype)
00030002	admin
00030011	admin
00032006	admin
00039001	admin
00039002	admin
00039011	admin
00039321	admin
00039322	admin
00039331	admin
00040001	admin
00040002	admin
00040011	admin
00040301	admin
00040302	admin
00040311	admin
00040501	admin
00040502	admin
00040511	admin
00040601	admin
00040602	admin
00040611	admin
00040623	admin
00040631	admin
00040632	admin
00040641	admin
00040751	admin
00040752	admin
00040761	admin
00040801	admin
00040802	admin

ID (log_id)	Sub Type (subtype)
00040811	admin
00040901	admin
00040902	admin
00040911	admin
00041001	admin
00041002	admin
00041011	admin
00041101	admin
00041102	admin
00041111	admin
00041201	admin
00041202	admin
00041211	admin
00041302	admin
00041401	admin
00041402	admin
00041411	admin
00041601	admin
00041602	admin
00041611	admin
00041801	admin
00041802	admin
00041811	admin
00042401	admin
00042402	admin
00042411	admin
00043001	admin
00043002	admin
00043011	admin
00044001	admin

ID (log_id)	Sub Type (subtype)
00044002	admin
00044011	admin
00044401	admin
00044411	admin
00044501	admin
00044502	admin
00044511	admin
00046001	admin
00046002	admin
00046011	admin
00050001	admin
00050002	admin
00050011	admin
00050201	admin
00050202	admin
00050211	admin
00050401	admin
00050402	admin
00050411	admin
00051001	admin
00051002	admin
00051011	admin
00051201	admin
00051202	admin
00051211	admin
00051401	admin
00051402	admin
00051411	admin
00051601	admin
00051602	admin

ID (log_id)	Sub Type (subtype)
00051611	admin
00051801	admin
00051802	admin
00051811	admin
00052201	admin
00052202	admin
00052211	admin
00052401	admin
00052402	admin
00052411	admin
00052601	admin
00052602	admin
00052611	admin
00053201	admin
00053202	admin
00053211	admin
00053701	admin
00053711	admin
00053901	admin
00053902	admin
00053911	admin
00054401	admin
00054402	admin
00054411	admin
00054601	admin
00054602	admin
00054611	admin
00054801	admin
00054802	admin
00054811	admin

ID (log_id)	Sub Type (subtype)
00055301	admin
00055302	admin
00055311	admin
00055501	admin
00055502	admin
00055511	admin
00055701	admin
00055702	admin
00055711	admin
00055901	admin
00055902	admin
00055911	admin
00055971	admin
00056401	admin
00056402	admin
00056411	admin
00056421	admin
00056601	admin
00056602	admin
00056611	admin
00058601	admin
00058602	admin
00058611	admin
00058621	admin
00058622	admin
00058631	admin
00059801	admin
00059802	admin
00059811	admin
00060001	admin

ID (log_id)	Sub Type (subtype)
00060002	admin
00060011	admin
00060201	admin
00060202	admin
00060211	admin
00061201	admin
00061202	admin
00061211	admin
00061401	admin
00061402	admin
00061411	admin
00061801	admin
00061802	admin
00061811	admin
00062001	admin
00062002	admin
00062011	admin
00062201	admin
00062202	admin
00062211	admin
00062401	admin
00062402	admin
00062411	admin
00063401	admin
00063402	admin
00063411	admin
00064401	admin
00064402	admin
00064411	admin
00065002	admin

ID (log_id)	Sub Type (subtype)
00065501	admin
00065502	admin
00065511	admin
00066002	admin
00066011	admin
00066101	admin
00066102	admin
00066111	admin
00066151	admin
00066201	admin
00066202	admin
00066211	admin
00066301	admin
00066302	admin
00066311	admin
00066401	admin
00066402	admin
00066411	admin
00066451	admin
00066452	admin
00066461	admin
00066501	admin
00066502	admin
00066511	admin
00066551	admin
00066552	admin
00066561	admin
00066601	admin
00066711	admin
00066801	admin

ID (log_id)	Sub Type (subtype)
00066802	admin
00066811	admin
00066901	admin
00066911	admin
00066921	admin
00066931	admin
00068001	admin
00068002	admin
00068011	admin
00068301	admin
00068302	admin
00068311	admin
00068401	admin
00068402	admin
00068411	admin
00068701	admin
00068711	admin
00068801	admin
00068802	admin
00068811	admin
00090001	admin
00090002	admin
00090011	admin
00090101	admin
00090102	admin
00090111	admin
00091101	admin
00091102	admin
00091111	admin
00093001	admin

ID (log_id)	Sub Type (subtype)
00093002	admin
00093011	admin
00093501	admin
00093502	admin
00093511	admin
10000009	system
10000010	system
10000011	system
10000012	system
10000013	system
10000014	system
10000015	system
10000016	system
10000017	system
10000018	system
10000019	system
10000020	system
10000021	system
10000022	system
10000023	system
10000027	system
10000028	system
10000031	system
10000048	system
11001008	system
11002003	system
11002004	system
11003601	system
11004002	system
11004601	system

ID (log_id)	Sub Type (subtype)
11004602	system
11004603	system
11004605	system
11004606	system
11004608	system
11005901	system
11006004	system
11006005	system
11006006	system
11006701	system
19999496	system
19999497	system
19999498	system

Reboot, shut down, & boot up messages

When FortiWeb is shutting down, if you are attached to the local console, the appliance outputs messages output to the CLI notifying you that the operating system is halting, such as:

The system is going down NOW !!

or:

System is rebooting...

As one of its final actions, if logging is enabled, FortiWeb records the shutdown (10000011) or reboot (10000010) in the event log. When FortiWeb starts up again, the local console displays:

System is started.

and it records the startup (10000009). Its subsystems are loaded and readied to do their work. At this time FortiWeb records daemon startups in the event log, such as 10000023 and 11001008.

Related

- 10000009
- 10000010
- 10000011
- 10000023
- 11001008

00001002

Meaning
An administrator changed a global setting.

Field name	Description
ID (`log_id`)	00001002 See Log ID numbers on page 24.
Level (`pri`)	`notification` or `information` See Priority level on page 25.

Examples
date=2016-02-18 time=10:00:05 log_id=00001002 msg_id=000067508821 device_id=FV400D3A15000010 vd="root" timezone="(GMT+3:00)Baghdad" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed global from GUI(172.22.6.66)"

Related

- 00021140
- 00006102

00001012

Meaning
A FortiWeb administrator changed the host name of the appliance.

Field name	Description
ID (`log_id`)	00001012 See Log ID numbers on page 24.
Level (`pri`)	`notification` or `information` (changing the idle GUI session timeout) See Priority level on page 25.

Examples
date=2014-04-10 time=12:11:17 log_id=00001012 msg_id=000000192621 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hostname global setting FortiWeb to 1KD_1 from GUI(172.22.6.240)"

Related

- 00001002

00001052

Meaning
An administrator changed the idle GUI session timeout.

Field name	Description
ID (`log_id`)	00001052 See Log ID numbers on page 24.
Level (`pri`)	`notification` or `information` (changing the idle GUI session timeout) See Priority level on page 25.

Examples
date=2014-04-10 time=12:10:51 log_id=00001052 msg_id=000000192620 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed idle GUI session timeout from GUI(172.22.6.240)"

Related

- 00001002

00001062

Meaning
An administrator changed the listening/source port for configuration synchronization with another FortiWeb.

Field name	Description
ID (`log_id`)	00001062 See Log ID numbers on page 24.
Level (`pri`)	`notice` See Priority level on page 25.

Examples
date=2014-09-10 time=22:16:40 log_id=00001062 msg_id=000003041952 device_id=FV400C3M14000006 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed sync-port global setting 8333 to 1111 from GUI(172.22.14.6)"

Related

- 00001002

00002202

Meaning
A FortiWeb administrator changed a setting in **System > Config > Advanced** on the appliance.

Field name	Description
ID (`log_id`)	00002202 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:43:22 log_id=00002202 msg_id=000000000042 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed advanced from GUI(172.20.120.47)"

00002801

Meaning
A FortiWeb administrator created an administrator access profile.

Field name	Description
ID (`log_id`)	00002801 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:43:04 log_id=00002801 msg_id=000000000041 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added accprofile read-only from GUI(172.20.120.47)"

Related

- 00002802
- 00002811
- 00003401

00002802

Meaning
A FortiWeb administrator changed an administrator access profile.

Field name	Description
ID (`log_id`)	00002802 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:43:14 log_id=00002802 msg_id=000000000042 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed accprofile read-only from GUI(172.20.120.47)"

Related

- 00002801
- 00002811
- 00003401

00002811

Meaning
A FortiWeb administrator deleted an administrator access profile.

Field name	Description
ID (`log_id`)	00002811 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:43:34 log_id=00002811 msg_id=000000000045 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted accprofile read-only from GUI(172.20.120.47)"

Related

- 00002801
- 00002802
- 00003401

00003401

Meaning
A FortiWeb administrator created an administrator account.

Field name	Description
ID (`log_id`)	00003401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:45:44 log_id=00003401 msg_id=000000000048 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added admin admin1 from GUI(172.20.120.47)"

Related

- 00003402
- 00003411
- 00002801
- 00004402
- 00010201
- 00010401
- 00010701

00003402

Meaning
A FortiWeb administrator changed an administrator account. This can include resetting the account's password.

Field name	Description
ID (`log_id`)	00003402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:45:44 log_id=00003402 msg_id=000000000049 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed admin admin1 from GUI(172.20.120.47)"

Related

- 00003401
- 00003411
- 00002801
- 00010201
- 00010401
- 00010701

00003411

Meaning
A FortiWeb administrator deleted an administrator account.

Field name	Description
ID (`log_id`)	00003411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:46:44 log_id=00003411 msg_id=000000000052 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted admin admin1 from GUI(172.20.120.47)"

Related

- 00003401
- 00003402
- 00002801

00003801

Meaning
A FortiWeb administrator added a WCCP client configuration.

Field name	Description
ID (`log_id`)	00003801 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:23:23 log_id=00003801 msg_id=000000004621 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wccp 52 from GUI(172.22.6.149)"

Related

- 00003802
- 00003811

00003802

Meaning
A FortiWeb administrator edited a WCCP client configuration.

Field name	Description
ID (`log_id`)	00003802 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:09:00 log_id=00003802 msg_id=000000004614 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wccp 51 from GUI(172.22.6.149)"

Related

- 00003801
- 00003811

00003811

Meaning
A FortiWeb administrator deleted a WCCP client configuration.

Field name	Description
ID (`log_id`)	00003811 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:41:12 log_id=00003811 msg_id=000000004626 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted wccp 52 from GUI(172.22.6.149)"

Related

- 00003801
- 00003802

00004401

Meaning
A FortiWeb administrator created a VLAN subinterface or link aggregate.

Field name	Description
ID (`log_id`)	00004401 See Log ID numbers on page 24.

Examples
date=2013-10-06 time=11:00:13 log_id=00004401 msg_id=000000001083 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=add status=success msg="User admin added interface vlan3 from console"

Related

- 00004402
- 00030001
- 00030011
- 11006004

00004402

Meaning
A FortiWeb administrator changed the IP address or allowed administrative access protocols of a network interface. This does **not** include bringing up or bringing down the interface (see 11006004).

Field name	Description
ID (`log_id`)	00004402 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI | none | telnet | ssh | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (`msg`)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2013-10-06 time=11:00:19 log_id=00004402 msg_id=000000001085 device_ id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed interface port1 from console"

Related

- 00003401
- 00004401
- 00006202
- 00030001

- 00030011
- 11006004

00004411

Meaning
A FortiWeb administrator deleted a VLAN subinterface or link aggregate.

Field name	Description
ID (`log_id`)	00004411 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI | none | telnet | ssh | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (`msg`)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2013-10-06 time=11:00:19 log_id=00004411 msg_id=000000001089 device_ id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=delete status=success msg="User admin deleted interface agg1 from console"

Related

- 00004401
- 00004402
- 00030001
- 00030011
- 11006004

00004902

Meaning
A FortiWeb administrator changed the operation mode.

Field name	Description
ID (`log_id`)	00004902 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (`msg`)	User <administrator_name> changed settings from {GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-05-14 time=18:05:27 log_id=00004902 msg_id=000000021625 device_id=FV-3KC3R10700108 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed settings from GUI(172.22.6.241)"

Related

- 00006001

00006001

Meaning
A FortiWeb administrator created a bridge (“V-Zone”).

Field name	Description
ID (`log_id`)	00006001 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}
Message (`msg`)	User <administrator_name> added V-Zone <bridge_name> from {GUI (<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin added V-Zone bridge1 from GUI(172.20.120.229)."

Related

- 00006002
- 00006011

00006002

Meaning
A FortiWeb administrator changed a bridge (“V-Zone”).

Field name	Description
ID (`log_id`)	00006002 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}
Message (`msg`)	User <administrator_name> modified V-Zone <bridge_name> from {GUI (<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin modified V-Zone bridge1 from GUI(172.20.120.229)."

Related

- 00006001
- 00006011

00006011

Meaning
A FortiWeb administrator deleted a bridge (“V-Zone”).

Field name	Description
ID (`log_id`)	00006011 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}
Message (`msg`)	User <administrator_name> deleted V-Zone <bridge_name> from {GUI (<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}.

Examples
date=2014-04-20 time=14:59:56 log_id=00090002 msg_id=000000176080 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=admin ui=GUI(172.20.120.229) msg="User admin deleted V-Zone bridge1 from GUI(172.20.120.229)."

Related

- 00006001
- 00006002

00006102

Meaning
A FortiWeb administrator changed the IP address of the configuration synchronization peer.

Field name	Description
ID (`log_id`)	00006102 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:47:28 log_id=00006102 msg_id=000000000060 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed conf-sync from GUI(172.20.120.47)"

Related

- 00001002

00006202

Meaning
A FortiWeb administrator changed the DNS settings.

Field name	Description
ID (`log_id`)	00006202 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:47:37 log_id=00006202 msg_id=000000000061 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed dns from GUI(172.20.120.47)"

Related

- 00004402
- 00030011

00006302

Meaning
A FortiWeb administrator changed the system-wide SNMP settings such as the description, location, or contact information.

Field name	Description
ID (`log_id`)	00006302 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:44:37 log_id=00006302 msg_id=000000000044 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed snmpsysinfo from GUI(172.20.120.47)"

Related

- 00004402
- 00006501

00006501

Meaning
A FortiWeb administrator added an SNMP community.

Field name	Description
ID (`log_id`)	00006501 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:45:04 log_id=00006501 msg_id=000000000045 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added snmp community 1 from GUI(172.20.120.47)"

Related

- 00004402
- 00006302
- 00006502
- 00006511

00006502

Meaning
A FortiWeb administrator changed an SNMP community setting such as the SNMP manager and trap events.

Field name	Description
ID (`log_id`)	00006502 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:45:04 log_id=00006502 msg_id=000000000046 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed snmp community 1 from GUI(172.20.120.47)"

Related

- 00004402
- 00006302
- 00006501
- 00006511

00006511

Meaning
A FortiWeb administrator deleted an SNMP community.

Field name	Description
ID (`log_id`)	00006511 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:47:11 log_id=00006511 msg_id=000000000059 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted snmp community 2 from GUI(172.20.120.47)"

Related

- 00004402
- 00006302
- 00006501
- 00006502

00006541

Meaning
A FortiWeb administrator added to an SNMP community the IP address of an SNMP manager that can receive traps from the FortiWeb appliance and is permitted to query the FortiWeb appliance.

Field name	Description
ID (`log_id`)	00006541 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=14:54:44 log_id=00006541 msg_id=000086989055 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added hosts 1 from GUI(172.22.6.114)"

Related

- 00006542
- 00006551

00006542

Meaning
In an SNMP community configuration, a FortiWeb administrator edited the IP address of an SNMP manager that can receive traps from the FortiWeb appliance and is permitted to query the FortiWeb appliance.

Field name	Description
ID (`log_id`)	00006542 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=15:15:08 log_id=00006542 msg_id=000086989074 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed hosts 1 from ssh(172.22.6.114)"

Related

- 00006541
- 00006551

00006551

Meaning
In an SNMP community configuration, a FortiWeb administrator deleted the IP address of an SNMP manager that can receive traps from the FortiWeb appliance and is permitted to query the FortiWeb appliance.

Field name	Description
ID (`log_id`)	00006551 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=15:11:35 log_id=00006551 msg_id=000086989063 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted hosts 1 from GUI(172.22.6.114)"

Related

- 00006541
- 00006542

00007302

Meaning
A FortiWeb administrator changed the setting that overrides the default Fortiguard Distribution Server (FDS).

Field name	Description
ID (`log_id`)	00007302 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=00:15:13 log_id=00007302 msg_id=000000070586 device_id=FV-1KC3R10700031 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-autoupdate-override from GUI(172.22.6.237)"

Related

- 00007402

00007402

Meaning
A FortiWeb administrator changed the configuration that determines how the FortiWeb appliance accesses the Fortinet Distribution Network (FDN) to retrieve updates.

Field name	Description
ID (`log_id`)	00007402 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:19:36 log_id=00007402 msg_id=000000734625 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-autoupdate-schedule from GUI(172.22.6.237)"

Related

- 00007302

00008101

Meaning
A FortiWeb administrator created a schedule for a periodic configuration backup to an FTP/SFTP server.

Field name	Description
ID (`log_id`)	00008101 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:42:14 log_id=00008101 msg_id=000000000037 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added backup scheduled_backup from GUI(172.20.120.47)"

Related

- 00004402
- 00008102
- 00008111

00008102

Meaning
A FortiWeb administrator changed a schedule for a periodic configuration backup to an FTP/SFTP server.

Field name	Description
ID (`log_id`)	00008102 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:42:24 log_id=00008102 msg_id=000000000038 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed backup scheduled_backup from GUI(172.20.120.47)"

Related

- 00004402
- 00008101
- 00008111

00008111

Meaning
A FortiWeb administrator deleted a schedule for a periodic configuration backup to an FTP/SFTP server.

Field name	Description
ID (`log_id`)	00008111 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:42:54 log_id=00008111 msg_id=000000000040 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted backup scheduled_backup from GUI(172.20.120.47)"

Related

- 00004402
- 00008101
- 00008102

00008602

Meaning
A FortiWeb administrator changed a TCP `SYN` flood denial of service (DoS) setting.

Field name	Description
ID (`log_id`)	00008602 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:38:51 log_id=00008602 msg_id=000000000174 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed dos-prevention from GUI(172.20.120.47)"

00008701

Meaning
A FortiWeb administrator uploaded a locally stored server certificate and (if applicable) private key.

Field name	Description
ID (`log_id`)	00008701 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:42:13 log_id=00008701 msg_id=000000000039 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added local certificate-with-key from GUI(172.20.120.47)"

Related

- 00008702
- 00008711

00008702

Meaning
A FortiWeb administrator changed the description of a locally stored server certificate and private key.

Field name	Description
ID (`log_id`)	00008702 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:42:53 log_id=00008702 msg_id=000000000040 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed local certificate-with-key from GUI(172.20.120.47)"

Related

- 00008701
- 00008711

00008711

Meaning
A FortiWeb administrator deleted a locally stored server certificate and (if applicable) private key.

Field name	Description
ID (`log_id`)	00008711 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=09:42:59 log_id=00008711 msg_id=000000000041 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted local certificate-with-key from GUI(172.20.120.47)"

Related

- 00008701
- 00008702

00008801

Meaning
A FortiWeb administrator added a configuration for a certificate of the HTTP CRL server of your certificate authority (CA).

Field name	Description
ID (`log_id`)	00008801 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:01:21 log_id=00008801 msg_id=000000179544 device_ id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added remote REMOTE_Cert_2 from GUI(172.22.6.66)"

Related

- 00008811
- 00009301
- 00009311
- 11006701

00008811

Meaning
A FortiWeb administrator deleted a configuration for a certificate of the HTTP CRL server of your certificate authority (CA).

Field name	Description
ID (`log_id`)	00008811 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:02:34 log_id=00008811 msg_id=000000179545 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted remote REMOTE_Cert_2 from GUI(172.22.6.66)"

Related

- 00008801
- 00009301
- 00009311
- 11006701

00008901

Meaning
A FortiWeb administrator added a certificate.

Field name	Description
ID (`log_id`)	00008901 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:03:26 log_id=00008901 msg_id=000000179546 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate ca CA_Cert_4 from GUI(172.22.6.66)"

Related

- 00008911

00008911

Meaning
A FortiWeb administrator deleted a certificate.

Field name	Description
ID (`log_id`)	00008911 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:03:31 log_id=00008911 msg_id=000000179547 device_ id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate ca CA_Cert_4 from GUI(172.22.6.66)"

Related

- 00008901

00009001

Meaning
A FortiWeb administrator added a certificate authorities (CA) group.

Field name	Description
ID (`log_id`)	00009001 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:06:20 log_id=00009001 msg_id=000000179548 device_ id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate ca-group ca_g from GUI(172.22.6.66)"

Related

- 00009011

00009011

Meaning
A FortiWeb administrator deleted a certificate authorities (CA) group.

Field name	Description
ID (`log_id`)	00009011 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:06:31 log_id=00009011 msg_id=000000179549 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate ca-group ca_g from GUI(172.22.6.66)"

Related

- 00009001

00009101

Meaning
A FortiWeb administrator added an intermediate CA certificate.

Field name	Description
ID (`log_id`)	00009101 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:09:10 log_id=00009101 msg_id=000000179550 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate intermediate-certificate Inter_Cert_1 from GUI (172.22.6.66)"

Related

- 00009111

00009111

Meaning
A FortiWeb administrator deleted an intermediate CA certificate.

Field name	Description
ID (`log_id`)	00009111 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:09:14 log_id=00009111 msg_id=000000179551 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate intermediate-certificate Inter_Cert_1 from GUI (172.22.6.66)"

Related

- 00009101

00009201

Meaning
A FortiWeb administrator added an intermediate CA certificate group.

Field name	Description
ID (`log_id`)	00009201 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:10:42 log_id=00009201 msg_id=000000179552 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate intermediate-certificate-group inter_g from GUI (172.22.6.66)"

Related

- 00009211

00009211

Meaning
A FortiWeb administrator deleted an intermediate CA certificate group.

Field name	Description
ID (`log_id`)	00009211 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:10:46 log_id=00009211 msg_id=000000179553 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate intermediate-certificate-group inter_g from GUI (172.22.6.66)"

Related

- 00009201

00009301

Meaning
A FortiWeb administrator added a certificate revocation list (CRL) configuration.

Field name	Description
ID (`log_id`)	00009301 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:12:24 log_id=00009301 msg_id=000000179554 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate crl CRL_4 from GUI(172.22.6.66)"

Related

- 00008801
- 00008811
- 00009311
- 11006701

00009311

Meaning
A FortiWeb administrator deleted a certificate revocation list (CRL) configuration.

Field name	Description
ID (`log_id`)	00009311 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:12:28 log_id=00009311 msg_id=000000179555 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate crl CRL_4 from GUI(172.22.6.66)"

Related

- 00008801
- 00008811
- 00009301
- 11006701

00009401

Meaning
A FortiWeb administrator added a certificate verification rule.

Field name	Description
ID (`log_id`)	00009401 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:15:06 log_id=00009401 msg_id=000000179559 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate verify CV from GUI(172.22.6.66)"

Related

- 00009402
- 00009411

00009402

Meaning
A FortiWeb administrator edited a certificate verification rule.

Field name	Description
ID (`log_id`)	00009402 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:15:11 log_id=00009402 msg_id=000000179560 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed certificate verify CV from GUI(172.22.6.66)"

Related

- 00009401
- 00009411

00009411

Meaning
A FortiWeb administrator deleted a certificate verification rule.

Field name	Description
ID (`log_id`)	00009411 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:15:14 log_id=00009411 msg_id=000000179561 device_id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate verify CV from GUI(172.22.6.66)"

Related

- 00009401
- 00009402

00009501

Meaning
A FortiWeb administrator added a Server Name Indication (SNI) configuration.

Field name	Description
ID (`log_id`)	00009501 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=11:16:33 log_id=00009501 msg_id=000000003148 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added certificate sni online_store from GUI(172.20.120.61)"

Related

- 00009502
- 00009511

00009502

Meaning
A FortiWeb administrator changed a Server Name Indication (SNI) configuration.

Field name	Description
ID (`log_id`)	00009502 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=11:16:33 log_id=00009502 msg_id=000000003148 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin changed certificate sni online_store from GUI(172.20.120.61)"

Related

- 00009501
- 00009511

00009511

Meaning
A FortiWeb administrator deleted a Server Name Indication (SNI) configuration.

Field name	Description
ID (`log_id`)	00009511 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=11:25:07 log_id=00009511 msg_id=000000003149 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted certificate sni online_store from GUI(172.20.120.61)"

Related

- 00009501
- 00009502

00009702

Meaning
A FortiWeb administrator changed system-wide FortiGuard Antivirus scan settings.

Field name	Description
ID (`log_id`)	00009702 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:31:09 log_id=00009702 msg_id=000000734627 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed system-antivirus from GUI(172.22.6.237)"

00010001

Meaning
A FortiWeb administrator added a locally-defined account for a website end-user.

