



FortiWeb™ Web Application Firewall

Version 4.0 MR2
Log Message Reference
Revision 1

FORTINET.

FortiWeb™ Web Application Firewall Log Message Reference

Version 4.0 MR2

Revision 1

29 March 2011

© Copyright 2011 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiWeb, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS



Caution: Risk of explosion if the battery on the main board is replaced by an incorrect type. Dispose of used batteries according to instructions.



Caution: The Fortinet equipment is intended for installation in a Restricted Access Location.

Contents

Introduction	11
Before you begin	11
How this log reference is organized	11
Document conventions	11
IP addresses	12
Cautions, Notes and Tips	12
Typographical conventions.	12
Registering your Fortinet product.	13
Customer service and technical support	13
Training	13
Fortinet documentation	13
Tools and Documentation CD	13
Fortinet Knowledge Base	13
Comments on Fortinet technical documentation	14
FortiWeb logging overview	15
Anatomy of a FortiWeb log message.	15
log_id field	16
msg_id field.	17
Log message syntax	17
Event log message syntax	17
Attack log message syntax	17
Traffic log message syntax	17
Log message field descriptions	17
Log types	19
Log subtypes	20
Log priority level	22
Event logs - 01	23
System	25
Administrator logs	25
30000	25
30001	26
30002	26
Auto update logs	27
30005	27
30006	27
30007	28
30008	28
30009	29
30010	29

30011	30
30012	30
30013	31
30014	31
30015	32
Certificate - CA logs	32
30020	32
30021	33
Certificate - CA group logs	33
30025	33
30026	34
30027	34
Certificate - CRL logs	35
30030	35
30031	35
30032	36
Certificate - Intermediate CA logs	36
30035	36
30036	37
Certificate - Intermediate CA group logs	37
30040	37
30041	38
30042	38
Certificate - Local logs	39
30045	39
30046	39
30047	40
30048	40
Certificate - Remote logs	41
30050	41
30051	41
Certificate - verify logs	42
30055	42
30056	42
30057	43
DNS logs	43
30060	43
DOS protection logs	44
30065	44
30066	44
HA-config logs	45
30070	45
RAID logs	45
30080	45
SNMP logs	46

30090	46
Vzone logs	46
30095	46
30096	47
30097	47
Admin	48
Access profile logs	48
31000	48
31001	48
31002	49
Backup and restore logs	49
31005	49
31006	50
Fail-open logs	50
31010	50
Interface logs	51
31015	51
31016	51
31017	52
31018	52
Mode of operation logs	53
31020	53
Settings logs	53
31025	53
31026	54
31027	54
Status logs	55
31030	55
31031	55
31032	56
31033	56
System time logs	57
31035	57
Update signature logs	57
31040	57
31041	58
Web Site with Anti-Defacement logs	58
31045	58
31046	59
31047	59
HA	60
HA logs	60
32000	60
Router	61
Route logs	61

33000	61
33001	61
33002	62
User.	62
LDAP user logs.	62
34000	62
34001	63
34002	63
Local user logs	64
34005	64
34006	64
34007	65
NTLM user logs	65
34010	65
34011	66
34012	66
User group logs	67
34015	67
34016	67
34017	68
Policy	68
Data type group logs	68
35000	68
35001	69
35002	69
Physical Server logs	70
35005	70
35006	70
35007	71
Policy logs	71
35010	71
35011	72
35012	72
Protected server logs.	73
35015	73
35016	73
35017	74
Server farm logs	74
35020	74
35031	75
35022	75
Server health check logs	