Field name	Description
ID (`log_id`)	00010001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:01:51 log_id=00010001 msg_id=000000000079 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added local-user user1 from GUI(172.20.120.47)"

Related

- 00010002
- 00010201
- 00010401
- 00010501

00010002

Meaning
A FortiWeb administrator changed a locally defined account for a website end-user.

Field name	Description
ID (`log_id`)	00010002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:01:56 log_id=00010002 msg_id=000000000080 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed local-user user1 from GUI(172.20.120.47)"

Related

- 00010001
- 00010011
- 00010501

00010011

Meaning
A FortiWeb administrator deleted a locally-defined account for a website end-user.

Field name	Description
ID (`log_id`)	00010011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:01:59 log_id=00010011 msg_id=000000000081 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted local-user user1 from GUI(172.20.120.47)"

Related

- 00010001
- 00010002

00010201

Meaning
A FortiWeb administrator added an LDAP query.

Field name	Description
ID (`log_id`)	00010201 See Log ID numbers on page 24.

Examples
date=2013-10-09 time=15:44:16 log_id=00010201 msg_id=000000000310 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added ldap-user ldap-query1 from GUI(172.20.120.47)"

Related

- 00010202
- 00010211
- 00010001
- 00003401

00010202

Meaning
A FortiWeb administrator changed an LDAP query.

Field name	Description
ID (`log_id`)	00010202 See Log ID numbers on page 24.

Examples
date=2013-10-09 time=15:44:23 log_id=00010202 msg_id=000000000311 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed ldap-user ldap-query1 from GUI(172.20.120.47)"

Related

- 00010201
- 00010211
- 00010001
- 00003401

00010211

Meaning
A FortiWeb administrator deleted an LDAP query.

Field name	Description
ID (`log_id`)	00010211 See Log ID numbers on page 24.

Examples
date=2013-10-09 time=15:44:32 log_id=00010211 msg_id=000000000312 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted ldap-user ldap-query1 from GUI(172.20.120.47)"

Related

- 00010201
- 00010202
- 00010001
- 00003401

00010401

Meaning
A FortiWeb administrator created a RADIUS query.

Field name	Description
ID (`log_id`)	00010401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:02:59 log_id=00010401 msg_id=000000000082 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added radius-user radius-query1 from GUI(172.20.120.47)"

Related

- 00010402
- 00010411
- 00010001
- 00003401

00010402

Meaning
A FortiWeb administrator changed a RADIUS query.

Field name	Description
ID (`log_id`)	00010402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:03:14 log_id=00010402 msg_id=000000000083 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed radius-user radius-query1 from GUI(172.20.120.47)"

Related

- 00010401
- 00010411
- 00010001
- 00003401

00010411

Meaning
A FortiWeb administrator deleted a RADIUS query.

Field name	Description
ID (`log_id`)	00010411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:03:24 log_id=00010411 msg_id=000000000084 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted radius-user radius-query1 from GUI(172.20.120.47)"

Related

- 00010401
- 00010402
- 00010001
- 00003401

00010501

Meaning
A FortiWeb administrator added an NTLM query.

Field name	Description
ID (`log_id`)	00010501 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:03:34 log_id=00010501 msg_id=000000000085 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added ntlm-user ntlm-query1 from GUI(172.20.120.47)"

Related

- 00010502
- 00010511
- 00010001

00010502

Meaning
A FortiWeb administrator changed an NTLM query.

Field name	Description
ID (`log_id`)	00010502 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:03:44 log_id=00010502 msg_id=000000000086 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed ntlm-user ntlm-query1 from GUI(172.20.120.47)"

Related

- 00010501
- 00010511
- 00010001

00010511

Meaning
A FortiWeb administrator deleted an NTLM query.

Field name	Description
ID (`log_id`)	00010511 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:03:54 log_id=00010511 msg_id=000000000087 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted ntlm-user ntlm-query1 from GUI(172.20.120.47)"

Related

- 00010501
- 00010502
- 00010001

00010601

Meaning
A FortiWeb administrator added a user group.

Field name	Description
ID (`log_id`)	00010601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:04:07 log_id=00010601 msg_id=000000000082 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added User Group user-group1 from GUI(172.20.120.47)"

Related

- 00010602
- 00010611
- 00010201
- 00010401
- 00010501
- 00010001

00010602

Meaning
A FortiWeb administrator changed a user group.

Field name	Description
ID (`log_id`)	00010602 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:06:24 log_id=00010602 msg_id=000000000083 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed user user-group user-group1 from GUI(172.20.120.47)"

Related

- 00010601
- 00010611
- 00010201
- 00010401
- 00010501
- 00010001

00010611

Meaning
A FortiWeb administrator deleted a user group.

Field name	Description
ID (`log_id`)	00010611 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:06:34 log_id=00010611 msg_id=000000000084 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin deleted user user-group user-group1 from GUI(172.20.120.47)"

Related

- 00010602
- 00010601
- 00010201
- 00010401
- 00010501
- 00010001

00010701

Meaning
A FortiWeb administrator added an administrator group.

Field name	Description
ID (`log_id`)	00010701 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:06:46 log_id=00010701 msg_id=000000000085 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added user admin-group admin-query-group1 from GUI(172.20.120.47)"

Related

- 00010711
- 00010201
- 00010401
- 00003401

00010711

Meaning
A FortiWeb administrator deleted an administrator group.

Field name	Description
ID (`log_id`)	00010711 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:06:46 log_id=00010701 msg_id=000000000085 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin deleted user admin-group admin-query-group1 from GUI(172.20.120.47)"

Related

- 00010701
- 00010201
- 00010401
- 00003401

00011521

Meaning
A FortiWeb administrator added an SNMP version 3 user.

Field name	Description
ID (`log_id`)	00011521 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=14:51:45 log_id=00011521 msg_id=000086989048 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added snmp user ccc from GUI(172.22.6.114)"

Related

- 00011522
- 00011531

00011522

Meaning
A FortiWeb administrator edited an SNMP version 3 user.

Field name	Description
ID (`log_id`)	00011522 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=15:18:15 log_id=00011522 msg_id=000086989075 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed snmp user aa from ssh(172.22.6.114)"

Related

- 00011521
- 00011531

00011531

Meaning
A FortiWeb administrator deleted an SNMP version 3 user.

Field name	Description
ID (`log_id`)	00011531 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=14:56:08 log_id=00011531 msg_id=000086989059 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted snmp user ccc from GUI(172.22.6.114)"

Related

- 00011521
- 00011522

00011671

Meaning
A FortiWeb administrator added the IP address of an SNMP manager that can receive traps from the FortiWeb appliance and is permitted to query the FortiWeb appliance to an SNMP version 3 user configuration.

Field name	Description
ID (`log_id`)	00011671 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=14:51:46 log_id=00011671 msg_id=000086989049 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added hosts 1 from GUI(172.22.6.114)"

Related

- 00011672
- 00011681

00011672

Meaning
A FortiWeb administrator edited the IP address of an SNMP manager that can receive traps from the FortiWeb appliance and is permitted to query the FortiWeb appliance to an SNMP version 3 user configuration.

Field name	Description
ID (`log_id`)	00011672 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=15:21:33 log_id=00011672 msg_id=000086989077 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed hosts 1 from ssh(172.22.6.114)"

Related

- 00011671
- 00011681

00011681

Meaning
A FortiWeb administrator deleted the IP address of an SNMP manager that can receive traps from the FortiWeb appliance and is permitted to query the FortiWeb appliance to an SNMP version 3 user configuration.

Field name	Description
ID (`log_id`)	00011681 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=15:21:57 log_id=00011681 msg_id=000086989078 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=delete status=success msg="User admin deleted hosts 1 from ssh(172.22.6.114)"

Related

- 00011671
- 00011672

00019001

Meaning
An administrator added an image to use in error or authentication pages.

Field name	Description
ID (`log_id`)	00019001 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=14:27:09 log_id=00019001 msg_id=000009038094 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added replacemsg-image cc from GUI(172.22.6.1)"

Related

- 00019011

00019011

Meaning
An administrator deleted an image to use in error or authentication pages.

Field name	Description
ID (`log_id`)	00019011 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=14:28:11 log_id=00019011 msg_id=000009038095 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted replacemsg-image cc from GUI(172.22.6.1)"

Related

- 00019001

00019102

Meaning
A FortiWeb administrator edited a replacement message.

Field name	Description
ID (`log_id`)	00019102 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
User Interface (`ui`)	`GUI`
Action (`action`)	`edit`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> changed replacemsg <page_name> from GUI(<mgmt_ip>)

Examples
date=2016-02-18 time=15:22:45 log_id=00019102 msg_id=000067508853 device_ id=FV400D3A15000010 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed replacemsg token from GUI(172.22.6.66)" date=2016-02-18 time=15:22:20 log_id=00019102 msg_id=000067508851 device_ id=FV400D3A15000010 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed replacemsg login from GUI(172.22.6.66)"

00019202

Meaning
A FortiWeb administrator edited the FortiGate integration configuration.

Field name	Description
ID (`log_id`)	00019202 See Log ID numbers on page 24.

Examples
date=2016-02-22 time=07:55:52 log_id=00019202 msg_id=000000003099 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed fortigate-integration from GUI(172.20.120.185)"

00020088

Meaning
During a firmware upgrade, if the new firmware uses a different format for any existing settings, FortiWeb will attempt also to upgrade the configuration. If FortiWeb had to convert any settings to the new format, this log is recorded. Normally, no action is required. However, if you notice any behavior changes after the upgrade, you may want to compare your configuration with a backup copy to verify that it has been converted correctly. This is especially true if you have not followed the upgrade path recommended in the Release Notes.

Field name	Description
ID (`log_id`)	00020088 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`unknown`
User Interface (`ui`)	
Action (`action`)	`upgrade`
Status (`status`)	`success`
Message (`msg`)	The old configurations are not compatible with the new version, and some of them have been changed to be correct.

Examples
date=2012-11-04 time=19:11:01 log_id=00020088 msg_id=000000853622 type=event subtype="system" pri=information device_id=FVVM080000005545 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" user=unknown ui="" action=upgrade status=success reason=none msg="The old configurations are not compatible with the new version, and some of them have been changed to be correct."

00020201

Meaning
A FortiWeb administrator configured a connection to a Syslog server.

Field name	Description
ID (`log_id`)	00020201 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:43:02 log_id=00020201 msg_id=000001014451 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added syslog-policy 1 from GUI(172.22.6.231)"

Related

- 00020202
- 00020211

00020202

Meaning
A FortiWeb administrator changed the configuration of a connection to a Syslog server.

Field name	Description
ID (`log_id`)	00020202 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:43:32 log_id=00020202 msg_id=000001014452 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed syslog-policy 1 from GUI(172.22.6.231)"

Related

- 00020201
- 00020211

00020211

Meaning
A FortiWeb administrator deleted a connection to a Syslog server.

Field name	Description
ID (`log_id`)	00020211 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:43:42 log_id=00020211 msg_id=000001014453 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted syslog-policy 1 from GUI(172.22.6.231)"

Related

- 00020201
- 00020202

00020301

Meaning
A FortiWeb administrator added an email policy.

Field name	Description
ID (`log_id`)	00020301 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:37:10 log_id=00020301 msg_id=000001014448 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added mail-policy test from GUI(172.22.6.231)"

Related

- 00020302
- 00020311

00020302

Meaning
A FortiWeb administrator made changes to an email policy.

Field name	Description
ID (`log_id`)	00020302 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:38:20 log_id=00020302 msg_id=000001014449 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed mail-policy test from GUI(172.22.6.231)"

Related

- 00020311

00020311

Meaning
A FortiWeb administrator deleted an email policy.

Field name	Description
ID (`log_id`)	00020311 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:40:17 log_id=00020311 msg_id=000001014450 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted mail-policy test from GUI(172.22.6.231)"

Related

- 00020302

00020701

Meaning
A FortiWeb administrator added a configuration that sends log messages to an FTP/TFTP server.

Field name	Description
ID (`log_id`)	00020701 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:46:22 log_id=00020701 msg_id=000139289582 device_id=FV-1KD3A15800072 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added ftp-policy 123 from GUI(172.22.6.234)"

Related

- 00020702
- 00020811

00020702

Meaning
A FortiWeb administrator edited a configuration that sends log messages to an FTP/TFTP server.

Field name	Description
ID (`log_id`)	00020702 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:52:44 log_id=00020702 msg_id=000139289584 device_id=FV-1KD3A15800072 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed ftp-policy 123 from GUI(172.22.6.234)"

Related

- 00020701
- 00020811

00020711

Meaning
A FortiWeb administrator deleted a configuration that sends log messages to an FTP/TFTP server.

Field name	Description
ID (`log_id`)	00020711 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:52:44 log_id=00020702 msg_id=000139289584 device_id=FV-1KD3A15800072 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted ftp-policy 123 from GUI(172.22.6.234)"

Related

- 00020701
- 00020702 on page 135

00020801

Meaning
A FortiWeb administrator added a configuration that sends log messages to a remote FortiAnalyzer appliance.

Field name	Description
ID (`log_id`)	00020801 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:06:28 log_id=00020801 msg_id=000001014461 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added fortianalyzer-policy test from GUI(172.22.6.231)"

Related

- 00020802
- 00020811

00020802

Meaning
A FortiWeb administrator made changes to a configuration that sends log messages to a remote FortiAnalyzer appliance.

Field name	Description
ID (`log_id`)	00020802 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:07:10 log_id=00020802 msg_id=000001014462 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed fortianalyzer-policy test from GUI(172.22.6.231)"

Related

- 00020801
- 00020811

00020811

Meaning
A FortiWeb administrator deleted a configuration that sends log messages to a remote FortiAnalyzer appliance.

Field name	Description
ID (`log_id`)	00020811 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:07:40 log_id=00020811 msg_id=000001014463 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted fortianalyzer-policy test from GUI(172.22.6.231)"

Related

- 00020801
- 00020802

00020901

Meaning
A FortiWeb administrator added a trigger policy that is used by the notification process.

Field name	Description
ID (`log_id`)	00020901 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:08:51 log_id=00020901 msg_id=000001014464 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added trigger-policy 1 from GUI(172.22.6.231)"

Related

- 00020902
- 00020911

00020902

Meaning
A FortiWeb administrator made a change to a trigger policy that is used by the notification process.

Field name	Description
ID (`log_id`)	00020902 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:09:39 log_id=00020902 msg_id=000001014465 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed trigger-policy 1 from GUI(172.22.6.231)"

Related

- 00020901
- 00020911

00020911

Meaning
A FortiWeb administrator deleted a trigger policy that is used by the notification process.

Field name	Description
ID (`log_id`)	00020911 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:10:10 log_id=00020911 msg_id=000001014466 device_id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted trigger-policy 1 from GUI(172.22.6.231)"

Related

- 00020901
- 00020902

00021002

Meaning
A FortiWeb administrator enabled or disabled storing logs on the appliance's hard disk.

Field name	Description
ID (`log_id`)	00021002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=01:34:07 log_id=00021002 msg_id=000000000016 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed setting for saving logs to disk from GUI"

Related

- 00021302

00021102

Meaning
A FortiWeb administrator changed the configuration for event logging to memory (RAM).

Field name	Description
ID (`log_id`)	00021102 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:10:52 log_id=00021102 msg_id=000001014467 device_ id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed memory from GUI(172.22.6.231)"

00021140

Meaning
The FortiWeb's system clock was updated via NTP. If you are using FortiWeb-VM, this message is often displayed after you unsuspend the VM.

Field name	Description
ID (`log_id`)	00021140 See Log ID numbers on page 24.
Level (`pri`)	`notification` See Priority level on page 25.
User (`user`)	`ntp_daemon`
User Interface (`ui`)	`none`

Examples
date=2014-09-11 time=11:51:56 log_id=00021140 msg_id=000000133596 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=notice trigger_policy="" user=ntp_daemon ui=none action=edit status=success msg="global time setting change field:date-time The ntp daemon changed time from Wed Sep 10 20:51:48 2014 to Thu Sep 11 03:51:56 2014 "

Related

- 00001002

00021202

Meaning
A FortiWeb administrator changed the configuration for recording attack log messages on the local FortiWeb disk.

Field name	Description
ID (`log_id`)	00021202 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=12:02:33 log_id=00021202 msg_id=000001014457 device_ id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed attack-log from GUI(172.22.6.231)"

00021302

Meaning
A FortiWeb administrator enabled or disabled storing traffic logs on the appliance's hard disk.

Field name	Description
ID (`log_id`)	00021302 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=01:34:51 log_id=00021302 msg_id=000000000017 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=edit status=success msg="User admin changed traffic log setting from GUI"

Related

- 00021002

00021402

Meaning
A FortiWeb administrator made changes to the configuration for event log recording.

Field name	Description
ID (`log_id`)	00021402 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:48:20 log_id=00021402 msg_id=000001015952 device_ id=FV400C3M12000023 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed event-log from GUI(172.22.6.231)"

00022997

Meaning

FortiWeb does not have enough hard disk space in order to store data gathered for auto-learning.

Solution

If you have just updated the firmware, check the Release Notes. (Some firmware updates require that you resize the partitions before you upgrade. If you missed this step, it will cause this log message.)

If this log message is preceded by log ID 11006005, auto-learning data could not be stored because the data disk's file system is not currently mounted. For solutions, see 11006005.

Otherwise, delete any unnecessary auto-learning data, and disable it in policies where it is no longer required. This will free disk space.

Field name	Description
ID (`log_id`)	00022997 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`alert` See Priority level on page 25.
Message (`msg`)	Disk free space is not enough for autolearn

Examples

date=2012-09-27 time=07:44:00 log_id=00022997 msg_id=000000018352 type=event subtype="system" pri=alert device_id=FV-1KC3R11700136 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" msg="Disk free space is not enough for autolearn"

Related

- 11006005

00030001

Meaning
An administrator created an IP-layer static route.

Field name	Description
ID (`log_id`)	00030001 See Log ID numbers on page 24.

Examples
date=2013-10-06 time=11:03:37 log_id=00030001 msg_id=000000001086 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=add status=success msg="User admin added static-route 1 from console"

Related

- 00004402
- 00006202
- 00030002
- 00030011
- 00040623

00030002

Meaning
An administrator changed an IP-layer static route.

Field name	Description
ID (`log_id`)	00030002 See Log ID numbers on page 24.

Examples
date=2013-10-06 time=11:03:47 log_id=00030002 msg_id=000000001087 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=add status=success msg="User admin changed static-route 1 from console"

Related

- 00004402
- 00006202
- 00030001
- 00030011
- 00040623

00030011

Meaning
An administrator deleted an IP-layer static route.

Field name	Description
ID (`log_id`)	00030011 See Log ID numbers on page 24.

Examples
date=2013-10-06 time=11:00:12 log_id=00030011 msg_id=000000001084 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=console action=del status=success msg="User admin deleted static-route 1 from console"

Related

- 00030001
- 00030002
- 00004402
- 00040623

00032006

Meaning
Either: • The maximum number of concurrent sessions has been reached. For more information on model- or configuration-dependent limits, see the *FortiWeb Administration Guide*. • A policy was reloaded after a configuration change in order to free memory.

Field name	Description
ID (`log_id`)	00032006 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
Level (`pri`)	`information` (login or daemon start) or `alert` (concurrent session limit reached) See Priority level on page 25.
Message (`msg`)	policy <policy_name> concurrent session exceed threshold policy <policy_name> refreshed to free resources

Examples
date=2012-10-25 time=09:31:07 log_id=00032006 msg_id=000066877877 type=event subtype="admin" pri=alert device_id=FVVM020000003619 vd="root" timezone="(GMT)Greenwich Mean Time: Dublin,Edinburgh,Lisbon,London" msg="policy policy1 concurrent session exceed threshold"
date=2013-01-16 time=12:27:33 log_id=00032006 msg_id=000000201047 type=event subtype="admin" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" msg="policy policy1 refreshed to free resources"

Related

- 10000014

00039001

Meaning
An administrator created a server health check.

Field name	Description
ID (`log_id`)	00039001 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=13:53:02 log_id=00039001 msg_id=000009038075 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added health abc from GUI(172.22.6.1)"

Related

- 00039002
- 00039011

00039002

Meaning
An administrator edited a server health check.

Field name	Description
ID (`log_id`)	00039002 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=14:05:31 log_id=00039002 msg_id=000009038078 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed health abc from GUI(172.22.6.1)"

Related

- 00039001
- 00039011

00039011

Meaning
An administrator deleted a server health check.

Field name	Description
ID (`log_id`)	00039011 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=14:12:54 log_id=00039011 msg_id=000009038082 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted health abc from GUI(172.22.6.1)"

Related

- 00039001
- 00039002

00039321

Meaning
An administrator created a rule in a server health check.

Field name	Description
ID (`log_id`)	00039321 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=13:53:02 log_id=00039321 msg_id=000009038076 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added health check list 1 from GUI(172.22.6.1)"

Related

- 00039322
- 00039331

00039322

Meaning
An administrator edited a rule in a server health check.

Field name	Description
ID (`log_id`)	00039322 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=14:10:02 log_id=00039322 msg_id=000009038080 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed health check list 1 from GUI(172.22.6.1)"

Related

- 00039321
- 00039331

00039331

Meaning
An administrator deleted a rule in a server health check.

Field name	Description
ID (`log_id`)	00039331 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=14:11:43 log_id=00039331 msg_id=000009038081 device_id=FV-3KC0123456789 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted health check list 1 from GUI(172.22.6.1)"

Related

- 00039321
- 00039322

00040001

Meaning
An administrator created a server availability monitor (“health check”).

Field name	Description
ID (`log_id`)	00040001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:14:10 log_id=00040001 msg_id=000000000105 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added health uptime-check1 from GUI(172.20.120.47)

Related

- 00040002
- 00040011
- 19999496

00040002

Meaning
An administrator changed a server availability monitor (“health check”).

Field name	Description
ID (`log_id`)	00040002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:14:20 log_id=00040002 msg_id=000000000106 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed health uptime-check1 from GUI(172.20.120.47)"

Related

- 00040001
- 00040011
- 19999496

00040011

Meaning
An administrator deleted a server availability monitor (“health check”).

Field name	Description
ID (`log_id`)	00040011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:14:30 log_id=00040011 msg_id=000000000107 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted health uptime-check1 from GUI(172.20.120.47)"

Related

- 00040002
- 00040001
- 19999496

00040301

Meaning
An administrator created a network service definition such as `HTTP_8080` or `HTTPS4443`.

Field name	Description
ID (`log_id`)	00040301 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:23:14 log_id=00040301 msg_id=000000000138 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=succes smsg="User admin added custome service soap-service from GUI(172.20.120.47)"

Related

- 00040302
- 00040311

00040302

Meaning
An administrator changed a network service definition.

Field name	Description
ID (`log_id`)	00040302 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:23:18 log_id=00040302 msg_id=000000000139 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=succes smsg="User admin changed custom service soap-service from GUI(172.20.120.47)"

Related

- 00040301
- 00040311

00040311

Meaning
An administrator deleted a network service definition.

Field name	Description
ID (`log_id`)	00040311 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:23:34 log_id=00040311 msg_id=000000000140 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=succes smsg="User admin deleted custom service soap-service from GUI(172.20.120.47)"

Related

- 00040302
- 00040301

00040501

Meaning
An administrator added a virtual server.

Field name	Description
ID (`log_id`)	00040501 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=14:15:55 log_id=00040501 msg_id=000000055147 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added Virtual Server 1 from GUI(172.22.6.149)"

Related

- 00040502
- 00040511

00040502

Meaning
An administrator edited a virtual server.

Field name	Description
ID (`log_id`)	00040502 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=14:16:22 log_id=00040502 msg_id=000000055149 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed Virtual Server FortiWeb_Vserver from GUI(172.22.6.149)"

Related

- 00040501
- 00040511

00040511

Meaning
An administrator deleted a virtual server.

Field name	Description
ID (`log_id`)	00040511 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=14:16:11 log_id=00040511 msg_id=000000055148 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted Virtual Server 1 from GUI(172.22.6.149)"

Related

- 00040501
- 00040502

00040601

Meaning
An administrator created an HTTP-layer route (“content route”).

Field name	Description
ID (`log_id`)	00040601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:11:09 log_id=00040601 msg_id=000000000091 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)"type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy HTTP-content-routing content-route1 from GUI(172.20.120.47)"

Related

- 00040611
- 00040623
- 00030001

00040602

Meaning
An administrator edited the server pool configuration in an HTTP Content Routing policy.

Field name	Description
ID (`log_id`)	00040602 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:42:11 log_id=00040602 msg_id=001248141083 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy HTTP-content-routing content-routing-policy-to-web from GUI (172.22.6.1)"

Related

- 00040601
- 00040611
- 00040623

00040611

Meaning
An administrator deleted an HTTP-layer route (“content route”).

Field name	Description
ID (`log_id`)	00040611 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:11:45 log_id=00040611 msg_id=000000000093 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy HTTP-content-routing content-route1 from GUI(172.20.120.47)"

Related

- 00040601
- 00040623
- 00030001

00040623

Meaning
An administrator changed an HTTP-layer route (“content route”).

Field name	Description
ID (`log_id`)	00040623 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=14:24:08 log_id=00040623 msg_id=000000055157 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin changed server-policy HTTP-content-routing FortiWeb_ContentRouting1 list 2 from GUI(172.22.6.149)"

Related

- 00040601
- 00040611
- 00030001

00040631

Meaning
An administrator added a list of objects to match in an HTTP Content Routing policy.

Field name	Description
ID (`log_id`)	00040631 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:30:01 log_id=00040631 msg_id=001248141069 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy HTTP-content-routing new-content-routing content-routing-match-list 1 from GUI(172.22.6.1)"

Related

- 00040632
- 00040641

00040632

Meaning
An administrator edited the list of objects to match in an HTTP Content Routing policy.

Field name	Description
ID (`log_id`)	00040632 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:39:51 log_id=00040632 msg_id=001248141079 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy HTTP-content-routing content-routing-policy-to-web content-routing- match-list 1 from GUI(172.22.6.1)"

Related

- 00040631
- 00040641

00040641

Meaning
An administrator deleted the list of objects to match in an HTTP Content Routing policy.

Field name	Description
ID (`log_id`)	00040641 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:41:11 log_id=00040641 msg_id=001248141081 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted server-policy HTTP-content-routing content-routing-policy-to-web content-routing-match-list 1 from GUI(172.22.6.1)"

Related

- 00040631
- 00040632

00040751

Meaning
An administrator uploaded a customized HTTP error web page.

Field name	Description
ID (`log_id`)	00040751 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:18:58 log_id=00040751 msg_id=000000820249 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy error-page myerrorpage from GUI(172.22.6.230)

Related

- 00040752
- 00040761

00040752

Meaning
An administrator changed the description for a customized HTTP error web page.

Field name	Description
ID (`log_id`)	00040752 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:22:11 log_id=00040752 msg_id=000000000132 device_id=FVVM00UNLICENSED timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy error-page custom-500 from GUI(172.20.120.47)"

Related

- 00040751
- 00040761

00040761

Meaning
An administrator deleted a customized HTTP error web page.

Field name	Description
ID (`log_id`)	00040761 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:22:21 log_id=00040761 msg_id=000000000133 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy error-page custom-500 from GUI(172.20.120.47)"

Related

- 00040751
- 00040752

00040801

Meaning
An administrator created a customized data type definition.

Field name	Description
ID (`log_id`)	00040801 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:36:11 log_id=00040801 msg_id=000000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy pattern custom-data-type data-type1 from GUI(172.20.120.47)"

Related

- 00040802
- 00040811

00040802

Meaning
An administrator changed a customized data type definition.

Field name	Description
ID (`log_id`)	00040802 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:36:14 log_id=00040802 msg_id=000000000157 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy pattern custom-data-type data-type1 from GUI(172.20.120.47)"

Related

- 00040801
- 00040811

00040811

Meaning
An administrator deleted a customized data type definition.

Field name	Description
ID (`log_id`)	00040811 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:36:21 log_id=00040811 msg_id=000000000158 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy pattern custom-data-type data-type1 from GUI(172.20.120.47)"

Related

- 00040802
- 00040801

00040901

Meaning
An administrator created a group of customized data type definitions.

Field name	Description
ID (`log_id`)	00040901 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:37:29 log_id=00040901 msg_id=000000000160 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy pattern data-type-group custom-data-type-group1 from GUI (172.20.120.47)"

Related

- 00040902
- 00040911

00040902

Meaning
An administrator changed a group of customized data type definitions.

Field name	Description
ID (`log_id`)	00040902 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:37:39 log_id=00040902 msg_id=000000000161 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy pattern data-type-group custom-data-type-group1 from GUI (172.20.120.47)"

Related

- 00040901
- 00040911

00040911

Meaning
An administrator deleted a group of customized data type definitions.

Field name	Description
ID (`log_id`)	00040911 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:37:49 log_id=00040911 msg_id=000000000161 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy pattern data-type-group custom-data-type-group1 from GUI (172.20.120.47)"

Related

- 00040902
- 00040901

00041001

Meaning
An administrator created a customized suspicious URL definition.

Field name	Description
ID (`log_id`)	00041001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:35:29 log_id=00041001 msg_id=000000000152 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-susp-url suspicious-url1 from GUI(172.20.120.47)"

Related

- 00041002
- 00041011

00041002

Meaning
An administrator changed a customized suspicious URL definition.

Field name	Description
ID (`log_id`)	00041002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:35:39 log_id=00041002 msg_id=000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-susp-url suspicious-url1 from GUI(172.20.120.47)"

Related

- 00041011
- 00041001

00041011

Meaning
An administrator deleted a customized suspicious URL definition.

Field name	Description
ID (`log_id`)	00041011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:35:49 log_id=00041011 msg_id=000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-susp-url suspicious-url1 from GUI(172.20.120.47)"

Related

- 00041002
- 00041001

00041101

Meaning
An administrator created a group of customized suspicious URL definitions (“policy”).

Field name	Description
ID (`log_id`)	00041101 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:35:44 log_id=00041101 msg_id=000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada) "type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-susp-url-rule suspicious-urls-all from GUI(172.20.120.47)"

Related

- 00041102
- 00041111

00041102

Meaning
An administrator changed a group of customized suspicious URL definitions.

Field name	Description
ID (`log_id`)	00041102 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:35:45 log_id=00041102 msg_id=000000000154 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada) "type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-susp-url-rule suspicious-urls-all from GUI(172.20.120.47)"

Related

- 00041101
- 00041111

00041111

Meaning
An administrator deleted a group of customized suspicious URL definitions.

Field name	Description
ID (`log_id`)	00041111 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:35:49 log_id=00041111 msg_id=000000000153 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-susp-url suspicious-url1 from GUI(172.20.120.47)"

Related

- 00041101
- 00041102

00041201

Meaning
An administrator created a customized suspicious URL definition (“rule”).

Field name	Description
ID (`log_id`)	00041201 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:36:50 log_id=00041201 msg_id=000000000157 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy pattern suspicious-url-rule custom-suspicious-urls from GUI (172.20.120.47)"

Related

- 00041202
- 00041211

00041202

Meaning
An administrator changed a customized suspicious URL definition.

Field name	Description
ID (`log_id`)	00041202 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:36:50 log_id=00041202 msg_id=000000000158 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy pattern suspicious-url-rule custom-suspicious-urls from GUI (172.20.120.47)"

Related

- 00041201
- 00041211

00041211

Meaning
An administrator deleted a customized suspicious URL definition.

Field name	Description
ID (`log_id`)	00041211 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:36:50 log_id=00041211 msg_id=000000000158 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy pattern suspicious-url-rule custom-suspicious-urls from GUI (172.20.120.47)"

Related

- 00041201
- 00041202

00041302

Meaning
An administrator disabled or enabled either: • a predefined global allow list object or • a definition of a known search engine crawler.

Field name	Description
ID (`log_id`)	00041302 See Log ID numbers on page 24.

Examples
date=2014-01-08 time=17:39:20 log_id=00041302 msg_id=000000004887 device_id=FV-3KC3R09700002 vd="adom_auto" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed the Global allow list"
date=2013-10-08 time=10:22:50 log_id=00041302 msg_id=000000000136 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=notification trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed the Global known Engines"

00041401

Meaning
An administrator created an allowed/protected `Host:` definition.

Field name	Description
ID (`log_id`)	00041401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:12:46 log_id=00041401 msg_id=000000000101 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added Protected Hostnames example_co_jp from GUI(172.20.120.47)"

Related

- 00041402
- 00041411

00041402

Meaning
An administrator changed an allowed/protected `Host:` definition.

Field name	Description
ID (`log_id`)	00041402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:12:52 log_id=00041402 msg_id=000000000102 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed Protected Hostnames example_com from GUI(172.20.120.47)"

Related

- 00041401
- 00041411

00041411

Meaning
An administrator deleted an allowed/protected `Host:` definition.

Field name	Description
ID (`log_id`)	00041411 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:01:30 log_id=00041411 msg_id=000000000637 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted Protected Hostnames example_co_uk from GUI(192.168.1.28)"

Related

- 00041401
- 00041402

00041601

Meaning
An administrator created an interpreter to locate parameters in a dynamic URL (“URL replacer”) when using auto-learning.

Field name	Description
ID (`log_id`)	00041601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:34:46 log_id=00041601 msg_id=000000000148 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy custom-application url-replace url-interpreter1 from GUI (172.20.120.47)"

Related

- 00041602
- 00041611

00041602

Meaning
An administrator changed a URL replacer.

Field name	Description
ID (`log_id`)	00041602 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:31:58 log_id=00041602 msg_id=000000000645 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy custom-application url-replace url-interpreter1 from GUI (192.168.1.28)"

Related

- 00041601
- 00041611

00041611

Meaning
An administrator deleted a URL replacer.

Field name	Description
ID (`log_id`)	00041611 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:33:21 log_id=00041611 msg_id=000000000147 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy custom-application url-replace url-interpreter1 from GUI (172.20.120.47)"

Related

- 00041601
- 00041602

00041801

Meaning
An administrator created a group of URL replacers (“application policy”).

Field name	Description
ID (`log_id`)	00041801 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:32:24 log_id=00041801 msg_id=000000000647 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-policy custom-application application-policy url-interpreter-group1 from GUI(192.168.1.28)"

Related

- 00041802
- 00041811

00041802

Meaning
An administrator changed a group of URL replacers (“application policy”).

Field name	Description
ID (`log_id`)	00041802 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:32:29 log_id=00041802 msg_id=000000000648 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-policy custom-application application-policy url-interpreter-group1 from GUI(192.168.1.28)"

Related

- 00041801
- 00041811

00041811

Meaning
An administrator deleted a group of URL replacers (“application policy”).

Field name	Description
ID (`log_id`)	00042401 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:32:39 log_id=00041811 msg_id=000000000649 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted server-policy custom-application application-policy url-interpreter-group1 from GUI(192.168.1.28)"

Related

- 00041801
- 00041802

00042401

Meaning
An administrator added a server pool.

Field name	Description
ID (`log_id`)	00042401 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:24:28 log_id=00042401 msg_id=001248141062 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added server-pool new-add-server-pool from GUI(172.22.6.1)"

Related

- 00042402
- 00042411

00042402

Meaning
An administrator edited a server pool.

Field name	Description
ID (`log_id`)	00042402 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:19:46 log_id=00042402 msg_id=001248141059 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed server-pool ContentRoutingTest-Server-pool--1 from GUI(172.22.6.1)"

Related

- 00042401
- 00042411

00042411

Meaning
An administrator deleted a server pool.

Field name	Description
ID (`log_id`)	00042411 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:27:42 log_id=00042411 msg_id=001248141064 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted server-pool new-add-server-pool from GUI(172.22.6.1)"

Related

- 00042401
- 00042402

00043001

Meaning
An administrator created a server policy.

Field name	Description
ID (`log_id`)	00043001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:20:37 log_id=00043001 msg_id=000000000128 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added policy policy2 from GUI(172.20.120.47)"

Related

- 00043011
- 00043002

00043002

Meaning
An administrator changed a server policy.

Field name	Description
ID (`log_id`)	00043002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:20:04 log_id=00043002 msg_id=000000000125 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed policy policy1 from GUI(172.20.120.47)"

Related

- 00043001
- 00043011

00043011

Meaning
An administrator deleted a server policy.

Field name	Description
ID (`log_id`)	00043011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:20:49 log_id=00043011 msg_id=000000000130 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted policy policy2 from GUI(172.20.120.47)"

Related

- 00043001
- 00043002

00044001

Meaning
An administrator added a site publishing policy rule.

Field name	Description
ID (`log_id`)	00044001 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:24:11 log_id=00044001 msg_id=000000179495 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added site-published-helper autotest.FortiWeb.com from GUI(172.22.6.66)"

Related

- 00044002
- 00044011
- 00044401
- 00044411

00044002

Meaning
An administrator edited a site publishing policy rule.

Field name	Description
ID (`log_id`)	00044002 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:30:16 log_id=00044002 msg_id=000000179501 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed site-published-helper autotest1.FortiWeb.com from GUI(172.22.6.66)"

Related

- 00044001
- 00044011
- 00044401
- 00044411

00044011

Meaning
An administrator deleted a site publishing policy rule.

Field name	Description
ID (`log_id`)	00044011 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:31:41 log_id=00044011 msg_id=000000179502 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted site-published-helper autotest1.FortiWeb.com from GUI(172.22.6.66)"

Related

- 00044001
- 00044002
- 00044401
- 00044411

00044401

Meaning
An administrator added a site publishing policy.

Field name	Description
ID (`log_id`)	00044401 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:32:28 log_id=00044401 msg_id=000000179503 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added site-published-helper-policy dd from GUI(172.22.6.66)"

Related

- 00044411
- 00044001
- 00044002
- 00044011

00044411

Meaning
An administrator deleted a site publishing policy.

Field name	Description
ID (`log_id`)	00044411 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:38:07 log_id=00044411 msg_id=000000179507 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted site-published-helper-policy dd from GUI(172.22.6.66)"

Related

- 00044401
- 00044001
- 00044002
- 00044011

00044501

Meaning
An administrator added a custom global allowlist item.

Field name	Description
ID (`log_id`)	00044501 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=15:03:01 log_id=00044501 msg_id=000000055170 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-global-whilte-list-group 1 from GUI(172.22.6.149)"

Related

- 00044502
- 00044511

00044502

Meaning
An administrator edited a custom global allowlist item.

Field name	Description
ID (`log_id`)	00044502 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=15:03:26 log_id=00044502 msg_id=000000055171 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-global-whilte-list-group 1 from GUI(172.22.6.149)"

Related

- 00044501
- 00044511

00044511

Meaning
An administrator deleted a custom global allowlist item.

Field name	Description
ID (`log_id`)	00044511 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=15:03:40 log_id=00044511 msg_id=000000055172 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-global-whilte-list-group 1 from GUI(172.22.6.149)"

Related

- 00044501
- 00044502

00046001

Meaning
An administrator created a session persistence configuration.

Field name	Description
ID (`log_id`)	00046001 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=10:47:27 log_id=00046001 msg_id=000000003145 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added persistence-policy persistent_ip from GUI(172.20.120.61)"

Related

- 00046002
- 00046011

00046002

Meaning
An administrator edited a session persistence configuration.

Field name	Description
ID (`log_id`)	00046002 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=10:56:36 log_id=00046002 msg_id=000000003146 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed persistence-policy persistent_ip from GUI(172.20.120.61)"

Related

- 00046001
- 00046011

00046011

Meaning
An administrator deleted a session persistence configuration.

Field name	Description
ID (`log_id`)	00046011 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=10:56:56 log_id=00046011 msg_id=000000003147 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted persistence-policy persistent_ip from GUI(172.20.120.61)"

Related

- 00046001
- 00046002

00050001

Meaning
An administrator created a compression exemption.

Field name	Description
ID (`log_id`)	00050001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:55:44 log_id=00050001 msg_id=000000000240 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added exclude-url gzip-exempt1 from GUI(172.20.120.47)"

Related

- 00050002
- 00050011

00050002

Meaning
An administrator changed a compression exemption.

Field name	Description
ID (`log_id`)	00050002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:55:55 log_id=00050002 msg_id=000000000241 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed exclude-url gzip-exempt1 from GUI(172.20.120.47)"

Related

- 00050001
- 00050011

00050011

Meaning
An administrator deleted a compression exemption.

Field name	Description
ID (`log_id`)	00050011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:55 log_id=00050011 msg_id=000000000242 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted exclude-url gzip-exempt1 from GUI(172.20.120.47)"

Related

- 00050001
- 00050002

00050201

Meaning
An administrator created a decompressor.

Field name	Description
ID (`log_id`)	00050201 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:11 log_id=00050201 msg_id=000000000243 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-uncompress-rule decompressor1 from GUI(172.20.120.47)"

Related

- 00050202
- 00050211

00050202

Meaning
An administrator changed a decompressor.

Field name	Description
ID (`log_id`)	00050202 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:23 log_id=00050202 msg_id=000000000244 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-uncompress-rule decompressor1 from GUI(172.20.120.47)"

Related

- 00050201
- 00050211

00050211

Meaning
An administrator deleted a decompressor.

Field name	Description
ID (`log_id`)	00050211 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:43 log_id=00050211 msg_id=000000000245 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin dleleted file-uncompress-rule decompressor1 from GUI(172.20.120.47)"

Related

- 00050201
- 00050202

00050401

Meaning
An administrator created a compressor.

Field name	Description
ID (`log_id`)	00050401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:34 log_id=00050401 msg_id=000000000245 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-compress-rule compressor1 from GUI(172.20.120.47)"

Related

- 00050402
- 00050411

00050402

Meaning
An administrator changed a compressor.

Field name	Description
ID (`log_id`)	00050402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:46 log_id=00050402 msg_id=000000000246 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-compress-rule compressor1 from GUI(172.20.120.47)"

Related

- 00050401
- 00050411

00050411

Meaning
An administrator deleted a compressor.

Field name	Description
ID (`log_id`)	00050411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:56:56 log_id=00050411 msg_id=000000000247 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted file-compress-rule compressor1 from GUI(172.20.120.47)"

Related

- 00050401
- 00050402

00051001

Meaning
An administrator created an HTTP flood prevention rule.

Field name	Description
ID (`log_id`)	00051001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:40:19 log_id=00051001 msg_id=000000000175 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added HTTP-request-flood-prevention-rule HTTP-flood-ip1 from GUI(172.20.120.47)"

Related

- 00051002
- 00051011

00051002

Meaning
An administrator changed an HTTP flood prevention rule.

Field name	Description
ID (`log_id`)	00051002 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:36:04 log_id=00051002 msg_id=000000000418 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-request-flood-prevention-rule HTTP-flood-ip1 from GUI (172.20.120.47)"

Related

- 00051001
- 00051011

00051011

Meaning
An administrator deleted an HTTP flood prevention rule.

Field name	Description
ID (`log_id`)	00051011 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:36:24 log_id=00051011 msg_id=000000000419 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted HTTP-request-flood-prevention-rule HTTP-flood-ip1 from GUI(172.20.120.47)"

Related

- 00051001
- 00051002

00051201

Meaning
An administrator created a malicious IPs rule.

Field name	Description
ID (`log_id`)	00051201 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:40:35 log_id=00051201 msg_id=000000000176 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added HTTP-connection-flood-check-rule dos-ip1 from GUI(172.20.120.47)"

Related

- 00051202
- 00051211

00051202

Meaning
An administrator changed a malicious IPs rule.

Field name	Description
ID (`log_id`)	00051202 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:36:13 log_id=00051202 msg_id=000000000419 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-connection-flood-check-rule dos-ip1 from GUI(172.20.120.47)"

Relate

- 00051201
- 00051211

00051211

Meaning
An administrator deleted a malicious IPs rule.

Field name	Description
ID (`log_id`)	00051211 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:36:23 log_id=00051211 msg_id=000000000420 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted HTTP-connection-flood-check-rule dos-ip1 from GUI(172.20.120.47)"

Related

- 00051201
- 00051202

00051401

Meaning
An administrator created a HTTP access limit rule.

Field name	Description
ID (`log_id`)	00051401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:40:35 log_id=00051401 msg_id=000000000176 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added layer4-access-limit-rule dos-ip1 from GUI(172.20.120.47)"

Related

- 00051402
- 00051411

00051402

Meaning
An administrator changed a HTTP access limit rule.

Field name	Description
ID (`log_id`)	00051402 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:36:13 log_id=00051402 msg_id=000000000419 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed layer4-access-limit-rule dos-ip1 from GUI(172.20.120.47)"

Related

- 00051401
- 00051411

00051411

Meaning
An administrator deleted a HTTP access limit rule.

Field name	Description
ID (`log_id`)	00051411 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:36:23 log_id=00051411 msg_id=000000000420 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted layer4-access-limit-rule dos-ip1 from GUI(172.20.120.47)"

Related

- 00051401
- 00051402

00051601

Meaning
An administrator created a TCP flood prevention rule.

Field name	Description
ID (`log_id`)	00051601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:41:36 log_id=00051601 msg_id=000000000178 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-layer4-connection-flood-check-rule tcp-flood-preventer1 from GUI (172.20.120.47)"

Related

- 00051602
- 00051611

00051602

Meaning
An administrator changed a TCP flood prevention rule.

Field name	Description
ID (`log_id`)	00051602 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:35:51 log_id=00051602 msg_id=000000000417 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-layer4-connection-flood-check-rule tcp-flood-preventer1 from GUI (172.20.120.47)"

Related

- 00051601
- 00051611

00051611

Meaning
An administrator deleted a TCP flood prevention rule.

Field name	Description
ID (`log_id`)	00051611 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:35:59 log_id=00051611 msg_id=000000000418 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin changed waf-layer4-connection-flood-check-rule tcp-flood-preventer1 from GUI (172.20.120.47)"

Related

- 00051601
- 00051602

00051801

Meaning
An administrator created a DoS protection policy.

Field name	Description
ID (`log_id`)	00051801 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:38:42 log_id=00051801 msg_id=000000000173 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added DoS protection policy dos-protection1 from GUI(172.20.120.47)"

Related

- 00051802
- 00051811

00051802

Meaning
An administrator changed a DoS protection policy.

Field name	Description
ID (`log_id`)	00051802 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:41:46 log_id=00051802 msg_id=000000000179 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed DoS protection policy dos-protection1 from GUI(172.20.120.47)"

Related

- 00051801
- 00051811

00051811

Meaning
An administrator deleted a DoS protection policy.

Field name	Description
ID (`log_id`)	00051811 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:41:56 log_id=00051811 msg_id=000000000180 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted DoS protection policy dos-protection1 from GUI(172.20.120.47)"

Related

- 00051801
- 00051802

00052201

Meaning
An administrator created a client IP allow list or block list.

Field name	Description
ID (`log_id`)	00052201 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=09:57:02 log_id=00052201 msg_id=000000000460 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf ip-list blocklist from GUI(172.20.120.47)"

Related

- 00052202
- 00052211

00052202

Meaning
An administrator changed a client IP allow list or block list.

Field name	Description
ID (`log_id`)	00052202 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=09:57:12 log_id=00052202 msg_id=000000000461 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf ip-list blocklist from GUI(172.20.120.47)"

Related

- 00052201
- 00052211

00052211

Meaning
An administrator deleted a client IP allow list or block list.

Field name	Description
ID (`log_id`)	00052211 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=09:57:22 log_id=00052211 msg_id=000000000462 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf ip-list blocklist from GUI(172.20.120.47)"

Related

- 00052201
- 00052202

00052401

Meaning
An administrator created a user authentication rule.

Field name	Description
ID (`log_id`)	00040002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:14:20 log_id=00040002 msg_id=000000000106 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed health uptime-check1 from GUI(172.20.120.47)"

Related

- 00052402
- 00052411

00052402

Meaning
An administrator changed a user authentication rule.

Field name	Description
ID (`log_id`)	00052402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:57:33 log_id=00052402 msg_id=000000000255 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-authen-rule user-auth-realms1 from GUI(172.20.120.47)"

Related

- 00052401
- 00052411

00052411

Meaning
An administrator deleted a user authentication rule.

Field name	Description
ID (`log_id`)	00052411 See Log ID numbers on page 24.

Examples
date=2013-10-09 time=16:15:22 log_id=00052411 msg_id=000000000316 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted HTTP-authen-rule user-auth-realms1 from GUI(172.20.120.47)"

Related

- 00052401
- 00052402

00052601

Meaning
An administrator created a user authentication policy.

Field name	Description
ID (`log_id`)	00052601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:57:59 log_id=00052601 msg_id=000000000257 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added HTTP-authen-policy user-auth-policy1 from GUI(172.20.120.47)"

Related

- 00052602
- 00052611

00052602

Meaning
An administrator changed a user authentication policy.

Field name	Description
ID (`log_id`)	00052602 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:58:02 log_id=00052602 msg_id=000000000258 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-authen-policy user-auth-policy1 from GUI(172.20.120.47)"

Related

- 00052601
- 00052611

00052611

Meaning
An administrator deleted a user authentication policy.

Field name	Description
ID (`log_id`)	00052611 See Log ID numbers on page 24.

Examples
date=2013-10-09 time=16:15:17 log_id=00052611 msg_id=000000000315 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted HTTP-authen-policy user-auth-connections-temp from GUI(172.20.120.47)"

Related

- 00052601
- 00052602

00053201

Meaning
An administrator added an input rule for HTTP requests.

Field name	Description
ID (`log_id`)	00053201 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:50:46 log_id=00053201 msg_id=000000734635 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added input-rule ddddd from GUI(172.22.6.237)"

Related

- 00053202
- 00053211

00053202

Meaning
An administrator edited an input rule for HTTP requests.

Field name	Description
ID (`log_id`)	00053202 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:54:39 log_id=00053202 msg_id=000000734636 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed input-rule ddddd from GUI(172.22.6.237)"

Related

- 00053201
- 00053211

00053211

Meaning
An administrator deleted an input rule for HTTP requests.

Field name	Description
ID (`log_id`)	00053211 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:56:42 log_id=00053211 msg_id=000000734637 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted input-rule ddddd from GUI(172.22.6.237)"

Related

- 00053201
- 00053202

00053701

Meaning
An administrator added a parameter validation rule.

Field name	Description
ID (`log_id`)	00053701 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:41:56 log_id=00053701 msg_id=000000734632 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added parameter-validation-rule 123 from GUI(172.22.6.237)"

Related

- 00053711

00053711

Meaning
An administrator deleted a parameter validation rule.

Field name	Description
ID (`log_id`)	00053711 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:49:47 log_id=00053711 msg_id=000000734634 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted parameter-validation-rule 123 from GUI(172.22.6.237)"

Related

- 00053701

00053901

Meaning
An administrator created a hidden input rule.

Field name	Description
ID (`log_id`)	00053901 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:51:19 log_id=00053901 msg_id=000000000218 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added hidden-fields-rule hidden-input-rule1 from GUI(172.20.120.47)"

Related

- 00053902
- 00053911

00053902

Meaning
An administrator changed a hidden input rule.

Field name	Description
ID (`log_id`)	00053902 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:51:25 log_id=00053902 msg_id=000000000219 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hidden-fields-rule hidden-input-rule1 from GUI(172.20.120.47)"

Related

- 00053901
- 00053911

00053911

Meaning
An administrator deleted a hidden input rule.

Field name	Description
ID (`log_id`)	00053911 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:51:35 log_id=00053911 msg_id=000000000220 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted hidden-fields-rule hidden-input-rule1 from GUI(172.20.120.47)"

Related

- 00053901
- 00053902

00054401

Meaning
An administrator created a hidden input policy.

Field name	Description
ID (`log_id`)	00054401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:52:11 log_id=00054401 msg_id=000000000222 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added hidden-fields-protection hidden-input-policy1 from GUI(172.20.120.47)"

Related

- 00054402
- 00054411

00054402

Meaning
An administrator changed a hidden input policy.

Field name	Description
ID (`log_id`)	00054402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:52:16 log_id=00054402 msg_id=000000000223 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed hidden-fields-protection hidden-input-policy1 from GUI(172.20.120.47)"

Related

- 00054401
- 00054411

00054411

Meaning
An administrator deleted a hidden input policy.

Field name	Description
ID (`log_id`)	00054411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:52:26 log_id=00054411 msg_id=000000000224 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted hidden-fields-protection hidden-input-policy1 from GUI(172.20.120.47)"

Related

- 00054401
- 00054402

00054601

Meaning
An administrator created a page order rule.

Field name	Description
ID (`log_id`)	00054601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:44:40 log_id=00054601 msg_id=000000000191 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added page-access-rule page-order1 from GUI(172.20.120.47)"

Related

- 00054602
- 00054611

00054602

Meaning
An administrator changed a page order rule.

Field name	Description
ID (`log_id`)	00054602 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:44:49 log_id=00054602 msg_id=000000000192 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed page-access-rule page-order1 from GUI(172.20.120.47)"

Related

- 00054601
- 00054611

00054611

Meaning
An administrator deleted a page order rule.

Field name	Description
ID (`log_id`)	00054611 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:44:49 log_id=00054611 msg_id=000000000193 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted page-access-rule page-order1 from GUI(172.20.120.47)"

Related

- 00054601
- 00054602

00054801

Meaning
An administrator created a rewrite/redirect rule.

Field name	Description
ID (`log_id`)	00054801 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=11:07:40 log_id=00054801 msg_id=000000000263 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added url-rewrite-rule HTTP-to-HTTPs-redirect from GUI(172.20.120.47)"

Related

- 00054802
- 00054811

00054802

Meaning
An administrator changed a rewrite/redirect rule.

Field name	Description
ID (`log_id`)	00054802 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=11:07:55 log_id=00054802 msg_id=000000000264 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-rewrite-rule HTTP-to-HTTPs-redirect from GUI(172.20.120.47)"

Related

- 00054801
- 00054811

00054811

Meaning
An administrator deleted a rewrite/redirect rule.

Field name	Description
ID (`log_id`)	00054811 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=11:08:55 log_id=00054811 msg_id=000000000265 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-rewrite-rule HTTP-to-HTTPs-redirect from GUI(172.20.120.47)"

Related

- 00054801
- 00054802

00055301

Meaning
An administrator created a rewrite/redirect policy.

Field name	Description
ID (`log_id`)	00055301 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=11:09:10 log_id=00055301 msg_id=000000000268 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added url-rewrite-policy request-rewrites1 from GUI(172.20.120.47)"

Related

- 00055302
- 00055311

00055302

Meaning
An administrator changed a rewrite/redirect policy.

Field name	Description
ID (`log_id`)	00055302 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=11:09:14 log_id=00055302 msg_id=000000000269 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-rewrite-policy request-rewrites1 from GUI(172.20.120.47)"

Related

- 00055301
- 00055311

00055311

Meaning
An administrator deleted a rewrite/redirect policy.

Field name	Description
ID (`log_id`)	00055311 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=11:09:34 log_id=00055311 msg_id=000000000270 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-rewrite-policy request-rewrites1 from GUI(172.20.120.47)"

Related

- 00055301
- 00055302

00055501

Meaning
An administrator created an allowed HTTP method exception.

Field name	Description
ID (`log_id`)	00055501 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:42:10 log_id=00055501 msg_id=000000000180 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added allow-method-exceptions method-exempt1 from GUI(172.20.120.47)"

Related

- 00055502
- 00055511

00055502

Meaning
An administrator changed an allowed HTTP method exception.

Field name	Description
ID (`log_id`)	00055502 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:42:33 log_id=00055502 msg_id=000000000181 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed allow-method-exceptions method-exempt1 from GUI(172.20.120.47)"

Related

- 00055501
- 00055511

00055511

Meaning
An administrator deleted an allowed HTTP method exception.

Field name	Description
ID (`log_id`)	00055511 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:42:43 log_id=00055511 msg_id=000000000182 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted allow-method-exceptions method-exempt1 from GUI(172.20.120.47)"

Related

- 00055501
- 00055502

00055701

Meaning
An administrator created an allowed HTTP method.

Field name	Description
ID (`log_id`)	00055701 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:43:04 log_id=00055701 msg_id=000000000183 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added allow-method-policy allowed-methods1 from GUI(172.20.120.47)"

Related

- 00055702
- 00055711

00055702

Meaning
An administrator changed an allowed HTTP method.

Field name	Description
ID (`log_id`)	00055702 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:43:14 log_id=00055702 msg_id=000000000184 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed allow-method-policy allowed-methods1 from GUI(172.20.120.47)"

Related

- 00055701
- 00055711

00055711

Meaning
An administrator deleted an allowed HTTP method.

Field name	Description
ID (`log_id`)	00055711 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:43:24 log_id=00055711 msg_id=000000000185 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted allow-method-policy allowed-methods1 from GUI(172.20.120.47)"

Related

- 00055701
- 00055702

00055901

Meaning
A FortiWeb administrator generated a URL access rule by importing a scanner report file.

Field name	Description
ID (`log_id`)	00055901 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:28 log_id=00055901 msg_id=000011519548 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added url-access-rule e-9 from scanner_integration"

Related

- 00055971
- 00056401
- 00056402
- 00056421
- 00066151
- 00066601
- 00066921
- 08999999

00055902

Meaning
An administrator changed an access control rule.

Field name	Description
ID (`log_id`)	00055902 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:46:12 log_id=00055902 msg_id=000000000197 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed url-access-rule access-control1 from GUI(172.20.120.47)"

Related

- 00055901
- 00055911

00055911

Meaning
An administrator deleted an access control rule.

Field name	Description
ID (`log_id`)	00055911 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:46:22 log_id=00055911 msg_id=000000000198 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-access-rule access-control1 from GUI(172.20.120.47)"

Related

- 00055901
- 00055902

00055971

Meaning
A FortiWeb administrator generated a URL access condition in a URL access rule by importing a scanner report file.

Field name	Description
ID (`log_id`)	00055971 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:28 log_id=00055971 msg_id=000011519555 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added url-access-rule e-10 match-condition 1 from scanner_integration"

Related

- 00055901
- 00056401
- 00056402
- 00056421
- 00066151
- 00066601
- 00066921
- 08999999

00056401

Meaning
A FortiWeb administrator generated a URL access policy by importing a scanner report file.

Field name	Description
ID (`log_id`)	00056401 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:28 log_id=00056401 msg_id=000011519546 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added url-access-policy e from scanner_integration"

Related

- 00055901
- 00055971
- 00056402
- 00056421
- 00066151
- 00066601
- 00066921
- 08999999

00056402

Meaning
A FortiWeb administrator changed an inline protection profile by importing a scanner report file.

Field name	Description
ID (`log_id`)	00056402 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:28 log_id=00062402 msg_id=000011519544 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=edit status=success msg="User daemon_admin changed inline-protection e from scanner_integration"

Related

- 00055901
- 00055971
- 00056401
- 00056421
- 00066151
- 00066601
- 00066921
- 08999999

00056411

Meaning
An administrator deleted an access control policy.

Field name	Description
ID (`log_id`)	00056411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:47:14 log_id=00056411 msg_id=000000000203 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted url-access-policy access-control-group1 from GUI(172.20.120.47)"

Related

- 00056401
- 00056402

00056421

Meaning
A FortiWeb administrator generated a URL access rule by importing a scanner report file.

Field name	Description
ID (`log_id`)	00056421 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:28 log_id=00056421 msg_id=000011519556 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added url-access-policy e rule 2 from scanner_integration"

Related

- 00055901
- 00055971
- 00056401
- 00056402
- 00066151
- 00066601
- 00066921
- 08999999

00056601

Meaning
An administrator created an HTTP constraint.

Field name	Description
ID (`log_id`)	00056601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:48:21 log_id=00056601 msg_id=000000000207 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added HTTP-protocol-parameter-restriction HTTP-contraints1 from GUI (172.20.120.47)"

Related

- 00056602
- 00056611

00056602

Meaning
An administrator changed an HTTP constraint.

Field name	Description
ID (`log_id`)	00056602 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=10:17:50 log_id=00056602 msg_id=000000000482 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-protocol-parameter-restriction HTTP-contraints1 from GUI (172.20.120.47)"

Related

- 00056601
- 00056611

00056611

Meaning
An administrator deleted an HTTP constraint.

Field name	Description
ID (`log_id`)	00056611 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=10:17:59log_id=00056611 msg_id=000000000483 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted HTTP-protocol-parameter-restriction HTTP-contraints1 from GUI (172.20.120.47)"

Related

- 00056601
- 00056602

00058601

Meaning
An administrator created an HTTP constraint exemption.

Field name	Description
ID (`log_id`)	00058601 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:47:28 log_id=00058601 msg_id=000000000204 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added HTTP-constraints-exception HTTP-contraints-exempt1 from GUI (172.20.120.47)"

Related

- 00058602
- 00058611

00058602

Meaning
An administrator changed an HTTP constraint exemption.

Field name	Description
ID (`log_id`)	00058602 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:47:51 log_id=00058602 msg_id=000000000205 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-constraints-exception HTTP-contraints-exempt1 from GUI (172.20.120.47)"

Related

- 00058601
- 00058611

00058611

Meaning
An administrator deleted an HTTP constraint exemption.

Field name	Description
ID (`log_id`)	00058611 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:48:51 log_id=00058611 msg_id=000000000206 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted HTTP-constraints-exception HTTP-contraints-exempt1 from GUI (172.20.120.47)"

Related

- 00058601
- 00058602

00058621

Meaning
A FortiWeb administrator added a rule to an HTTP protocol constraint exception.

Field name	Description
ID (`log_id`)	00058621 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:49:15 log_id=00058621 msg_id=000000004646 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added HTTP-constraints-exception hello HTTP_constraints-exception-list 2 from GUI (172.22.6.149)"

Related

- 00058622
- 00058631

00058622

Meaning
A FortiWeb administrator edited a rule in an HTTP protocol constraint exception.

Field name	Description
ID (`log_id`)	00058622 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:53:37 log_id=00058622 msg_id=000000004649 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed HTTP-constraints-exception 1w1w HTTP_constraints-exception-list 2 from GUI(172.22.6.149)"

Related

- 00058621
- 00058631

00058631

Meaning
A FortiWeb administrator deleted a rule in an HTTP protocol constraint exception.

Field name	Description
ID (`log_id`)	00058631 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=17:10:08 log_id=00058631 msg_id=000000004654 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted HTTP-constraints-exception 1w1w HTTP_constraints-exception-list 2 from GUI(172.22.6.149)"

Related

- 00058621
- 00058622

00059801

Meaning
An administrator created a custom signature.

Field name	Description
ID (`log_id`)	00059801 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:54:06 log_id=00059801 msg_id=000000000232 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-protection-rule custom-signature1 from GUI(172.20.120.47)"

Related

- 00059802
- 00059811

00059802

Meaning
An administrator changed a custom signature.

Field name	Description
ID (`log_id`)	00059802 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:54:22 log_id=00059802 msg_id=000000000233 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-protection-rule custom-signature1 from GUI(172.20.120.47)"

Related

- 00059801
- 00059811

00059811

Meaning
An administrator deleted a custom signature.

Field name	Description
ID (`log_id`)	00059811 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:55:25 log_id=00059811 msg_id=000000000239 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-protection-rule custom-signature2 from GUI(172.20.120.47)"

Related

- 00059801
- 00059802

00060001

Meaning
An administrator created a group of custom signatures.

Field name	Description
ID (`log_id`)	00060001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:54:46 log_id=00060001 msg_id=000000000235 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-protection-group custom-signatures1 from GUI(172.20.120.47)"

Related

- 00060002
- 00060011

00060002

Meaning
An administrator changed a group of custom signatures.

Field name	Description
ID (`log_id`)	00060002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:54:51 log_id=00060002 msg_id=000000000236 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-protection-group custom-signatures1 from GUI(172.20.120.47)"

Related

- 00060001
- 00060011

00060011

Meaning
An administrator deleted a group of custom signatures.

Field name	Description
ID (`log_id`)	00060011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:55:51 log_id=00060011 msg_id=000000000237 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=delstatus=success msg="User admin deleted custom-protection-group custom-signatures1 from GUI(172.20.120.47)"

Related

- 00060001
- 00060002

00060201

Meaning
An administrator created an attack signatures rule.

Field name	Description
ID (`log_id`)	00060201 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=21:58:28 log_id=00060201 msg_id=000000000762 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added signature attack-signatures2 from GUI(192.168.1.28)"

Related

- 00060202
- 00060211

00060202

Meaning
An administrator changed an attack signatures rule.

Field name	Description
ID (`log_id`)	00060202 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=21:47:39 log_id=00060202 msg_id=000000000759 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed signature attack-signatures1 from GUI(192.168.1.28)"

Related

- 00060201
- 00060211

00060211

Meaning
An administrator deleted an attack signatures rule.

Field name	Description
ID (`log_id`)	00060211 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=21:58:46 log_id=00060211 msg_id=000000000763 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted signature attack-signatures2 from GUI(192.168.1.28)"

Related

- 00060201
- 00060202

00061201

Meaning
An administrator created an `X-Forwarded-For:` rule.

Field name	Description
ID (`log_id`)	00061201 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:04:30 log_id=00061201 msg_id=000000000764 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added x-forwarded-for xff1 from GUI(192.168.1.28)"

Related

- 00061202
- 00061211

00061202

Meaning
An administrator changed an `X-Forwarded-For:` rule.

Field name	Description
ID (`log_id`)	00061202 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:04:35 log_id=00061202 msg_id=000000000765 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed x-forwarded-for xff1 from GUI(192.168.1.28)"

Related

- 00061201
- 00061211

00061211

Meaning
An administrator deleted an `X-Forwarded-For:` rule.

Field name	Description
ID (`log_id`)	00061211 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:04:44 log_id=00061211 msg_id=000000000766 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted x-forwarded-for xff1 from GUI(192.168.1.28)"

Related

- 00061201
- 00061202

00061401

Meaning
An administrator created a session initiation rule (“start page rule”).

Field name	Description
ID (`log_id`)	00061401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:43:33 log_id=00061401 msg_id=000000000184 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added start-pages session-init-page1 from GUI(172.20.120.47)"

Related

- 00061402
- 00061411

00061402

Meaning
An administrator changed a session initiation rule (“start page rule”).

Field name	Description
ID (`log_id`)	00061402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:43:46 log_id=00061402 msg_id=000000000185 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed start-pages session-init-page1 from GUI(172.20.120.47)"

Related

- 00061401
- 00061411

00061411

Meaning
An administrator deleted a session initiation rule (“start page rule”).

Field name	Description
ID (`log_id`)	00061411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:43:56 log_id=00061411 msg_id=000000000186 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted start-pages session-init-page1 from GUI(172.20.120.47)"

Related

- 00061401
- 00061402

00061801

Meaning
An administrator has added a brute force login attack profile.

Field name	Description
ID (`log_id`)	00061801 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=10:38:38 log_id=00061801 msg_id=000000055127 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-brute-force-login dwg from GUI(172.22.6.149)"

Related

- 00061802
- 00061811

00061802

Meaning
An administrator edited a brute force login attack profile.

Field name	Description
ID (`log_id`)	00061802 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:15:21 log_id=00061802 msg_id=000000055128 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-brute-force-login dwg from GUI(172.22.6.149)"

Related

- 00061801
- 00061811

00061811

Meaning
An administrator has edited a brute force login attack profile.

Field name	Description
ID (`log_id`)	00061811 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=11:15:47 log_id=00061811 msg_id=000000055129 device_id=FV-4KC3R11700001 vd="root" timezone="(GMT+7:00)Krasnoyarsk" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-brute-force-login dwg from GUI(172.22.6.149)"

Related

- 00061801
- 00061802

00062001

Meaning
An administrator created an upload restriction rule.

Field name	Description
ID (`log_id`)	00062001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:49:10 log_id=00062001 msg_id=000000000208 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-upload-restriction-rule video-uploads-limit1 from GUI(172.20.120.47)"

Related

- 00062002
- 00062011

00062002

Meaning
An administrator changed an upload restriction rule.

Field name	Description
ID (`log_id`)	00062002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:49:49 log_id=00062002 msg_id=000000000209 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-upload-restriction-rule video-uploads-limit1 from GUI(172.20.120.47)"

Related

- 00062001
- 00062011

00062011

Meaning
An administrator deleted an upload restriction rule.

Field name	Description
ID (`log_id`)	00062011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:49:59 log_id=00062011 msg_id=000000000210 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted file-upload-restriction-rule video-uploads-limit1 from GUI(172.20.120.47)"

Related

- 00062001
- 00062002

00062201

Meaning
An administrator created an upload restriction policy.

Field name	Description
ID (`log_id`)	00062201 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:27:13 log_id=00062201 msg_id=000000000770 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-file-upload-restriction-policy all-file-uploads1 from GUI(192.168.1.28)"

Related

- 00062202
- 00062011

00062202

Meaning
An administrator changed an upload restriction policy.

Field name	Description
ID (`log_id`)	00062202 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:27:24 log_id=00062202 msg_id=000000000772 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-file-upload-restriction-policy all-file-uploads1 from GUI(192.168.1.28)"

Related

- 00062201
- 00062211

00062211

Meaning
An administrator deleted an upload restriction policy.

Field name	Description
ID (`log_id`)	00062211 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:27:32 log_id=00062211 msg_id=000000000773 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-file-upload-restriction-policy file-uploads from GUI(192.168.1.28)"

Related

- 00062201
- 00062202

00062401

Meaning
An administrator created an inline protection profile.

Field name	Description
ID (`log_id`)	00062401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:09:59 log_id=00062401 msg_id=000000000088 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added inline-protection inline-protection-profile1 from GUI(172.20.120.47)"

Related

- 00062402
- 00062411

00062402

Meaning
An administrator changed an inline protection profile.

Field name	Description
ID (`log_id`)	00062402 See Log ID numbers on page 24.

Examples
date=2013-10-10 time=00:32:06 log_id=00062402 msg_id=000000000377 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed inline-protection inline-protection-profile1 from GUI(172.20.120.47)"

Related

- 00062401
- 00062411

00062411

Meaning
An administrator deleted an inline protection profile.

Field name	Description
ID (`log_id`)	00062411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:18:34 log_id=00062411 msg_id=000000000118 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted inline-protection temp from GUI(172.20.120.47)"

Related

- 00062401
- 00062402

00063401

Meaning
An administrator created an Offline Protection profile.

Field name	Description
ID (`log_id`)	00063401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:18:44 log_id=00063401 msg_id=000000000119 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added offline-protection temp from GUI(172.20.120.47)"

Related

- 00063402
- 00063411

00063402

Meaning
An administrator changed an Offline Protection profile.

Field name	Description
ID (`log_id`)	00063402 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:18:49 log_id=00063402 msg_id=000000000120 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed offline-protection temp from GUI(172.20.120.47)"

Related

- 00063401
- 00063411

00063411

Meaning
An administrator deleted an Offline Protection profile.

Field name	Description
ID (`log_id`)	00063411 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:18:53 log_id=00063411 msg_id=000000000121 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted offline-protection temp from GUI(172.20.120.47)"

Related

- 00063401
- 00063402

00064401

Meaning
An administrator created an auto-learning profile.

Field name	Description
ID (`log_id`)	00064401 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:37:50 log_id=00064401 msg_id=000000000166 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added autolearning-profile auto-learning1 from GUI(172.20.120.47)"

Related

- 00064402
- 00064411

00064402

Meaning
An administrator changed an auto-learning profile.

Field name	Description
ID (`log_id`)	00064402 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:31:30 log_id=00064402 msg_id=000000000643 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed autolearning-profile auto-learning2 from GUI(192.168.1.28)"

Related

- 00064401
- 00064411

00064411

Meaning
An administrator deleted an auto-learning profile.

Field name	Description
ID (`log_id`)	00064411 See Log ID numbers on page 24.

Examples
date=2013-10-15 time=20:31:37 log_id=00064411 msg_id=000000000644 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted autolearning-profile auto-learning2 from GUI(192.168.1.28)"

Related

- 00064401
- 00064402

00065002

Meaning
An administrator changed an IP reputation setting.

Field name	Description
ID (`log_id`)	00065002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:38:03 log_id=00065002 msg_id=000000000171 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed IP Reputation from GUI(172.20.120.47)"

00065501

Meaning
An administrator created an IP reputation exemption.

Field name	Description
ID (`log_id`)	00065501 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:38:14 log_id=00065501 msg_id=000000000172 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added IP Reputation Exception 1 from GUI(172.20.120.47)"

Related

- 00065502
- 00065511

00065502

Meaning
An administrator changed an IP reputation exemption.

Field name	Description
ID (`log_id`)	00065502 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:51:51 log_id=00065502 msg_id=000000000789 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed IP Reputation Exception 2 from GUI(192.168.1.28)"

Related

- 00065501
- 00065511

00065511

Meaning
An administrator deleted an IP reputation exemption.

Field name	Description
ID (`log_id`)	00065511 See Log ID numbers on page 24.

Examples
date=2013-10-17 time=22:51:54 log_id=00065511 msg_id=000000000790 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted IP Reputation Exception 2 from GUI(192.168.1.28)"

Related

- 00065501
- 00065502

00066002

Meaning
Either: • An administrator edited the Severity and Trigger Action settings in a custom access rule. • An administrator edited a signature violation filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066002 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=11:59:11 log_id=00066002 msg_id=001248141094 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web from GUI(172.22.6.1)" date=2016-02-24 time=12:17:02 log_id=00066002 msg_id=001248141108 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web from GUI(172.22.6.1)"

Related

- 00066711

00066011

Meaning
An administrator added an IP address filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066101 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:40:49 log_id=00066011 msg_id=001248141135 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web from GUI(172.22.6.1)"

Related

- 00066002

00066101

Meaning
An administrator added an IP address filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066101 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:09:19 log_id=00066101 msg_id=001248141099 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web source-ip-filter 1 from GUI (172.22.6.1)"

Related

- 00066102
- 00066111

00066102

Meaning
An administrator changed an IP address filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066102 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:10:11 log_id=00066102 msg_id=001248141100 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web source-ip-filter 1 from GUI (172.22.6.1)"

Related

- 00066101
- 00066111

00066111

Meaning
An administrator deleted an IP address filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066111 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:10:54 log_id=00066111 msg_id=001248141101 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web source-ip-filter 1 from GUI (172.22.6.1)"

Related

- 00066101
- 00066102

00066151

Meaning
A FortiWeb administrator generated a URL filter in a custom rule by importing a scanner report file.

Field name	Description
ID (`log_id`)	00066151 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:29 log_id=00066151 msg_id=000011519635 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added custom-rule e-24 url-filter 2 from scanner_integration"

Related

- 00055901
- 00055971
- 00056401
- 00056402
- 00056421
- 00066601
- 00066921
- 08999999

00066201

Meaning
An administrator added an HTTP header filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066201 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:00:48 log_id=00066201 msg_id=001248141095 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web HTTP-header-filter 1 from GUI (172.22.6.1)"

Related

- 00066202
- 00066211

00066202

Meaning
An administrator changed an HTTP header filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066202 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:02:43 log_id=00066202 msg_id=001248141096 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web HTTP-header-filter 1 from GUI (172.22.6.1)"

Related

- 00066201
- 00066211

00066211

Meaning
An administrator deleted an HTTP header filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066211 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:07:17 log_id=00066211 msg_id=001248141097 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web HTTP-header-filter 1 from GUI (172.22.6.1)"

Related

- 00066201
- 00066202

00066301

Meaning
An administrator added an access rate limit filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066301 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:13:05 log_id=00066301 msg_id=001248141103 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web access-limit-filter 1 from GUI (172.22.6.1)"

Related

- 00066302
- 00066311

00066302

Meaning
An administrator edited an access rate limit filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066302 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:13:37 log_id=00066302 msg_id=001248141104 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web access-limit-filter 1 from GUI (172.22.6.1)"

Related

- 00066301
- 00066311

00066311

Meaning
An administrator deleted an access rate limit filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066311 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:14:52 log_id=00066311 msg_id=001248141105 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web access-limit-filter 1 from GUI (172.22.6.1)"

Related

- 00066301
- 00066302

00066401

Meaning
An administrator added a transaction timeout filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066401 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:25:09 log_id=00066401 msg_id=001248141113 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web HTTP-transaction 1 from GUI (172.22.6.1)"

Related

- 00066402
- 00066411

00066402

Meaning
An administrator edited a transaction timeout filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066402 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:29:01 log_id=00066402 msg_id=001248141114 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web HTTP-transaction 1 from GUI (172.22.6.1)"

Related

- 00066401
- 00066411

00066411

Meaning
An administrator deleted a transaction timeout filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066411 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:29:36 log_id=00066411 msg_id=001248141115 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web HTTP-transaction 1 from GUI (172.22.6.1)"

Related

- 00066401
- 00066402

00066451

Meaning
An administrator added an HTTP response code filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066451 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:30:18 log_id=00066451 msg_id=001248141116 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web response-code 1 from GUI (172.22.6.1)"

Related

- 00066452
- 00066461

00066452

Meaning
An administrator changed an HTTP response code filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066452 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:31:20 log_id=00066452 msg_id=001248141117 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web response-code 1 from GUI (172.22.6.1)"

Related

- 00066451
- 00066461

00066461

Meaning
An administrator deleted an HTTP response code filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066461 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:31:55 log_id=00066461 msg_id=001248141118 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web response-code 1 from GUI (172.22.6.1)"

Related

- 00066451
- 00066452

00066501

Meaning
An administrator added a content type filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066501 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:32:31 log_id=00066501 msg_id=001248141119 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web content-type 1 from GUI (172.22.6.1)"

Related

- 00066502
- 00066511

00066502

Meaning
An administrator edited a content type filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066502 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:33:14 log_id=00066502 msg_id=001248141120 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web content-type 1 from GUI (172.22.6.1)"

Related

- 00066501
- 00066511

00066511

Meaning
An administrator deleted a content type filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066511 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:33:20 log_id=00066511 msg_id=001248141121 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web content-type 1 from GUI (172.22.6.1)"

Related

- 00066501
- 00066502

00066551

Meaning
An administrator added a packet interval timeout filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066551 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:33:51 log_id=00066551 msg_id=001248141122 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web packet-interval 1 from GUI (172.22.6.1)"

Related

- 00066552
- 00066561

00066552

Meaning
An administrator edited a packet interval timeout filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066552 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:34:06 log_id=00066552 msg_id=001248141123 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web packet-interval 1 from GUI (172.22.6.1)"

Related

- 00066551
- 00066561

00066561

Meaning
An administrator deleted a packet interval timeout filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066561 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:34:36 log_id=00066561 msg_id=001248141124 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web packet-interval 1 from GUI (172.22.6.1)"

Related

- 00066551
- 00066552

00066601

Meaning
A FortiWeb administrator generated a custom rule by importing a scanner report file.

Field name	Description
ID (`log_id`)	00066601 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:29 log_id=00066001 msg_id=000011519604 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added custom-rule e-19 from Scanner Integration "

Related

- 00055901
- 00055971
- 00056401
- 00056402
- 00056421
- 00066151
- 00066921
- 08999999

00066711

Meaning
An administrator deleted a signature violation filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066711 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:24:00 log_id=00066711 msg_id=001248141110 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web custom-signature 0 from GUI (172.22.6.1)"

Related

- 00066002

00066801

Meaning
An administrator added an occurrence filter to a custom access rule.

Field name	Description
ID (`log_id`)	00066801 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:36:57 log_id=00066801 msg_id=001248141127 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule New-custom-access-rule-for-web occurrence 1 from GUI (172.22.6.1)"

Related

- 00066802
- 00066811

00066802

Meaning
An administrator edited an occurrence filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066802 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:37:05 log_id=00066802 msg_id=001248141128 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule New-custom-access-rule-for-web occurrence 1 from GUI (172.22.6.1)"

Related

- 00066801
- 00066811

00066811

Meaning
An administrator deleted an occurrence filter in a custom access rule.

Field name	Description
ID (`log_id`)	00066811 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:37:34 log_id=00066811 msg_id=001248141129 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-rule New-custom-access-rule-for-web occurrence 1 from GUI (172.22.6.1)"

Related

- 00066801
- 00066802

00066901

Meaning
A FortiWeb administrator added a custom access policy.

Field name	Description
ID (`log_id`)	00066901 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:42:41 log_id=00066901 msg_id=001248141136 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-policy custom-policy from GUI(172.22.6.1)"

Related

- 00066911
- 00066921

00066911

Meaning
A FortiWeb administrator deleted a custom access policy.

Field name	Description
ID (`log_id`)	00066911 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:45:48 log_id=00066911 msg_id=001248141141 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-policy custom-policy from GUI(172.22.6.1)"

Related

- 00066901
- 00066921

00066921

Meaning
A FortiWeb administrator generated a custom access policy by importing a scanner report file.

Field name	Description
ID (`log_id`)	00066921 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:30 log_id=00066921 msg_id=000011519648 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin added custom-policy e rule 17 from scanner_integration"

Related

- 00055901
- 00055971
- 00056401
- 00056402
- 00056421
- 00066151
- 00066601
- 08999999

00066931

Meaning
A FortiWeb administrator removed a rule from a custom access policy.

Field name	Description
ID (`log_id`)	00066931 See Log ID numbers on page 24.

Examples
date=2016-02-24 time=12:44:19 log_id=00066931 msg_id=001248141138 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=delete status=success msg="User admin deleted custom-policy custom-policy rule 1 from GUI(172.22.6.1)"

Related

- 00066901
- 00066911

00068001

Meaning
An administrator created a combination access control and rate limit rule (“custom rule”).

Field name	Description
ID (`log_id`)	00068001 See Log ID numbers on page 24.

Examples
date=2014-04-21 time=18:19:40 log_id=00068001 msg_id=000000047914 device_ id=FV400C3M12000060 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-rule Custom_rule_for_PNG_server1 from GUI(172.22.6.231)"

Related

- 00068002
- 00068011

00068002

Meaning
An administrator changed a combination access control and rate limit rule (“custom rule”).

Field name	Description
ID (`log_id`)	00068002 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=09:21:30 log_id=00068002 msg_id=000000000441 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-rule combo-IP-rate1 from GUI(172.20.120.47)"

Related

- 00068011

00068011

Meaning
An administrator deleted a combination access control and rate limit rule (“custom rule”).

Field name	Description
ID (`log_id`)	00068011 See Log ID numbers on page 24.

Examples
date=2013-10-11 time=09:21:40 log_id=00068011 msg_id=000000000442 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-rule combo-IP-rate1 from GUI(172.20.120.47)"

Related

- 00068001
- 00068002

00068301

Meaning
An administrator created a combination access control and rate limit policy (“custom policy”).

Field name	Description
ID (`log_id`)	00068301 See Log ID numbers on page 24.

Examples
date=2014-04-21 time=18:25:26 log_id=00068301 msg_id=000000047918 device_ id=FV400C3M12000060 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added custom-policy Custom_Policy_For_PNG from GUI(172.22.6.231)"

Related

- 00068302
- 00068311

00068302

Meaning
An administrator changed a combination access control and rate limit policy (“custom policy”).

Field name	Description
ID (`log_id`)	00068302 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:53:29 log_id=00068302 msg_id=000000000230 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed custom-policy combo-access-controls1 from GUI(172.20.120.47)"

Related

- 00068301
- 00068311

00068311

Meaning
An administrator deleted a combination access control and rate limit policy (“custom policy”).

Field name	Description
ID (`log_id`)	00068311 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:53:39 log_id=00068311 msg_id=000000000231 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted custom-policy combo-access-controls1 from GUI(172.20.120.47)"

Related

- 00068301
- 00068302

00068401

Meaning
An administrator has added an padding oracle rule.

Field name	Description
ID (`log_id`)	00068401 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=18:19:31 log_id=00068401 msg_id=000000820334 device_ id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added waf-padding-oracle padding_001 from GUI(172.22.6.230)"

Related

- 00068402
- 00068411

00068402

Meaning
An administrator edited an padding oracle rule.

Field name	Description
ID (`log_id`)	00068402 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=18:24:59 log_id=00068402 msg_id=000000820335 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed waf-padding-oracle padding_001 from GUI(172.22.6.230)"

Related

- 00068401
- 00068411

00068411

Meaning
An administrator deleted an padding oracle rule.

Field name	Description
ID (`log_id`)	00068411 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=18:26:05 log_id=00068411 msg_id=000000820336 device_id=FVVM020000018475 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted waf-padding-oracle padding_001 from GUI(172.22.6.230)"

Related

- 00068401
- 00068402

00068701

Meaning
An administrator added a web cache policy exception.

Field name	Description
ID (`log_id`)	00068701 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:44:43 log_id=00068701 msg_id=000000179517 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added web-cache-exception ddd from GUI(172.22.6.66)"

Related

- 00068711
- 00068801
- 00068802
- 00068811

00068711

Meaning
An administrator deleted a web cache policy exception.

Field name	Description
ID (`log_id`)	00068711 See Log ID numbers on page 24.

Examples
date=2014-09-11 time=02:00:30 log_id=00068711 msg_id=000003041973 device_id=FV400C3M14000006 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted web-cache-exception ddd from GUI(172.22.14.6)"

Related

- 00068701
- 00068801
- 00068802
- 00068811

00068801

Meaning
An administrator added a web cache policy.

Field name	Description
ID (`log_id`)	00068801 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:41:57 log_id=00068801 msg_id=000000179514 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added web-cache-policy FortiWeb_web_cache from GUI(172.22.6.66)"

Related

- 00068802
- 00068811
- 00068701
- 00068711

00068802

Meaning
An administrator changed a web cache policy.

Field name	Description
ID (`log_id`)	00068802 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:43:10 log_id=00068802 msg_id=000000179515 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed web-cache-policy FortiWeb_web_cache from GUI(172.22.6.66)"

Related

- 00068801
- 00068811
- 00068701
- 00068711

00068811

Meaning
An administrator deleted a web cache policy.

Field name	Description
ID (`log_id`)	00068811 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=16:43:41 log_id=00068811 msg_id=000000179516 device_id=FVVM040000018473 vd="domain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted web-cache-policy FortiWeb_web_cache from GUI(172.22.6.66)"

Related

- 00068801
- 00068802
- 00068701
- 00068711

00090001

Meaning
An administrator created a vulnerability scan schedule.

Field name	Description
ID (`log_id`)	00090001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:24:24 log_id=00090001 msg_id=000000000140 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs schedule vuln-scan-schedule1 from GUI(172.20.120.47)"

Related

- 00090002
- 00090011

00090002

Meaning
An administrator changed a vulnerability scan schedule.

Field name	Description
ID (`log_id`)	00090002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:24:34 log_id=00090002 msg_id=000000000141 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wvs schedule vuln-scan-schedule1 from GUI(172.20.120.47)"

Related

- 00090001
- 00090011

00090011

Meaning
An administrator deleted a vulnerability scan schedule.

Field name	Description
ID (`log_id`)	00090011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:24:44 log_id=00090011 msg_id=000000000142 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs schedule vuln-scan-schedule1 from GUI(172.20.120.47)"

Related

- 00090001
- 00090002

00090101

Meaning
An administrator created a vulnerability scan profile.

Field name	Description
ID (`log_id`)	00090101 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:38:53 log_id=00090101 msg_id=000000734654 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs profile ddddd from GUI(172.22.6.237)"

Related

- 00090102
- 00090111

00090102

Meaning
An administrator changed a vulnerability scan profile.

Field name	Description
ID (`log_id`)	00090102 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:29:10 log_id=00090102 msg_id=000000000144 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wvs profile vuln-scan-profile1 from GUI(172.20.120.47)"

Related

- 00090101
- 00090111

00090111

Meaning
An administrator deleted a vulnerability scan profile.

Field name	Description
ID (`log_id`)	00090111 See Log ID numbers on page 24.

Examples
date=2014-04-10 time=17:42:52 log_id=00090111 msg_id=000000734655 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs profile ddddd from GUI(172.22.6.237)"

Related

- 00090101
- 00090102

00091101

Meaning
An administrator created a vulnerability scan policy.

Field name	Description
ID (`log_id`)	00091101 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:29:40 log_id=00091101 msg_id=000000000144 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added wvs policy vulnscan1 from GUI(172.20.120.47)"

Related

- 00091102
- 00091111

00091102

Meaning
An administrator changed a vulnerability scan policy.

Field name	Description
ID (`log_id`)	00091102 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:29:50 log_id=00091102 msg_id=000000000145 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed wvs policy vulnscan1 from GUI(172.20.120.47)"

Related

- 00091101
- 00091111

00091111

Meaning
An administrator deleted a vulnerability scan policy.

Field name	Description
ID (`log_id`)	00091111 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:29:59 log_id=00091111 msg_id=000000000146 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted wvs policy vulnscan1 from GUI(172.20.120.47)"

Related

- 00091101
- 00091102

00093001

Meaning
An administrator created an anti-defacement monitor.

Field name	Description
ID (`log_id`)	00093001 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:17:38 log_id=00093001 msg_id=000000000114 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added website 1 from GUI(172.20.120.47)"

Related

- 00093002
- 00093011

00093002

Meaning
An administrator changed an anti-defacement monitor.

Field name	Description
ID (`log_id`)	00093002 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:17:46 log_id=00093002 msg_id=000000000115 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed website 1 from GUI(172.20.120.47)"

Related

- 00093001
- 00093011

00093011

Meaning
An administrator deleted an anti-defacement monitor.

Field name	Description
ID (`log_id`)	00093011 See Log ID numbers on page 24.

Examples
date=2013-10-08 time=10:17:56 log_id=00093011 msg_id=000000000116 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="admin "pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted website 1 from GUI(172.20.120.47)"

Related

- 00093001
- 00093002

00093501

Meaning
An administrator created an anti-defacement file filter.

Field name	Description
ID (`log_id`)	00093501 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=11:54:59 log_id=00093501 msg_id=000000003151 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=add status=success msg="User admin added file-filter video_content from GUI(172.20.120.61)"

Related

- 00093502
- 00093511

00093502

Meaning
An administrator edited an anti-defacement file filter.

Field name	Description
ID (`log_id`)	00093502 See Log ID numbers on page 24.

Examples
date=2014-09-10 time=17:06:02 log_id=00093502 msg_id=000085523288 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=edit status=success msg="User admin changed file-filter video_files from GUI(172.22.14.6)"

Related

- 00093501
- 00093511

00093511

Meaning
An administrator deleted an anti-defacement file filter.

Field name	Description
ID (`log_id`)	00093511 See Log ID numbers on page 24.

Examples
date=2014-09-03 time=12:15:06 log_id=00093511 msg_id=000000003152 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin deleted file-filter video_content from GUI(172.20.120.61)"

Related

- 00093501
- 00093502

08999999

Meaning
A FortiWeb administrator imported a scanner report file.

Field name	Description
ID (`log_id`)	08999999 See Log ID numbers on page 24.

Examples
date=2016-02-18 time=16:42:30 log_id=08999999 msg_id=000011519649 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="admin" pri=information trigger_policy="" user=daemon_admin ui=sys action=add status=success msg="User daemon_admin integrated vulnerabilities in /var/log/export.xml from Scanner Integration "

Related

- 00055901
- 00055971
- 00056401
- 00056402
- 00056421
- 00066151
- 00066601
- 00066921

10000009

Meaning
An administrator powered on the FortiWeb appliance.

Field name	Description
ID (`log_id`)	10000009 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
Action (`action`)	`start`

Examples
date=2013-10-08 time=01:33:34 log_id=10000009 msg_id=000000000007 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system)" pri=information trigger_policy="" user=system ui=sys action=start status=success msg="FortiWeb started"

Related

- Reboot, shut down, & boot up messages
- 10000010
- 10000011

10000010

Meaning
A FortiWeb administrator rebooted the operating system of the appliance. If the administrator did this through the web UI, the log message includes the administrator's comment, if he or she provided one.

Field name	Description
ID (`log_id`)	10000010 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
Action (`action`)	`reboot`
User Interface (`ui`)	{GUI | none | telnet | ssh | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (`msg`)	User <administrator_name> changed interface <interface_name> from {GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2013-10-08 time=09:48:54 log_id=10000010 msg_id=000000000070 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system)" pri=critical trigger_policy="" user=admin ui=GUI action=reboot status=success msg="User admin rebooted the device from GUI(172.20.120.47).This is my comment."

Related

- Reboot, shut down, & boot up messages
- 10000009
- 10000011

10000011

Meaning
An administrator halted the operating system of the FortiWeb appliance in preparation to power off the hardware.

Field name	Description
ID (`log_id`)	10000011 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notification` See Priority level on page 25.
Action (`action`)	`shutdown`

Examples
date=2014-06-16 time=02:41:42 log_id=10000011 msg_id=000000022971 device_id=FVVM020000018466 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=shutdown status=success msg="User admin shut down the device from GUI(172.22.6.241)."

Related

- Reboot, shut down, & boot up messages
- 10000009
- 10000010

10000012

Meaning
An administrator's inactive session timed out.

Field name	Description
ID (`log_id`)	10000012 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notification` See Priority level on page 25.
Action (`action`)	`shutdown`

Examples
date=2013-10-09 time=20:37:24 log_id=10000012 msg_id=000000000340 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system)" pri=notification trigger_policy="" user=admin ui=console action=logout status=success msg="User admin time out on console"

Related

- 10000016

10000013

Meaning
An administrator uploaded a data analytics definition file.

Field name	Description
ID (`log_id`)	10000013 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
Action (`action`)	`update`

Examples
date=2014-04-10 time=13:01:33 log_id=10000013 msg_id=000044293782 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin success loaded data analytics file from GUI(10.200.10.80)."

10000014

Meaning
An administrator deleted a locally-stored attack log, event log, or traffic log file.

Field name	Description
ID (`log_id`)	10000014 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notice` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`del`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> has deleted disk log <file_str> from {GUI (<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-04-10 time=18:09:47 log_id=10000014 msg_id=000000195890 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=GUI action=del status=success msg="User admin has deleted disk log elog(2014-04-09-23:34:02).log from GUI(172.22.6.240)"

Related

- 00032006

10000015

Meaning
Either: • A FortiWeb administrator downloaded a log file. • A FortiWeb downloaded a client certificate file from the HSM (hardware security module).

Field name	Description
ID (`log_id`)	10000015 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User Interface (`ui`)	`GUI`
Action (`action`)	`backup` or `hsm`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> download {Attack | Event | Traffic } from GUI (<mgmt_ip>) User <administrator_name> download hsm client certificate file from GUI (<mgmt_ip>)

Examples
date=2013-10-07 time=16:13:10 log_id=10000015 msg_id=000000001218 device_ id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=backup status=success msg="Successfully. User admin download Event LOG from GUI(172.20.120.47)." date=2016-02-18 time=15:10:57 log_id=10000015 msg_id=000067508836 device_ id=FV400D3A15000010 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=hsm status=success msg="User admin download hsm client certificate file from GUI(172.22.6.66)"

Related

- 10000048

10000016

Meaning
Either a FortiWeb administrator logged in successfully, or attempted to log in but failed.

Field name	Description
ID (`log_id`)	10000016 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notification` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`login`
Status (`status`)	`success` `failed`
Message (`msg`)	User <administrator_name> logged in successfully from {(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>)} User <administrator_name> login failed from {(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>)}

Examples
date=2014-04-10 time=13:31:37 log_id=10000016 msg_id=000044294845 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=telnet action=login status=success msg="User admin logged in successfully from telnet(10.200.0.1)"

Related

- 10000012

10000017

Meaning
Someone attempted to log in to a FortiWeb administrator account, successfully or failed.

Solution
If you suspect that an unauthorized person is attempting to log in to your FortiWeb, there are some preventative measures that you can take. Restrict physical access to the FortiWeb to ensure that only authorized persons can attach a console or computer to the appliance's local console port. Configure all administrator accounts with trusted IPs that restrict login attempts to ones that originate **only** from your trusted, physically secured, private administrative network. Do not allow login attempts from hostile or untrusted IP addresses. If **any** administrator account uses a broad trusted IP definition such as `0.0.0.0/0.0.0.0`, then due to that account, FortiWeb must allow login attempts from all IP addresses, including the Internet. Brute force login attempts are then a significant risk. Enable strong password enforcement. Passwords must be significantly complex in length and character types in order to make brute force login attempts impractically slow. Require regular password changes. Enable only secure administrative protocols (SSH and HTTPS) on network interfaces. Insecure protocols such as HTTP and Telnet are easily susceptible to eavesdropping, man-in-the-middle, and other attacks that could compromise your connection, your password, or both.

Field name	Description
ID (`log_id`)	10000017 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
Level (`pri`)	`alert` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	`{GUI(<mgmt_ip>) | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}`
Action (`action`)	`login`

Field name	Description
Status (`status`)	`failure | success`
Message (`msg`)	User <administrator_name> login failed from {GUI(<mgmt_ip>) | telnet (<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples

2023-03-13T17:53:18.818570+08:00 10.20.128.44 date=2023-03-13 time=00:27:21 log_id=10000017 msg_id=000004513309 device_id=FVVM02TM22001887 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" timezone_dayst="GMT+8" type=event subtype="system" pri=alert trigger_policy="N/A" user=admin ui=GUI action=login status=failure msg="User admin login failed from GUI->HTTPS (172.23.132.33)"

2023-03-13T17:53:21.419753+08:00 10.20.128.44 date=2023-03-13 time=00:27:24 log_id=10000017 msg_id=000004513310 device_id=FVVM02TM22001887 vd="root" timezone="(GMT-8:00)Pacific Time (US&Canada)" timezone_dayst="GMT+8" type=event subtype="system" pri=information trigger_policy="N/A" user=admin ui=GUI action=login status=success msg="User admin logged in successfully from GUI->HTTPS(172.23.132.33)"

10000018

Meaning
A FortiWeb administrator logged out.

Field name	Description
ID (`log_id`)	10000018 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notification` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`logout`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> logout from {GUI(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2013-10-08 time=11:25:37 log_id=10000018 msg_id=000000000272 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system)" pri=information trigger_policy="" user=admin ui=GUI action=logout status=success msg="User admin logs out from GUI(172.20.120.47)"

Related

- 10000012

10000019

Meaning
A FortiWeb administrator upgraded the firmware image.

Field name	Description
ID (`log_id`)	10000019 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`upgrade`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> upgrade the image from {GUI(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-04-10 time=15:26:51 log_id=10000019 msg_id=000000550016 device_id=FVVM040000018474 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=upgrade status=success msg="User admin upgrade the image from GUI(10.200.0.1)"

Related

- 10000020

10000020

Meaning
A FortiWeb administrator downgraded the firmware image.

Field name	Description
ID (`log_id`)	10000020 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`downgrade`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> downgraded the image from {GUI(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-04-10 time=15:22:38 log_id=10000020 msg_id=000000548987 device_id=FVVM040000018474 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=downgrade status=success msg="User admin downgraded the image from GUI(10.200.0.1)"

Related

- 10000019

10000021

Meaning
A FortiWeb administrator restored the system configuration.

Field name	Description
ID (`log_id`)	10000021 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`restore`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> downgraded the image from {GUI(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console}

Examples
date=2014-08-06 time=18:37:45 log_id=10000021 msg_id=000016328576 device_id=FV-4KD3R13800048 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=restore status=success msg="User admin restored the configuration from GUI(172.22.6.149)"

10000022

Meaning
A FortiWeb administrator manually requested an update to either the FortiWeb regular virus database, the FortiWeb extended virus database, or the virus engine.

Field name	Description
ID (`log_id`)	10000022 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`update`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> manually update {virus signature | virus extend signature | virus engine} from {GUI(<mgmt_ip>) | jsconsole | telnet (<mgmt_ip>) | ssh(<mgmt_ip>) | console} success

Examples

date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292728 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin manually update virus signature from GUI(10.200.10.80) success"

date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292727 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin update virus extend signature from GUI(10.200.10.80) success"

date=2014-04-10 time=12:48:29 log_id=10000022 msg_id=000044292726 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin update virus engine from GUI(10.200.10.80) success"

10000023

Meaning
One of the following events: • A FortiWeb configuration backup to an FTP/SFTP server either succeeded or failed. • The scheduled configuration backup daemon started. Normally, this occurs at boot time. • An administrator downloaded a log file. • An administrator downloaded a backup of the system configuration file, fweb_system.conf. • An administrator downloaded an X.509 CSR.

Solution
There could be several reasons why the backup failed. Check the IP address and login credentials that you have defined for FortiWeb's FTP/SFTP connection. Verify that the directory you specified to receive backups exists, and has write permissions for that user name. Make sure that the FTP/SFTP server's disk is not full, that it has enough disk space to receive the backup, and that that user name has not consumed its disk space quota, if any. Verify that FortiWeb's system time is accurate. Make sure that the backup is not scheduled during a network or server maintenance window, when the server or daemon are down. Test that a **reliable** route exists between FortiWeb and the FTP/SFTP server by using `execute ping` and `execute traceroute` commands in the CLI. Keep in mind that if the network or the server was down for maintenance at the time of the backup attempt, the backup would have failed during that time, even if connectivity works for you now. If you have firewalls or routers performing NAT between FortiWeb and the server, verify that FTP connections are allowed between them. Firewalls include host-based ones that may be on the server itself, such as Windows Firewall or `ipfw`. Keep in mind that the FTP protocol typically requires port 21, but that its mechanism style could be active or passive FTP, and that the protocol has both a command channel and a data transfer channel. If either of these channels fail, the backup will fail. SFTP typically requires port 22.

Field name	Description
ID (`log_id`)	10000023 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User	`system`

Field name	Description
(user)	
User Interface (ui)	sys
Action (action)	backup start
Message (msg)	backup backup_<FTP-backup_name>_<timestamp_str> to <server_ipv4> <folder_str> {FAIL | OK}

Examples

date=2013-10-08 time=09:42:19 log_id=10000023 msg_id=000000000038 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system)" pri=notification trigger_policy="" user=system ui=sys action=backup status=failed msg="ftp backup backup_scheduled_backup_20131008094215 to ftp.example.com / FAILED"

date=2013-10-08 time=10:59:14 log_id=10000023 msg_id=000000146032 type=event subtype="system" pri=information device_id=FVVM020000003619 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" user=system action=backup msg="backup backup_backup-to-ftp-server_20121113105913 to 172.20.120.225 Downloads/fortiweb/backups/ OK"

date=2013-10-05 time=19:26:12 log_id=10000023 msg_id=000000001038 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=system ui=sys action=start status=success msg="Backup daemon started"

date=2014-04-10 time=18:14:52 log_id=10000023 msg_id=000000195894 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the Logging file from GUI(172.22.6.240)"

date=2014-04-10 time=18:17:06 log_id=10000023 msg_id=000000195895 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the System config file from GUI(172.22.6.240)"

date=2014-04-10 time=18:18:05 log_id=10000023 msg_id=000000195897 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=backup status=success msg="User admin backed up the Local Cert(CSR) file from GUI(172.22.6.240)"

Related

- 11001008

10000027

Meaning
A FortiWeb administrator changed the system time.

Field name	Description
ID (`log_id`)	10000027 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`change-time`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> changed time from <date & time> to <date & time>.

Examples
date=2014-04-10 time=15:13:20 log_id=10000027 msg_id=000044298000 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=console action=change-time status=failed msg="User admin changed time from Thu Apr 10 15:13:06 2014 to Thu Apr 10 15:13:20 2014 ."

10000028

Meaning
A FortiWeb administrator manually updated the IP reputation signature file.

Field name	Description
ID (`log_id`)	10000028 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`critical` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`update`
Status (`status`)	`success`
Message (`msg`)	User <administrator_name> manually update IP Reputation signature from time from from {GUI(<mgmt_ip>) | jsconsole | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} success.

Examples
date=2014-04-10 time=12:54:45 log_id=10000028 msg_id=000044293771 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=admin ui=GUI action=update status=success msg="User admin manually update IP Reputation signature from GUI(10.200.0.1) success"

10000031

Meaning
A FortiWeb administrator did not specify the cookie name for a Rewrite Cookie persistence policy.

Field name	Description
ID (`log_id`)	10000031 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notice` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI(<mgmt_ip>) | none | telnet(<mgmt_ip>) | ssh(<mgmt_ip>) | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Action (`action`)	`edit`
Status (`status`)	`failure`
Message (`msg`)	Command failed: 'next ' Return code -56: Empty value isn't allowed.

Examples
date=2016-02-24 time=11:44:32 log_id=10000031 msg_id=001248141085 device_id=FV-3KC3R09700002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=admin ui=GUI action=edit status=failure msg="Command failed: 'next ' Return code -56: Empty value isn't allowed."

10000048

Meaning
An administrator changed the HSM (hardware security module) configuration settings.

Field name	Description
ID (`log_id`)	10000048 See Log ID numbers on page 24.
Level (`pri`)	`information` See Priority level on page 25.

Examples
date=2016-02-18 time=15:08:02 log_id=10000048 msg_id=000067508828 device_ id=FV400D3A15000010 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=hsm status=failure msg="User admin add hsm partition success from GUI(172.22.6.66)." date=2016-02-18 time=14:51:29 log_id=10000048 msg_id=000067508810 device_ id=FV400D3A15000010 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=hsm status=failure msg="User admin delete hsm partition success from GUI(172.22.6.66)." date=2016-02-18 time=15:13:21 log_id=10000048 msg_id=000067508841 device_ id=FV400D3A15000010 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=GUI action=hsm status=failure msg="User admin register hsm success from GUI(172.22.6.66)."

Related

- 10000015

11001008

Meaning
The logging daemon started. Normally, this occurs at boot time.

Field name	Description
ID (`log_id`)	11001008 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`start`
Status (`status`)	`success`
Message (`msg`)	Log daemon started

Examples
date=2013-10-05 time=19:26:02 log_id=11001008 msg_id=000000001037 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=start status=success msg="Log daemon started"

Related

- 10000023

11002003

Meaning
Someone attempted to log in to a website where you have configured FortiWeb to provide end-user authentication, but failed.

Solution
If you suspect that an unauthorized person is attempting to log in to your website, there are some preventative measures that you can take. Require regular password changes. Require strong passwords. Passwords must be significantly complex in length and character types in order to make brute force login attempts impractically slow. Redirect requests for HTTP to a secure (HTTPS) URL. Insecure protocols such as HTTP are easily susceptible to eavesdropping, man-in-the-middle, and other attacks that could compromise your connection, your password, or both.

Field name	Description
ID (`log_id`)	11002003 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`alert` See Priority level on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`login`
Status (`status`)	`failed`
Message (`msg`)	User <user_name> <auth-method_str> login failed from <source_ipv4> request_url: <url>

Examples

date=2014-09-10 time=17:43:31 log_id=11002003 msg_id=000000852763 device_id=FV-3KD3R13800027 vd="Adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=login status=failed msg="User test1 HTTP BASIC login failed from 10.0.6.25 request_ url:fortinet.fortiweb.com/autotest/ldapuser.html"

Related

- 11002004

11002004

Meaning
An end-user successfully logged in to a website that you have configured FortiWeb to provide with authentication.

Field name	Description
ID (`log_id`)	11002004 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`login`
Status (`status`)	`success`
Message (`msg`)	User <user_name> <auth-method_str> login successfully from <source_ipv4> request_url: <url>

Examples
date=2014-09-10 time=17:43:39 log_id=11002004 msg_id=000000852769 device_id=FV-3KD3R13800027 vd="Adomain_new" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=login status=success msg="User test1 HTTP BASIC login successfully from 10.0.6.25 request_url:fortinet.fortiweb.com/autotest/ldapuser.html"

Related

- 11002003

11003601

Meaning
FortiWeb has detected a change to a website file that could indicate a defacement attack.

Field name	Description
ID (`log_id`)	11003601 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`monitor`
Status (`status`)	`success`
Message (`msg`)	File <file_name> on site <site_name> has been changed. Please confirm or restore it.

Examples
date=2014-04-10 time=14:43:11 log_id=11003601 msg_id=000044296936 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=monitor status=failed msg="File [/sig-db/signature.db] on site [2] has been changed. Please confirm or restore it."

11004002

Meaning
FortiWeb failed to connect to a website that you have configured to be monitored by the anti-defacement feature. Therefore it could not determine whether or not the website has been defaced.

Solution
If anti-defacement could not connect to the website: Verify the login and IP address that you provided. On the web server, check the file system permissions for the account that FortiWeb is using to connect. (FortiWeb must be able to both read and, if it will be restoring files, write to the folder and files. On Microsoft Windows, you may need to examine your security policy configuration to make sure that the account is authenticating as itself, and is not degrading to the guest account.) Verify that a route exists between the FortiWeb and the web server, and that connectivity is reliable, with no packet loss. Verify that any routers or firewalls between the appliance and the server, including Windows Firewall, are not blocking SSH, FTP, or CIFS connections. Other troubleshooting varies by the protocol that FortiWeb is using to connect, such as checking for a compatible protocol version and cipher suite.

Field name	Description
ID (`log_id`)	11004002 See Log ID numbers on page 24.
Sub Type (`subtype`)	`admin` See Subtypes on page 25.
Level (`pri`)	`warning` See Priority level on page 25.
User Interface (`ui`)	`anti-defacement`
Action (`action`)	`monitor`
Status (`status`)	`alert`
Message (`msg`)	Fail to connect to website <anti-defacement_name> (host is <server_ipv4>)

Examples

date=2012-02-13 time=18:49:09 log_id=00032901 msg_id=000015400628 type=event subtype="admin" pri=warning device_id=FV-1KC3R08600008 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" ui=anti-defacement action=monitor status=alert reason=filechange msg="Fail to connect to website www.example.com (host is 10.0.0.1)"

11004601

Meaning
A failover occurred — that is, the secondary (standby) appliance in the FortiWeb high availability (HA) cluster assumed the duties of processing traffic because it detected that the primary (active) appliance had failed.

Field name	Description
ID (`log_id`)	11004601 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`HA-Switch`
Status (`status`)	`success`
Message (`msg`)	HA switch from standby to main.

Examples
date=2014-04-10 time=14:35:54 log_id=11004601 msg_id=000044296931 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-Switch status=success msg="HA switch from standby to main."

Related

- 11004602
- 11004603
- 11004605
- 11004606
- 11004608

11004602

Meaning
An administrator has manually synchronized configuration files from the active HA appliance to the standby appliance.

Field name	Description
ID (`log_id`)	11004602 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`admin`
User Interface (`ui`)	`console`
Action (`action`)	`HA-Synchronize`
Status (`status`)	`success`
Message (`msg`)	User admin synchronize the waf configuration to standby device from console.

Examples
date=2014-04-10 time=14:55:59 log_id=11004602 msg_id=000044296940 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=admin ui=console action=HA-Synchronize status=success msg="User admin synchronize the waf configuration to standby device from console."

Related

- 11004601
- 11004603
- 11004605
- 11004606
- 11004608

11004603

Meaning
An appliance has been added to or removed from the high availability (HA) cluster.

Field name	Description
ID (`log_id`)	11004603 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`HA-member-left`
Status (`status`)	`success`
Message (`msg`)	Member <device_id> {left | join to the} HA group.

Examples
date=2014-04-10 time=15:37:31 log_id=11004603 msg_id=000044298015 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-member-left status=success msg="Member (FV-1KD3A13800001) left HA group." date=2014-04-10 time=15:38:42 log_id=11004603 msg_id=000044298021 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-member-join status=success msg="Member (FV-1KD3A13800001) join to the HA group."

Related

- 11004601
- 11004602

- 11004605
- 11004606
- 11004608

11004605

Meaning
In a high availability (HA) cluster, the configuration has been restored from the active (primary) to the standby (secondary) appliance.

Field name	Description
ID (`log_id`)	11004605 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`restore`
Status (`status`)	`success`
Message (`msg`)	HA restored the configuration from primary : <device_id>

Examples
date=2014-04-10 time=15:56:40 log_id=11004605 msg_id=000000187139 device_id=FV-1KD3A13800001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=restore status=success msg="HA restored the configuration from primary : FV-1KD3A13800002"

Related

- 11004601
- 11004602
- 11004603
- 11004606
- 11004608

11004606

Meaning
In a high availability (HA) cluster, the firmware has been restored from the active (primary) to the standby (secondary) appliance.

Field name	Description
ID (`log_id`)	11004606 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`restore`
Status (`status`)	`success`
Message (`msg`)	HA restored the image from primary : <device_id>

Examples
date=2014-04-10 time=16:49:38 log_id=11004606 msg_id=000000188232 device_id=FV-1KD3A13800001 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=restore status=success msg="HA restored the image from primary : FV-1KD3A13800002"

Related

- 11004601
- 11004602
- 11004603
- 11004605
- 11004608

11004608

Meaning
In a high availability (HA) cluster, the up/down status of the port that is monitored for link failure has changed..

Field name	Description
ID (`log_id`)	11004608 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`daemon`
Action (`action`)	`HA-monitor-port`
Status (`status`)	`success`
Message (`msg`)	HA monitor port <port_name> status changed from down to up.

Examples
date=2014-09-11 time=18:30:41 log_id=11004608 msg_id=000085524326 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-monitor-port status=success msg="HA monitor port (port4) status changed from up to down." date=2014-09-11 time=18:30:35 log_id=11004608 msg_id=000085524325 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=warning trigger_policy="" user=daemon ui=daemon action=HA-monitor-port status=success msg="HA monitor port (port4) status changed from down to up."

Related

- 11004601
- 11004602
- 11004603
- 11004605
- 11004606

11005901

Meaning

Either:

- the FortiGuard Antivirus, FortiGuard FortiWeb Security Service, or FortiGuard IP Reputation Intelligence Service (IRIS) license could not be authenticated
- the FortiGuard services were up-to-date as of the time when FortiWeb polled FortiGuard for updates
- FortiWeb could not connect to the FDN update servers, or the connection was interrupted, and therefore could not update its packages for FortiGuard services
- a FortiGuard service update installation failed
- a FortiGuard service update succeeded
- License authentication determined that the FortiWeb-VM license uploaded by an administrator is either valid or invalid.

Solution

If a FortiGuard license could not be authenticated:

Check with Fortinet Customer Service & Support (HTTPs://support.fortinet.com/) to make sure that you have purchased a license for this FortiWeb. If you have an HA pair, you should have one license for each appliance in the pair.

Verify that the license is not currently expired, or not yet in effect.

Verify that FortiWeb can connect to the Internet to validate its license. To do this, it will require a valid route, DNS settings, and possibly also time settings. If connectivity is unreliable, the initial license request may fail. In this case, you can either wait 30 minutes for the appliance to request authorization again, or use the CLI command `execute update-now` to force an immediate license authentication query.

If FortiWeb could not connect to the FDN or package retrieval failed, verify that FortiWeb has reliable Internet connectivity.

If the license is invalid:

Check with Fortinet Customer Service & Support (HTTPs://support.fortinet.com/) to make sure that you have purchased a license for this FortiWeb. If you have an HA pair, you should have one license for each appliance in the pair. If you are using a trial license, verify that the trial period has not expired.

If you are using a purchased license, verify that you have uploaded the license file to FortiWeb-VM.

Verify that the license has not been already used by another. (If you upload the license and it is currently associated with a different management IP, the web UI will display an error message: `Duplicate license detected.`)

Verify that the number of allocated vCPUs does not exceed the limit of the license.

Verify that FortiWeb can connect to the Internet to validate its license. To do this, it will require a valid route, DNS settings, and possibly also time settings. If connectivity is unreliable, the initial license request may fail. In this case, you can either wait 30 minutes for the appliance to request authorization again, or use the CLI command `execute update-now` to force an immediate license authentication query.

Field name	Description
ID (`log_id`)	11005901 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`error` (for unauthorized licenses, update failures, or connectivity errors) `information` (for up-to-date results from the FortiGuard poll) `critical` (for invalid license) See Priority level on page 25.
Message (`msg`)	Fortiweb {ip intelligence signature | virus engine | virus extend signature | virus signature | waf signature} is unauthorized
	Fortiweb {ip intelligence signature | virus engine | virus extend signature | virus signature | waf signature} is already up-to-date
	update failed, failed to connect to fds server!
	update failed, couldn't receive a update package!
	Fortiweb {ip intelligence signature | virus engine | virus extend signature | virus signature | waf signature} update failed
	Fortiweb {ip intelligence signature | virus engine | virus extend signature | virus signature | waf signature} update succeeded
	License status changed to {VALID | INVALID}

Examples
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000195866 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus engine is unauthorized"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000123728 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus extend signature is unauthorized"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000123727 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus signature is unauthorized"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000146653 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb waf signature is already up-to-date"

Examples
Fortiweb waf signature is unauthorized
date=2014-04-10 time=16:00:02 log_id=11005901 msg_id=000000734617 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb waf signature is unauthorized"
date=2014-04-10 time=16:00:02 log_id=11005901 msg_id=000000734621 device_id=FV-1KD3A13800027 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb ip intelligence signature is unauthorized"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000189416 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb ip reputation signature is already up-to-date"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000158889 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="update failed failed to connect fds server!"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000070564 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=error trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus extend signature update failed"
date=2014-04-10 time=17:00:02 log_id=11005901 msg_id=000000068286 device_id=FV-1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=daemon action=update status=failed msg="Fortiweb virus engine update succeeded"
date=2014-04-10 time=09:36:15 log_id=11005901 msg_id=000000022248 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="License status changed to VALID"
date=2014-04-10 time=09:36:15 log_id=11005901 msg_id=000000104120 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=event subtype="system" pri=critical trigger_policy="" user=daemon ui=daemon action=update status=failed msg="License status changed to INVALID"

11006004

Meaning
A FortiWeb administrator brought up or brought down a network interface,

Field name	Description
ID (`log_id`)	11006004 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`information` See Priority level on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`none`
Action (`action`)	`check-resource`
Status (`status`)	`failed`
Message (`msg`)	interface <interface_name> link {up | down}

Examples
date=2013-10-08 time=09:48:12 log_id=11006004 msg_id=000000000068 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system)" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="interface port2 link up" date=2013-10-08 time=14:09:10 log_id=11006004 msg_id=000000000286 device_ id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="interface vlan3 link down"

Related

- 00004401
- 00004402
- 00004411

11006005

Meaning
Either the CPU usage: • became too high and exceeded the alert threshold, or • lowered until it did not exceed the alert threshold anymore

Field name	Description
ID (`log_id`)	11006005 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`none`
Action (`action`)	`check-resource`
Status (`status`)	`failed`
Message (`msg`)	CPU usage raise too high,CPU(<percentage_int>) CPU usage reduced,CPU(<percentage_int>)

Examples
date=2013-10-05 time=20:26:59 log_id=11006005 msg_id=000000001043 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="CPU usage raise too high,CPU(96)" date=2013-10-07 time=15:29:35 log_id=11006005 msg_id=000000001207 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="CPU usage reduced, CPU usage is 53"

Related

- 00032006
- 11006006

11006006

Meaning
Either the RAM usage: • became too high and exceeded the alert threshold, or • lowered until it did not exceed the alert threshold anymore

Field name	Description
ID (`log_id`)	11006006 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
User (`user`)	`daemon`
User Interface (`ui`)	`none`
Action (`action`)	`check-resource`
Status (`status`)	`failed`
Message (`msg`)	mem usage raise too high,mem(<usage_int>) mem usage reduced,mem(<usage_int>)

Examples
date=2013-10-05 time=20:26:59 log_id=11006006 msg_id=000000001042 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="mem usage raise too high,mem(96)" date=2013-10-05 time=20:29:06 log_id=11006006 msg_id=000000001048 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=information trigger_policy="" user=daemon ui=none action=check-resource status=failed msg="mem usage reduced,mem(52)"

Related

- 00032006
- 11006005

11006701

Meaning
A certificate revocation list (CRL) has been updated using a query to a server.

Field name	Description
ID (`log_id`)	11006701 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`notice` See Priority level on page 25.
User (`user`)	`system`
User Interface (`ui`)	`none`
Action (`action`)	`edit`
Status (`status`)	`success`
Message (`msg`)	A CRL is updated crl=<crl_name> method=HTTP

Examples
date=2014-04-10 time=17:14:18 log_id=11006701 msg_id=000000179557 device_ id=FVVM040000018473 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice trigger_policy="" user=system ui=none action=edit status=success msg=" A CRL is updated crl=CRL_4 method=HTTP"

Related

- 00008801
- 00008811
- 00009301
- 00009311

19999496

Meaning
A web server that belongs to a server pool definition became available (up) or unavailable (down) according to the configured server health check, if any.

Solution
If a web server is being detected as unavailable, but it is actually up: Verify that you have selected a server health check in the server pool definition. Verify that the server health check is using a method to contact the server that the server can respond to. If you are using **Ping**, for example, the server must be responsive to ICMP `ECHO_REQUEST` signals.

Field name	Description
ID (`log_id`)	19999496 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`alert` See Priority level on page 25.
User (`user`)	`<administrator_name>`
User Interface (`ui`)	{GUI | none | telnet | ssh | console} Logins from `jsconsole` indicate use of the **CLI Console** widget on **System > Status > Status** in the web UI (GUI). The source IP address is the same as the one recorded in the corresponding log message for the GUI login.
Message (`msg`)	policy <policy_name> Physical Server[<pserver_name>:<pserver-port_int>] is {down | up}

Examples

date=2013-10-07 time=12:27:45 log_id=19999496 msg_id=000000001136 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy policy1 Physical Server[apache1:80] is up"

date=2013-10-05 time=19:26:44 log_id=19999496 msg_id=000000001039 device_id=FVVM040000010871 vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy policy1 Physical Server[apache1:80] is down"

Related

- 00040001
- 00040002
- 00040011

19999497

Meaning
The number of concurrent sessions has been reduced. For more information on model- or configuration-dependent limits, see the *FortiWeb Administration Guide*.

Field name	Description
ID (`log_id`)	19999497 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`alert` See Priority level on page 25.
Message (`msg`)	policy <policy_name> concurrent session reduced

Examples
date=2014-04-10 time=18:04:19 log_id=19999497 msg_id=000044306075 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=none status=failed msg="policy test concurrent session reduced"

Related

- 19999498

19999498

Meaning
The maximum number of concurrent sessions has been reached. For more information on model- or configuration-dependent limits, see the *FortiWeb Administration Guide*.

Field name	Description
ID (`log_id`)	19999498 See Log ID numbers on page 24.
Sub Type (`subtype`)	`system` See Subtypes on page 25.
Level (`pri`)	`alert` See Priority level on page 25.
Message (`msg`)	policy <policy_name> concurrent session exceed threshold

Examples
date=2014-04-10 time=18:03:39 log_id=19999498 msg_id=000044305882 device_id=FV-1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert trigger_policy="" user=daemon ui=daemon action=check-resource status=failed msg="policy test concurrent session exceed threshold"

Related

- 19999497

Attack

Attack log messages record traffic that violated its matching policy. Log ID numbers of this type are listed in the table Attack logs by main type, subtype & ID.

The operating mode, network topology, and the rule's configured **Action** can all affect how a policy responds to an attack, data leak, or server information disclosure. Depending on your configuration, violating traffic is either:

- blocked
- sanitized, then passed through
- allowed to continue unmodified (that is, logged only)

Attacks that generate log messages periodically

FortiWeb does not record the following types of attack logs individually. Instead, it records them periodically while the attack is ongoing, even if the attack has multiple sources:

- DoS attacks
- Padding oracle attacks
- HTTP/HTTPS protocol constraints

This aggregation prevents FortiWeb from flooding attack logs with identical or very similar messages. To differentiate logs caused by individual attacks from those caused by multiple attacks in the same category, FortiWeb records whether it generated the attack log message after matching multiple signatures.

In the attack log, the message field of aggregated log messages displays the message `rule_name : Custom Access Violation`.

In aggregated attacks log, the type field displays the message `Multiple Custom access rule Violations`.

Logging for threat scoring

By default, FortiWeb does not display all signature violations that contributed to a threat scoring attack log message as individual entries in the attack log. Instead, a single attack log message is displayed for the signature violations that contributed to a combined threat score that exceeded the maximum. However, all the signature violations that contributed to the score are displayed in the message details. (Double-click the message to display its details.)

Also by default, FortiWeb does not display messages for signature violations that generated a threat score but did not exceed the threat scoring threshold.

Use the following CLI command to display the signature violations that contributed to a threat scoring attack log message as individual entries and to display any signature violations that generated a threat score but did not exceed the threat scoring threshold:

config log attack-log

set show-all-log {enable | disable}

For more information on CLI commands, see *FortiWeb CLI Reference*:

https://docs.fortinet.com/product/fortiweb

Threat scoring attack log messages are also displayed in the aggregated attacks log.

Attack log descriptions

To locate a description for an attack log message, match the **ID** (`log_id`) field in the attack log message with that shown in the table Attack logs by main type, subtype & ID on page 451. All attack log messages have the same body fields, described in "Attack log fields" on page 1.

For attack log messages generated by a HTTP protocol constraint, the associated policy name is displayed in the raw view ([policy_name:**<protocol_constraint_name>**]) but not in the formatted view.

Attack logs by main type, subtype & ID

ID	main type	sub-type
20000001	Allow Method	N/A
20000002	Protected Hostnames	N/A
20000003	Page Access	N/A
20000004	Start Pages	N/A
20000005	Parameter Validation	N/A
20000006	Black IP List	N/A
20000007	URL Access	N/A
20000008	Signature Detection	• Cross Site Scripting • Cross Site Scripting (Extended) • Generic Attacks • Generic Attacks (Extended) • Bad Robot • Information Disclosure • Known Exploits • SQL Injection • SQL Injection (Extended) • SQL Injection (Syntax Based Detection) • Personally Identifiable Information • Trojans
20000009	Custom Signature Detection	N/A
20000011	Hidden Fields	N/A
20000012	Site Publish	Account Lockout
20000014	DoS Protection	• HTTP Flood Prevention • Malicious IPs • HTTP Access Limit • TCP Flood Prevention

ID	main type	sub-type
20000015	SYN Flood Protection	N/A
20000016	HTTPS Connection Failure	N/A
20000017	File Upload Restriction	• Antivirus Detection • Trojan Detection • FortiSandbox Detection • Illegal File Type • Illegal File Size
20000018	GEO IP	N/A
20000021	Custom Access	• Predefined-Crawler • Predefined-Vulnerability Scanning • Predefined-Slow-Attack • Predefined-Content-Scraping
20000022	IP Reputation	• Botnet • Anonymous Proxy • Phishing • Spam • Tor • Others
20000023	Padding Oracle	N/A
20000024	CSRF Protection	N/A
20000025	Quarantined IPs	N/A
20000026	HTTP Protocol Constraints	• Header Length Violation • Header Line Violation • Body Length Violation • Content Length Violation • Parameter Length Violation • HTTP Request Length Violation • URL Parameter Length Violation • Illegal HTTP Version • Cookie Number Overflow • Request Header Line number Overflow • URL Parameter Number Overflow • Illegal Hostname • Range Header Violation • Illegal HTTP Method • Illegal Content Length • Illegal Content Type • Illegal Response Code

ID	main type	sub-type
		• Missing POST Content Type • Body Parameter Length Violation • Header Name Length Violation • Header Value Length Violation • NULL Character in Parameter Name • NULL Character in Paramter Value • Illegal Header Name • Illegal Header Value • HTTP Request Filename Violation • Web Socket Protocol • Illegal Frame Type • Illegal Frame Flag • Illegal Connection Preface • HTTP/2 Header Table Size Overflow • HTTP/2 Concurrent Stream Number Overflow • HTTP/2 Initial Window Size Overflow • HTTP/2 Frame Size Overflow • HTTP/2 Header List Overflow • Illegal URL Parameter Name • Illegal URL Parameter Value • URL Parameter Name Overflow • URL Parameter Value Overflow • NULL Character in URL • Illegal Character in URL • Redundant HTTP Header • Malformed URL • Illegal Chunk Size • HTTP Parsing Error • HTTP Duplicated Parameter Name • Odd and Even Space Attack
20000027	Credential Stuffing Defense	• User Tracking • Site Publish
20000028	User Tracking	N/A
20000029	XML Validation Violation	• XML Schema Validation Violation • XML Element Attribute Number Overflow • XML Element Attribute Name Length Violations • XML Element Attribute Value Length Violations • XML Element Cdata Length Violations • XML Element Depth Violations • XML Element Name Length Violations • XML External Entity Violation • XML Entity Expansion Violations • XML XInclude Violation

ID	main type	sub-type
		• XML SchemaLocation Violation • XML SOAP Protocol Violation • XML SOAPAction Violation • XML SOAP Header Violation • XML SOAP Body Violation • SOAP Signature Error • SOAP Signature Verification Error • SOAP Encryption Error • SOAP Decryption Error
20000030	Cookie Security	• Cookie Decryption Error • Cookie Signed Verification Failed • IP replay protection violation
20000031	FTP Command Restriction	N/A
20000033	Timeout Session	N/A
20000035	FTP File Security	• FTP Antivirus Detection • FTP FortiSandbox Detection
20000036	FTPS Connection Failure	N/A
20000037	Machine Learning	• Anomaly in HTTP argument • HTTP Method violation • Charset detect failed
20000038	Openapi Validation Violation	• Openapi Query Parameter Violation • Openapi Path Parameter Violation • Openapi Cookie Parameter Violation • Openapi Header Parameter Violation • Openapi Request Body Violation
20000039	WebSocket Security	• Disallow WebSocket • Disallow Extensions • Illegal Format • Illegal Frame Size • Illegal Message Size • Disallow Origin • Parse error
20000040	MiTB AJAX Security	N/A
20000041	Bot Detection	N/A
20000042	CORS Check Security	• Invalid Origin • Disallow CORS • Disallow Origin

ID	main type	sub-type
		• Disallow method • Disallow header
20000043	JSON Validation Security	• JSON Schema Validation Violation • JSON Format Invalid Violation • JSON Data Size Violation • JSON Key Size Violation • JSON Key Number Violation • JSON Value Size Violation • JSON Value Number Violation • JSON Value Number in Array Violation • JSON Object Depth Violation

20000001

Meaning
HTTP Method Violation

Field name	Description
`log_id`	20000001 See Log ID numbers on page 24.
`main_type`	Allow Method
`subtype`	N/A

Examples

date=2022-07-10 time=15:48:46 log_id=20000001 msg_id=000000171391 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Allow Method" sub_type="N/A" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=54100 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/test1.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Allow Method Violation - HTTP request method (GET) is not allowed." signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000002

Meaning

Protected Hostnames violation

Field name	Description
log_id	20000002 See Log ID numbers on page 24.
main_type	Protected Hostnames
subtype	N/A

Examples

date=2022-07-09 time=06:59:42 log_id=20000002 msg_id=000034349837 device_id=FV3K1E3216000005 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Protected Hostnames" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=56756 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/dwg/common.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="HTTP Host Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FortiWeb_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=100 history_threat_weight=0 threat_level=Severe ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000003

Meaning

Page Access Rule Violation.

Field name	Description
log_id	20000003 See Log ID numbers on page 24.
main_type	Page Access
subtype	N/A

Examples

date=2022-07-30 time=17:49:39 log_id=20000003 msg_id=000000268842 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Page Access" sub_type="N/A" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=13.52.123.123 src_port=52970 dst=10.102.0.1 dst_port=80 http_method=get http_

Examples

url="/AUTOTEST/page_access/7.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Page Access Rule Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000004

Meaning

Start Page Violation.

Field name	Description
log_id	20000004 See Log ID numbers on page 24.
main_type	Start Pages
subtype	N/A

Examples

date=2022-07-30 time=18:04:15 log_id=20000004 msg_id=000000269047 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Start Pages" sub_type="N/A" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=13.52.123.123 src_port=53128 dst=10.102.0.1 dst_port=80 http_method=get http_

Examples

url="/autotest/test2.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Start Page Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000005

Meaning

Parameter name - (URI) triggered paramater validation.

Field name	Description
`log_id`	20000005 See Log ID numbers on page 24.
`main_type`	Parameter Validation
`subtype`	N/A

Examples

date=2022-07-10 time=14:59:01 log_id=20000005 msg_id=000000167489 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Parameter Validation" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=53779 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/input_rule/1.html?input=12345678901" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Parameter name - (input) triggered paramater validation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000006

Meaning

IP in block list was blocked.

Field name	Description
log_id	20000006 See Log ID numbers on page 24.
main_type	Black IP List
subtype	N/A

Examples
date=2022-07-30 time=18:33:03 log_id=20000006 msg_id=000003690359 device_id=FVVM04TM22000797 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Black IP List" sub_type="N/A" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=tcp action=Alert_Deny policy="port1-1-vip" src=44.1.254.5 src_port=10000 dst=44.1.0.2 dst_port=80 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="IP in black list was blocked" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="F11DE82FC4938D4110528102E0821F043A19" es=0 threat_weight=500 history_threat_weight=500 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Malicious" x509_cert_subject="none" owasp_api_top10="N/A"

20000007

Meaning
URL Access rule violation

Field name	Description
log_id	20000007 See Log ID numbers on page 24.
main_type	URL Access
subtype	N/A

Examples

date=2022-07-10 time=15:32:41 log_id=20000007 msg_id=000000170085 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="URL Access" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=53937 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/test8.html" http_host="10.0.0.22:8080" http_agent="python-for-fortiweb" http_session_id=none msg="URL Access Violation- URL matched the condition of rule (FWB_url_access_rule)." signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=50 history_threat_weight=0 threat_level=Substantial ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A01:2021-Broken Access Control" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000008

Meaning

Parameter, URL, or other elements in the packets triggered signatures included in the signature policy.

Field name	Description
`log_id`	20000008 See Log ID numbers on page 24.
`main_type`	Signature Detection
`subtype`	• Cross Site Scripting • Cross Site Scripting (Extended) • Generic Attacks • Generic Attacks (Extended) • Bad Robot • Information Disclosure • Known Exploits • SQL Injection • SQL Injection (Extended) • SQL Injection (Syntax Based Detection) • Personally Identifiable Information • Trojans

Examples

date=2022-07-11 time=13:59:15 log_id=20000008 msg_id=000000192894 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Signature Detection" sub_type="Cross Site Scripting" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55395 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/server_protection/1.html?para1=mocha:" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Parameter (para1) triggered signature ID 010000002 of Signatures policy FWB_server_protection" signature_subclass="Cross Site Scripting" signature_id="010000002" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A03:2021-Injection" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000009

Meaning

custom signature rule violation.

Field name	Description
log_id	20000009 See Log ID numbers on page 24.
main_type	Custom Signature Detection
subtype	N/A

Examples
date=2022-07-11 time=14:27:50 log_id=20000009 msg_id=000000194278 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Custom Signature Detection" sub_type="N/A" trigger_policy="N/A" severity_level=High proto=tcp service=https/tls1.2 backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55444 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/test.html?para1=auto1test" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Parameter triggered custom signature rule FWB_custom_protection_rule" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000010

Meaning
Brute Force Login Violation

Field name	Description
`log_id`	20000010 See Log ID numbers on page 24.
`main_type`	Brute Force Login
`subtype`	• Based on TCP Session • Based on Source IP

Examples

date=2022-07-25 time=14:42:16 log_id=20000010 msg_id=000000098389 device_id=FV1KE4417900002 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Brute Force Login" sub_type="Based on TCP Session" trigger_policy="" severity_level=High proto=tcp service=http action=Period_Block policy="FortiWeb_Policy_Default_AutoTest" src=10.200.10.100 src_port=57948 dst=10.0.1.5 dst_port=80 http_method=post http_url="/autotest/site_publishing_helper/login_check/0" http_host="FortiWebqa-win2k3.FortiWebqa.com" http_agent="python-for-fortiweb" http_session_id=none msg="Brute Force Login Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FortiWeb_server_pool_10.0.1.5" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=50 history_threat_weight=0 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A07:2021-Identification and Authentication Failures" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000011

Meaning

Hidden Field Manipulation

Field name	Description
log_id	20000011 See Log ID numbers on page 24.
main_type	Hidden Fields
subtype	N/A

Examples

date=2022-07-10 time=16:07:03 log_id=20000011 msg_id=000000172707 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Hidden Fields" sub_type="N/A" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=54288 dst=10.102.0.1 dst_port=80 http_method=post http_url="/autotest/price.jsp" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=678A3E0D2827A1BA431E73B767FEC87A msg="Hidden Field Manipulation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="505D9560F09669E9A3CFA1F0F16A3E7A17D7" es=0 threat_weight=50 history_threat_weight=50 threat_level=Substantial ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000012

Meaning

User defined in site publish has been locked out.

Field name	Description
log_id	20000012 See Log ID numbers on page 24.
main_type	Site Publish
subtype	Account Lockout See Subtypes on page 25.

Examples
date=2022-07-11 time=17:05:31 log_id=20000012 msg_id=000000207666 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Site Publish" sub_type="Account Lockout" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=56123 dst=10.0.1.5 dst_port=80 http_method=post http_url="/autotest/site_publishing_helper/login_check/0" http_host="fwbqa-win2k3.fwbqa.com" http_agent="python-for-fortiweb" http_session_id=none msg="User qa002 [Site Publish] has been locked out" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool_10.0.1.5" false_positive_mitigation="none" user_name="qa002" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A07:2021-Identification and Authentication Failures" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000013

Meaning
HTTP Parsing Error.

Field name	Description
log_id	20000013 See Log ID numbers on page 24.
main_type	HTTP Parsing Error
subtype	HTTP Parsing Error

Examples

date=2022-07-25 time=15:07:41 log_id=20000013 msg_id=000034681747 device_id=FV3K1E3216000005 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="HTTP Parsing Error" sub_type="HTTP Parsing Error" trigger_policy="" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert policy="FortiWeb_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=56020 dst=10.114.0.1 dst_port=80 http_method=get http_url="none" http_host="none" http_agent="none" http_session_id=none msg="Too Many Parameters" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000014

Meaning

DoS protection violation.

Field name	Description
log_id	20000014 See Log ID numbers on page 24.
main_type	DoS Protection
subtype	• HTTP Flood Prevention • Malicious IPs • HTTP Access Limit • TCP Flood Prevention

Examples
date=2022-07-25 time=12:42:43 log_id=20000014 msg_id=000003644544 device_ id=FVVM04TM22000797 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_ dayst="GMTa+7" type=attack pri=alert main_type="DoS Protection" sub_type="HTTP Access Limit" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=44.1.28.2 src_port=23896 dst=10.20.128.42 dst_port=80 http_method=post http_ url="/autotest/test2.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_ session_id=none msg="HTTP Access Limit Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_ name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_ status="Disabled" http_refer="none" http_version="1.x" dev_ id="9365DE6B98A2F64B4816AAA1181206DCF3B8" es=0 threat_weight=498 history_threat_ weight=59899420 threat_level=Substantial ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_ hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_ mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_ svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Malicious" x509_cert_subject="none" owasp_api_ top10="API4:2019 Lack of Resources & Rate Limiting"

20000015

Meaning
SYN Flood Protection.

Field name	Description
`log_id`	20000015 See Log ID numbers on page 24.
`main_type`	SYN Flood Protection
`subtype`	N/A

Examples
date=2022-07-25 time=14:37:16 log_id=20000015 msg_id=000306703852 device_ id=FV3KE3217000031 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_ dayst="GMTa+7" type=attack pri=alert main_type="SYN Flood Protection" sub_type="N/A" trigger_ policy="N/A" severity_level=Low proto=tcp service=tcp backend_service=tcp action=Alert policy="" src=0.0.0.0 src_port=0 dst=10.200.10.115 dst_port=0 http_method=none http_url="none" http_ host="none" http_agent="none" http_session_id=none msg="DoS Attack: SYN Flood" signature_ subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Unknown" content_switch_ name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_ weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_ mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_ svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000016

Meaning
HTTPS Connection Failure.

Field name	Description
log_id	20000016 See Log ID numbers on page 24.
main_type	HTTPS Connection Failure
subtype	N/A

Examples
date=2022-08-03 time=15:29:27 log_id=20000016 msg_id=000000288836 device_id=FV1KE4417900002 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="HTTPS Connection Failure" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=https/tls1.2 action=Alert_Deny policy="FortiWeb_Policy_Default_AutoTest" src=10.200.10.100 src_port=64643 dst=10.200.10.111 dst_port=443 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="SSL Error(267) - wrong version number" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000017

Meaning
File upload restrictions violation

Field name	Description
`log_id`	20000017 See Log ID numbers on page 24.
`main_type`	File Upload Restriction
`subtype`	• Antivirus Detection • Trojan Detection • FortiSandbox Detection • Illegal File Type • Illegal File Size

Examples
date=2022-07-10 time=16:32:45 log_id=20000017 msg_id=000000175392 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="File Upload Restriction" sub_type="Illegal File Type" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=54507 dst=10.102.0.1 dst_port=80 http_method=post http_url="/upload/servlet/UploadServlet" http_host="10.0.0.147:8090" http_agent="Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)" http_session_id=none msg="File name [filup.pdf]: Illegal file type" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="http://10.12.0.39:1001/upload/~upload" http_version="1.x" dev_id="none" es=0 threat_weight=50 history_threat_weight=0 threat_level=Substantial ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000018

Meaning
Unauthorized Geo IP.

Field name	Description
log_id	20000018 See Log ID numbers on page 24.
main_type	GEO IP
subtype	N/A

Examples
date=2022-07-30 time=22:04:53 log_id=20000018 msg_id=000003691445 device_id=FVVM04TM22000797 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="GEO IP" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=tcp action=Alert_Deny "FWB_Policy_Default_AutoTest" src=44.1.27.1 src_port=10000 dst=44.1.0.27 dst_port=80 http_method=none url="/autotest/test2.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Unauthorized GEO IP from United States was not allowed" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="5DF2CCDF1D3F838F5820EBC38B544CF29981" es=0 threat_weight=500 history_threat_weight=500 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Malicious" x509_cert_subject="none" owasp_api_top10="N/A"

20000021

Meaning
Custom Access rule violation

Field name	Description
`log_id`	20000021 See Log ID numbers on page 24.
`main_type`	Custom Access
`subtype`	• Predefined-Crawler • Predefined-Vulnerability Scanning • Predefined-Slow-Attack • Predefined-Content-Scraping

Examples

date=2022-07-11 time=14:46:24 log_id=20000021 msg_id=000000196980 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Custom Access" sub_type="N/A" trigger_policy="N/A" severity_level=Medium proto=tcp service=https/tls1.2 backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55622 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/test.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Custom Access rule (custom_access_rule) violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000022

Meaning

IP reputation violation.

Field name	Description
`log_id`	20000022 See Log ID numbers on page 24.
`main_type`	IP Reputation
`subtype`	• Botnet • Anonymous Proxy • Phishing • Spam • Tor • Others

Examples

date=2022-07-25 time=10:53:21 log_id=20000022 msg_id=000003643355 device_id=FVVM04TM22000797 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="IP Reputation" sub_type="Tor" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=tcp action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=185.220.100.252 src_port=10000 dst=185.220.100.10 dst_port=80 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="Bad IP triggered ip reputation category Tor" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Germany" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="23345892624CCCC3DB86B0743DD1DA7BED25" es=0 threat_weight=500 history_threat_weight=2000 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Malicious" x509_cert_subject="none" owasp_api_top10="N/A"

20000023

Meaning

Padding Oracle Attack.

Field name	Description
log_id	20000023 See Log ID numbers on page 24.
main_type	Padding Oracle
subtype	N/A

Examples
date=2022-07-11 time=15:56:44 log_id=20000023 msg_id=000000202303 device_ id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_ dayst="GMTa+7" type=attack pri=alert main_type="Padding Oracle" sub_type="N/A" trigger_ policy="N/A" severity_level=Medium proto=tcp service=http backend_service=unknown action=Alert_ Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55847 dst=10.102.0.1 dst_ port=80 http_method=get http_ url="/autotest/bruteforce/raw.html?uid=000000000000xSd8Qu5Jotox2Oyn7E0GRpGckz-uozJfKxzyZh3FlnBA6rw8JO2FlSDG5NpWAxBSAzlcKK2SfLGcYJnEuYg7n8i1LjPpC8Q=" http_ host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Padding Oracle Attack" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_ positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_ version="1.x" dev_id="none" es=0 threat_weight=100 history_threat_weight=0 threat_level=Severe ftp_ mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_ prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_ types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_ dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A02:2021-Cryptographic Failures" bot_ info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

Related

- 00040001
- 00040002
- 00040011

20000024

Meaning
CSRF Detection.

Field name	Description
log_id	20000024 See Log ID numbers on page 24.
main_type	CSRF Protection
subtype	N/A

Examples
date=2022-07-11 time=16:46:38 log_id=20000024 msg_id=000000206285 device_ id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_ dayst="GMTa+7" type=attack pri=alert main_type="CSRF Protection" sub_type="N/A" trigger_ policy="N/A" severity_level=Low proto=tcp service=https/tls1.2 backend_service=unknown action=Alert_ Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=56041 dst=10.102.0.1 dst_ port=80 http_method=get http_url="/autotest/CSRF/request_ information.php?a=100&tknfv=xx678A3E0D4EF96F744F9553D4362946C3xx" http_ host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_ id=678A3E0D4EF96F744F9553D4362946C3 msg="CSRF Detection, Token length" signature_ subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_ name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_ name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_ id="0439ABB6C35C5C0625CC4AA576110D1389FE" es=0 threat_weight=50 history_threat_ weight=150 threat_level=Substantial ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_ WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_ mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_ arg_dbid=0 ml_allow_method="none" owasp_top10="A01:2021-Broken Access Control" bot_info="none" client_level="Suspicious" x509_cert_subject="none" owasp_api_top10="N/A"

20000025

Meaning
Quarantined IPs.

Field name	Description
`log_id`	20000025 See Log ID numbers on page 24.
`main_type`	Quarantined IPs
`subtype`	N/A

Examples

date=2022-08-03 time=16:18:20 log_id=20000025 msg_id=000000271216 device_id=FV1KE4417900091 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Quarantined IPs" sub_type="N/A" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=tcp action=Alert policy="FortiWeb_Policy_Default_AutoTest" src=10.51.1.13 src_port=60500 dst=10.51.1.241 dst_port=8090 http_method=none

http_url="none" http_host="none" http_agent="none" http_session_id=none msg="FortiGate Quarantined IP- A new connection from a FortiGate Quarantined IP address 10.51.1.13:60500" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000026

Meaning

HTTP Protocol Constraints violation.

Field name	Description
`log_id`	20000026 See Log ID numbers on page 24.
`main_type`	HTTP Protocol Constraints
`subtype`	• Header Length Violation • Header Line Violation • Body Length Violation • Content Length Violation • Parameter Length Violation • HTTP Request Length Violation • URL Parameter Length Violation • Illegal HTTP Version • Cookie Number Overflow • Request Header Line number Overflow • URL Parameter Number Overflow • Illegal Hostname

Field name	Description
	• Range Header Violation • Illegal HTTP Method • Illegal Content Length • Illegal Content Type • Illegal Response Code • Missing POST Content Type • Body Parameter Length Violation • Header Name Length Violation • Header Value Length Violation • NULL Character in Parameter Name • NULL Character in Paramter Value • Illegal Header Name • Illegal Header Value • HTTP Request Filename Violation • Web Socket Protocol • Illegal Frame Type • Illegal Frame Flag • Illegal Connection Preface • HTTP/2 Header Table Size Overflow • HTTP/2 Concurrent Stream Number Overflow • HTTP/2 Initial Window Size Overflow • HTTP/2 Frame Size Overflow • HTTP/2 Header List Overflow • Illegal URL Parameter Name • Illegal URL Parameter Value • URL Parameter Name Overflow • URL Parameter Value Overflow • NULL Character in URL • Illegal Character in URL • Redundant HTTP Header • Malformed URL • Illegal Chunk Size • HTTP Parsing Error • HTTP Duplicated Parameter Name • Odd and Even Space Attack

Examples
date=2022-07-10 time=16:22:35 log_id=20000026 msg_id=000000174073 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="HTTP Protocol Constraints" sub_type="Content Length Violation" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=54443 dst=10.102.0.1 dst_port=80 http_method=post http_url="/autotest/protocalConstrait" http_host="vote3.contentlen.com.cn" http_agent="Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.2.10) Gecko/20100914 Firefox/3.6.10" http_session_id=none msg="[policy_name=FWB_protocol_constraints] : Content Length Exceeded: (The content length (1232) exceeded the maximum allowed - 1024)" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000027

Meaning
Credential stuffing defense violation.

Field name	Description
`log_id`	20000027 See Log ID numbers on page 24.
`main_type`	Credential Stuffing Defense
`subtype`	• User Tracking • Site Publish

Examples

date=2022-07-11 time=20:22:50 log_id=20000027 msg_id=000000209059 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Credential Stuffing Defense" sub_type="User Tracking" trigger_policy="N/A" severity_level=Low proto=tcp service=https/tls1.2 backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=56271 dst=10.102.0.1 dst_port=80 http_method=post http_url="/autotest/user_tracking/login.php" http_host="login.fwbqa.com" http_agent="python-for-fortiweb" http_session_id=none msg="Triggered by user pklangdon4@msn.com : Credential Stuffing Defense Violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_id="none" es=0 threat_weight=100 history_threat_weight=0 threat_level=Severe ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A02:2021-Cryptographic Failures" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000028

Meaning

User tracking rules violation.

Field name	Description
log_id	20000028 See Log ID numbers on page 24.
main_type	User Tracking
subtype	N/A

Examples

date=2022-08-03 time=16:24:04 log_id=20000028 msg_id=000000275262 device_id=FV1KE4417900002 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="User Tracking" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http action=Alert policy="FortiWeb_Policy_Default_AutoTest" src=10.200.10.100 src_port=57030 dst=10.101.0.1 dst_port=80 http_method=get http_url="/autotest/serverfarm/belonghost.html" http_host="fortinet.fortiweb.com" http_agent="python-forfortiweb" http_session_id=none msg="Triggered by user user4 : Session Timeout Enforcement" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FortiWeb_server_pool" false_positive_mitigation="none" user_name="user4" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A01:2021-Broken Access Control" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000029

Meaning

XML Validation Violation.

Field name	Description
log_id	20000029 See Log ID numbers on page 24.
main_type	XML Validation Violation
subtype	• XML Schema Validation Violation • XML Element Attribute Number Overflow • XML Element Attribute Name Length Violations • XML Element Attribute Value Length Violations • XML Element Cdata Length Violations • XML Element Depth Violations • XML Element Name Length Violations • XML External Entity Violation • XML Entity Expansion Violations • XML XInclude Violation • XML SchemaLocation Violation • XML SOAP Protocol Violation

Field name	Description
	• XML SOAPAction Violation • XML SOAP Header Violation • XML SOAP Body Violation • SOAP Signature Error • SOAP Signature Verification Error • SOAP Encryption Error • SOAP Decryption Error • WS-I Basic Profile Check • XML SOAP Attachment Violation • XML Format Violation

Examples

v012xxxxdate=2022-05-31 time=17:01:25 log_id=20000029 msg_id=000004625221 device_id=FV-1KET119900275 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="XML Validation Violation" sub_type="XML Schema Validation Violation" trigger_policy="N/A" severity_level=Medium proto=tcp service=https/tls1.2 backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=10.0.4.13 src_port=59291 dst=10.20.4.22 dst_port=80 http_method=post http_url="/testPath" http_host="172.22.6.4:8080" http_agent="none" http_session_id=none msg="XML Schema Validation Violation : Failed to validate schema schema1.xsd. Element '{http://www.w3school.com.cn}dateborn': 'aaa' is not a valid value of the atomic type 'xs:date'." signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000030

Meaning

Cookie Security violation.

Field name	Description
log_id	20000030 See Log ID numbers on page 24.
main_type	Cookie Security
subtype	• Cookie Decryption Error • Cookie Signed Verification Failed • IP replay protection violation

Examples

date=2022-07-11 time=15:42:10 log_id=20000030 msg_id=000000200949 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Cookie Security" sub_type="Cookie Signed Verification Failed" trigger_policy="N/A" severity_level=High proto=tcp service=https/tls1.2 backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55801 dst=10.102.0.1 dst_port=80 http_method=post http_url="/autotest/multicookie.php" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=678A3E0D800473935B504EC91A6BD345 msg="Cookie name (vimay), signed verification failed; [123 -> 123456]; Domain: fortinet.fortiweb.com; Path: /autotest/" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="52F6FBA6F468249C6C601733CEE796262963" es=0 threat_weight=50 history_threat_weight=50 threat_level=Substantial ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A01:2021-Broken Access Control" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000031

Meaning

FTP Command Restriction.

Field name	Description
log_id	20000031 See Log ID numbers on page 24.

Field name	Description
main_type	FTP Command Restriction
subtype	N/A

Examples

date=2022-08-03 time=16:39:48 log_id=20000031 msg_id=000000259165 device_id=FV1KE4417900002 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="FTP Command Restriction" sub_type="N/A" trigger_policy="N/A" severity_level=High proto=tcp service=ftp action=Alert policy="FortiWeb_FTP_Policy" src=10.200.10.100 src_port=59713 dst=10.200.10.114 dst_port=21 http_method=RETR http_url="none" http_host="none" http_agent="none" http_session_id=none msg="FTP command RETR is Illegal command type" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="vimay2" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="Passive" ftp_cmd="RETR /123.txt" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000033

Meaning

Session was timed out.

Field name	Description
log_id	20000033 See Log ID numbers on page 24.
main_type	Timeout Session
subtype	N/A

Examples

date=2022-08-03 time=16:52:14 log_id=20000033 msg_id=000034295233 device_id=FV3K1E3216000005 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Timeout Session" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=tcp action=Alert_Deny policy="FortiWeb_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=51347 dst=10.114.0.1 dst_port=80 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="Received 0 byte since this connection established" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000035

Meaning

FTP File Security violation.

Field name	Description
`log_id`	20000035 See Log ID numbers on page 24.
`main_type`	FTP File Security
`subtype`	• FTP Antivirus Detection • FTP FortiSandbox Detection

Examples

date=2022-08-03 time=16:57:56 log_id=20000035 msg_id=000007146026 device_id=FV1KE4417900002 vd="adomain_new" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="FTP File Security" sub_type="FTP Antivirus Detection" trigger_policy="N/A" severity_level=Medium proto=tcp service=ftp backend_service=ftp action=Alert policy="FortiWeb_FTP_Policy" src=10.200.10.200 src_port=56714 dst=10.200.10.114 dst_port=49655 http_method=STOR http_url="none" http_host="none" http_agent="none" http_session_id=none msg="filename [level3.zip] virus name [Jerusalem.2080]: FTP file security virus violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="vimay2" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="Passive" ftp_cmd="STOR /level3.zip" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000036

Meaning

FTPS connection failure.

Field name	Description
log_id	20000036 See Log ID numbers on page 24.
main_type	FTPS Connection Failure
subtype	N/A

Examples

date=2022-08-03 time=18:03:01 log_id=20000036 msg_id=000000345704 device_id=FV1KE4417900002 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="FTPS Connection Failure" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=ftps action=Alert_Deny policy="FortiWeb_FTP_Policy" src=10.200.10.100 src_port=58278 dst=10.200.10.114 dst_port=21 http_method=AUTH http_url="none" http_host="none" http_agent="none" http_session_id=none msg="SSL Error(1070) - tlsv1 alert protocol version" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="Positive" ftp_cmd="AUTH /" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000037

Meaning

Machine Learning anomaly detection violation.

Field name	Description
`log_id`	20000037 See Log ID numbers on page 24.
`main_type`	Machine Learning
`subtype`	• Anomaly in HTTP argument • HTTP Method violation • Charset detect failed

Examples

date=2019-08-03 time=18:03:01 log_id=20000036 msg_id=000000345704 device_id=FV1KE4417900002 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="FTPS Connection Failure" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=ftps action=Alert_Deny policy="FortiWeb_FTP_Policy" src=10.200.10.100 src_port=58278 dst=10.200.10.114 dst_port=21 http_method=AUTH http_url="none" http_host="none" http_agent="none" http_session_id=none msg="SSL Error(1070) - tlsv1 alert protocol version" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FTP_ServerPool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="Positive" ftp_cmd="AUTH /" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000038

Meaning

OpenAPI validation violation.

Field name	Description
`log_id`	20000038 See Log ID numbers on page 24.
`main_type`	Openapi Validation Violation
`subtype`	• Openapi Query Parameter Violation • Openapi Path Parameter Violation • Openapi Cookie Parameter Violation • Openapi Header Parameter Violation • Openapi Request Body Violation

Examples
date=2022-07-11 time=20:47:03 log_id=20000038 msg_id=000000211730 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Openapi Validation Violation" sub_type="Openapi Header Parameter Violation" trigger_policy="N/A" severity_level=Low proto=tcp service=https/tls1.2 backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=56389 dst=10.102.0.1 dst_port=80 http_method=get http_url="/inheader/requiredfalse/false?pid=30" http_host="www.openapi.io" http_agent="python-for-fortiweb" http_session_id=none msg="API Validation violation - Header parameter "X-FWB-HEADER" validation failure : Failed to validate schema in-header-required-false-type-boolen.yaml" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000039

Meaning
WebSocket security violation.

Field name	Description
`log_id`	20000039 See Log ID numbers on page 24.
`main_type`	WebSocket Security
`subtype`	• Disallow WebSocket • Disallow Extensions • Illegal Format • Illegal Frame Size • Illegal Message Size • Disallow Origin • Parse error

Examples

date=2022-07-10 time=18:02:38 log_id=20000039 msg_id=000000180727 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="WebSocket Security" sub_type="Illegal Format" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=54731 dst=10.159.27.200 dst_port=8081 http_method=get http_url="/autotest/input_rule/1.html" http_host="192.168.1.228:8090" http_agent="none" http_session_id=none msg="[policy_name=websocketsecurityPolicy] : WebSocket Disallow Plain Format" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000040

Meaning

MiTB AJAX security violation.

Field name	Description
log_id	20000040 See Log ID numbers on page 24.
main_type	MiTB AJAX Security
subtype	N/A

Examples

date=2022-08-03 time=18:27:55 log_id=20000040 msg_id=000034369491 device_id=FV3K1E3216000005 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="MiTB AJAX Security" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=http action=Alert policy="FortiWeb_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=51426 dst=10.114.0.1 dst_port=80 http_method=get http_url="http://10.200.10.210:91/autotest/cors.html" http_host="10.114.0.1" http_agent="Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0" http_session_id=none msg="MITB AJAX Detection" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FortiWeb_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="http://10.114.0.1/autotest/mitb/ajax/ajax_cors.html" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000041

Meaning

Machine learning bot detection violation.

Field name	Description
log_id	20000041 See Log ID numbers on page 24.
main_type	Bot Detection
subtype	N/A

Examples

date=2022-08-03 time=18:33:15 log_id=20000041 msg_id=000034371543 device_id=FV3K1E3216000005 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Bot Detection" sub_type="N/A" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=tcp action=Alert policy="FortiWeb_Policy_Default_AutoTest_ttp" src=10.114.0.102 src_port=53734 dst=10.114.0.1 dst_port=80 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="Bot Verification failed (Real Browser Enforcement)" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="none" es=0 threat_weight=10 history_threat_weight=0 threat_level=Medium ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="{"dimen_count": 13, "boxplot_info": [{"id": 1, "value": [1.00, 1.00, 1.00]}, {"id": 2, "value": [1.00, 2.00, 2.00]}, {"id": 3, "value": [0.00, 0.00, 0.00]}, {"id": 4, "value": [0.00, 0.00, 0.00]}, {"id": 5, "value": [1.00, 1.00, 1.00]}, {"id": 6, "value": [0.00, 0.00, 0.00]}, {"id": 7, "value": [0.00, 0.00, 0.00]}, {"id": 8, "value": [1.00, 1.00, 1.00]}, {"id": 9, "value": [0.00, 0.00, 0.00]}, {"id": 10, "value": [0.00, 0.00, 0.00]}, {"id": 11, "value": [0.00, 0.00, 0.00]}, {"id": 12, "value": [1.00, 1.00, 2.00]}, {"id": 13, "value": [1.00, 1.00, 1.00]}], "vector": [100.00,100.00,0.00,0.00,100.00,0.00,0.00,100.00,0.00,0.00,0.00,2.00,2.00]}" client_level="Unidentified" x509_cert_subject="none"

20000042

Meaning

CORS check security violation.

Field name	Description
`log_id`	20000042 See Log ID numbers on page 24.
`main_type`	CORS Check Security
`subtype`	• Invalid Origin • Disallow CORS • Disallow Origin • Disallow method • Disallow header

Examples

date=2022-07-11 time=16:04:35 log_id=20000042 msg_id=000000203639 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="CORS Check Security" sub_type="Disallow Origin" trigger_policy="N/A" severity_level=Low proto=tcp service=https/tls1.2 backend_service=unknown action=Return_403_error policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55905 dst=10.102.0.1 dst_port=91 http_method=get http_url="/autotest/test.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="[policy_name=Fwb_Cors_Policy] : Origin http://123.com is not allowed" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_id="none" es=0 threat_weight=25 history_threat_weight=0 threat_level=Moderate ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000043

Meaning

JSON validation security violation.

Field name	Description
`log_id`	20000043 See Log ID numbers on page 24.
`main_type`	JSON Validation Security
`subtype`	• JSON Schema Validation Violation • JSON Format Invalid Violation • JSON Data Size Violation • JSON Key Size Violation • JSON Key Number Violation • JSON Value Size Violation • JSON Value Number Violation • JSON Value Number in Array Violation • JSON Object Depth Violation

Examples
date=2022-07-11 time=16:20:59 log_id=20000043 msg_id=000000204954 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="JSON Validation Security" sub_type="JSON Data Size Violation" trigger_policy="N/A" severity_level=Low proto=tcp service=https/tls1.2 backend_service=unknown action=Alert policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55959 dst=10.102.0.1 dst_port=80 http_method=post http_url="/autotest/server_protection/1.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="[rule_name = FWB_json_protection_rule] : JSON Data Size Exceeded:(The json data size 1048 Bytes exceeded the maximum allowed - 1024 Bytes)" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="2.0" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000045

Meaning
BOT Deception violation.

Field name	Description
log_id	20000045 See Log ID numbers on page 24.
main_type	BOT Deception
subtype	N/A

Examples

date=2022-07-05 time=15:13:14 log_id=20000045 msg_id=000000154919 device_id=FVVM08TM21000756 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="BOT Deception" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=52058 dst=10.102.0.1 dst_port=80 http_method=get http_url="/test/test.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Bot Deception" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

20000046

Meaning

BOT Biometrics Based Detection violation.

Field name	Description
log_id	20000046 See Log ID numbers on page 24.
main_type	Biometrics Based Detection
subtype	N/A

Examples

date=2022-07-10 time=22:19:10 log_id=20000046 msg_id=000000186089 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Biometrics Based Detection" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=13.52.123.123 src_port=55053 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/bot_test.html" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Biometrics Based Detection: 13.52.123.123 is a bot due to lack of Mouse Movement, matched URL /autotest/bot_test.html" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000047

Meaning

BOT Threshold Based Detection violation.

Field name	Description
log_id	20000047 See Log ID numbers on page 24.
main_type	Threshold Based Detection
subtype	N/A

Examples

date=2022-07-10 time=18:29:39 log_id=20000047 msg_id=000000184735 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Threshold Based Detection" sub_type="N/A" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=http action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=13.52.123.123 src_port=54959 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/condition_404.php?404=true" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="Threshold Based Crawler Detection (threshold_based_Detection) violation" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=0 history_threat_weight=0 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000051

Meaning

Known Bots Detection violation.

Field name	Description
log_id	20000051 See Log ID numbers on page 24.
main_type	Known Bots Detection
subtype	N/A

Examples

date=2022-07-10 time=22:41:04 log_id=20000051 msg_id=000000188855 device_id=FVVM08TM21000756 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Known Bots Detection" sub_type="DoS" trigger_policy="N/A" severity_level=High proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=55138 dst=10.102.0.1 dst_port=80 http_method=get http_url="/autotest/test1.html" http_host="fortinet.fortiweb.com" http_agent="Yoyo-DDoS" http_session_id=none msg="Known Bots triggered Malicious Bot Yoyo-DDoS in category DoS of Known Bots policy FWB_know-bots_policy" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=200 history_threat_weight=0 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Unidentified" x509_cert_subject="none" owasp_api_top10="N/A"

20000052

Meaning

Client Management violation.

Field name	Description
log_id	20000052 See Log ID numbers on page 24.
main_type	Client Management
subtype	N/A

Examples

date=2022-07-05 time=16:54:11 log_id=20000052 msg_id=000001005386 device_id=FVVM04TM21000545 vd="root" timezone="(GMT+1:00)Brussels,Copenhagen,Madrid,Paris" timezone_dayst="GMTc-2" type=attack pri=alert main_type="Client Management" sub_type="N/A" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Period_Block policy="port1-HPC" src=44.1.28.1 src_port=10031 dst=10.20.128.42 dst_port=80 http_method=post http_url="/index.php" http_host="44.1.0.28" http_agent="Firefox/62.0" http_session_id=none msg="IP 44.1.28.1 has been period blocked for 1 minute(s) because of exceeded threat score limit." signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="128" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="511852CB0D52A82F2BFB255587FD2DF7D9CB" es=0 threat_weight=0 history_threat_weight=1996 threat_level=Off ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Malicious" x509_cert_subject="none" owasp_api_top10="N/A"

20000053

Meaning

IP not in allow only list was blocked.

Field name	Description
log_id	20000053 See Log ID numbers on page 24.
main_type	Allow Only IP List
subtype	N/A

Examples

date=2022-07-30 time=14:32:39 log_id=20000053 msg_id=000003687260 device_id=FVVM04TM22000797 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" timezone_dayst="GMTa+7" type=attack pri=alert main_type="Allow Only IP List" sub_type="N/A" trigger_policy="N/A" severity_level=Medium proto=tcp service=http backend_service=tcp action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=44.1.3.2 src_port=10000 dst=44.1.0.5 dst_port=80 http_method=none http_url="none" http_host="none" http_agent="none" http_session_id=none msg="IP not in allow only list was blocked" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="United States" content_switch_name="none" server_pool_name="none" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="Unknown" dev_id="5E2C970F726EB67694A96F208781046D7F71" es=0 threat_weight=500 history_threat_weight=500 threat_level=Critical ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="N/A" bot_info="none" client_level="Malicious" x509_cert_subject="none" owasp_api_top10="N/A"

20000054

Meaning

Web Shell Detection violation.

Field name	Description
`log_id`	20000054 See Log ID numbers on page 24.
`main_type`	Web Shell Detection
`subtype`	• Fuzzy Web Shell Detection • Known Web Shell Detection

Examples

date=2022-07-05 time=16:24:05 log_id=20000054 msg_id=000000157502 device_id=FVVM08TM21000756 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" timezone_dayst="GMTa-8" type=attack pri=alert main_type="Web Shell Detection" sub_type="Fuzzy Web Shell Detection" trigger_policy="N/A" severity_level=Low proto=tcp service=http backend_service=unknown action=Alert_Deny policy="FWB_Policy_Default_AutoTest" src=192.168.1.8 src_port=52167 dst=10.102.0.1 dst_port=80 http_method=post http_url="/autotest/upload/upload.php" http_host="fortinet.fortiweb.com" http_agent="python-for-fortiweb" http_session_id=none msg="File [PHP.Agent.b53eda3] matched web shell [PHP-PHP.Agent.b53eda3](100%)" signature_subclass="N/A" signature_id="N/A" signature_cve_id="N/A" srccountry="Reserved" content_switch_name="none" server_pool_name="FWB_server_pool" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refer="none" http_version="1.x" dev_id="none" es=0 threat_weight=100 history_threat_weight=0 threat_level=Severe ftp_mode="N/A" ftp_cmd="N/A" cipher_suite="none" ml_log_hmm_probability=0.000000 ml_log_sample_prob_mean=0.000000 ml_log_sample_arglen_mean=0.000000 ml_log_arglen=0 ml_svm_log_main_types=0 ml_svm_log_match_types="none" ml_svm_accuracy="none" ml_domain_index=0 ml_url_dbid=0 ml_arg_dbid=0 ml_allow_method="none" owasp_top10="A05:2021-Security Misconfiguration" bot_info="none" client_level="Unidentified" x509_cert_subject="none"

Traffic

Traffic log messages record requests that a FortiWeb policy accepted or blocked. If the request was successful, it also includes the reply. Each log message represents its whole HTTP transaction.

Traffic logs do **not** record non-HTTP/HTTPS traffic such as FTP. This type of traffic is forwarded to your web servers if you have enabled IP-layer forwarding.

Traffic log messages are described below. For descriptions of header fields not mentioned here, see Header & body fields on page 14.

Meaning
Traffic matching and complying with a policy passed through or by FortiWeb. If there is an error in the message and the request/response used HTTPS, FortiWeb could not scan it. Depending on the mode of operation, an attack could have bypassed FortiWeb.

Solution
Response times can often be improved by regular expression tuning, offloading SSL/TLS from your back-end server to your FortiWeb (especially if the model supports hardware acceleration), and/or offloading compression. For performance tips, see the *FortiWeb Administration Guide*. If HTTPS traffic is not flowing as you expect or not being inspected, and you have recently enabled HTTPS, typically this is due to a misconfiguration. The error message in the `msg` field will indicate the appropriate solution: • `No Server Certificate for SSL Connection` — FortiWeb does not have the server certificate, so it cannot decode the SSL traffic. To fix this, upload the web server's certificate to FortiWeb. • `SSL Certificate Key Mismatch` — An X.509 server certificate was uploaded to FortiWeb, but its private key did not match the one used by this HTTPS session. To fix this, upload the back-end web server's current certificate. • `Ephemeral keys cannot be decrypted` — Ephemeral Diffie-Hellman key exchange can't be inspected due to the property of perfect forward secrecy, which makes real-time HTTPS inspection impossible. To fix this, disable ephemeral Diffie-Hellman on the back-end web server, and select a different key exchange method. • `Unsupported Cipher for SSL Connection` — Either message digest (MAC) authentication failed or the MAC did not exist, or the transaction used an unsupported cipher suite. To fix this, on the back-end web server, disable cipher suites that are not supported by FortiWeb. • `Unmonitored SSL Connection` — The HTTPS session was initiated before FortiWeb was deployed or before the server policy was enabled, so FortiWeb could not listen for the key exchange, and therefore cannot decrypt subsequent requests/responses in this HTTPS session. To fix this, on the back-end web server, clear HTTPS sessions and force clients to renegotiate. If FortiWeb is operating in Reverse Proxy or True Transparent Proxy mode, the traffic was blocked and no attack could have passed through to your protected web servers. **No action is required except to make sure that you have uploaded to FortiWeb the correct certificate for all protected web servers.** Otherwise, if your appliance was: • operating in Offline Protection or Transparent Inspection mode **or** • configured only to **monitor** traffic (e.g. **Monitor Mode** was enabled or the **Action** is **Alert**, not **Alert & Deny**)

Solution
examine the web server to determine whether or not an encrypted attack has passed through. You should also examine your web server's HTTPS configuration and disable cipher suites and key exchanges that are not supported by FortiWeb so that during negotiation with clients, your web server does not agree to use encryption that FortiWeb cannot scan for attacks. By the nature of log-only actions, detected attack attempts are logged but **not** blocked. You may also want to determine if the attack is from a single source IP address or distributed: blocklisting an offending client may help you to efficiently prevent further attack attempts, improving performance, until you can take further action. By the nature of the network topology for Offline Protection mode (which can potentially cause differences in speeds of the separate routing paths), and asynchronous inspection for Transparent Inspection mode, **blocking cannot be guaranteed and some key exchanges are not supported**. For details, see the *FortiWeb Administration Guide*.

Field name	Description
ID (`log_id`)	`30000000` All traffic log messages share the same ID (`log_id=30000000`). See Log ID numbers on page 24.
Sub Type (`subtype`)	`HTTP` All traffic log messages share the same subtype (`subtype=HTTP`). See Subtypes on page 25.
Level (`pri`)	`notification` See Priority level on page 25.
Message (`msg`)	If the HTTP request triggered the FortiWeb web caching feature, the message begins with `[Replied by Cache].` The HTTP/HTTPS request's: • method • IP layer source and destination address and port numbers (IPv6 addresses are surrounded by square brackets to better demarcate the port number, e.g. `[2001:470:19:ad7:6::230]:443`) such as: • `HTTP` **GET** `request from 10.0.2.5:8239 to 10.0.2.1:443` • `HTTP` **POST** `request from 10.0.2.5:8100 to 10.0.2.1:80` If the transaction used HTTPS, and there was an error when either decoding it or participating in the handshake, there may be an error message instead of the HTTP method, such as: `HTTP request from 192.0.2.1:40170 to 10.0.2.1:443`, **Ephemeral keys cannot be decrypted**
Source Country (`srccountry`)	The country that is the source of the traffic.
HTTP Content Routing (`content_switch_name`)	The name of the associated HTTP content routing policy.

Field name	Description
Server Pool Name (`server_pool_name`)	The name of the server pool in the associated server policy.

Examples
date=2014-06-26 time=00:43:37 log_id=30000000 msg_id=000001351251 device_id=FV-1KD3A14800059 vd="root" timezone="(GMT-8:00)Pacific Time(US&Canada)" type=traffic subtype="HTTP" pri=notice proto=tcp service=HTTP status=success reason=none policy=Auto-policy src=10.0.8.103 src_port=8142 dst=10.20.8.22 dst_port=80 HTTP_request_time=0 HTTP_response_time=0 HTTP_request_bytes=444 HTTP_response_bytes=401 HTTP_method=get HTTP_url="/" HTTP_host="10.0.8.22" HTTP_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; " HTTP_retcode=200 msg="HTTP GET request from 10.0.8.103:8142 to 10.20.8.22:80" srccountry="Reserved" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
date=2014-04-11 time=09:26:22 log_id=30000000 msg_id=000000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="HTTP" pri=notification proto=tcp service=HTTPs status=success reason="none" policy="policy1" src=172.20.120.47 src_port=53817 dst=172.20.120.47 dst_port=80 HTTP_request_time=18 HTTP_response_time=1 HTTP_request_bytes=464 HTTP_response_bytes=3060 HTTP_method=get HTTP_url="/index" HTTP_host="172.20.120.48" HTTP_agent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" HTTP_retcode=**200** msg="HTTPS **GET** request from 172.20.120.47:53817 to 172.20.120.47:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"
date=2014-04-11 time=10:16:29 log_id=30000000 msg_id=000000000230 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="HTTP" pri=notification proto=tcp service=HTTP status=success reason="none" policy="policy1" src=172.20.120.46 src_port=49234 dst=172.20.120.48 dst_port=80 HTTP_request_time=0 HTTP_response_time=0 HTTP_request_bytes=257 HTTP_response_bytes=0 HTTP_method=get HTTP_url="/admin" HTTP_host="172.20.120.48" HTTP_agent="Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)" HTTP_retcode=**500** msg="HTTP **POST** request from 172.20.120.46:49234 to 172.20.120.48:80 " srccountry="United States" content_switch_name="testa" server_pool_name="Auto-ServerFarm"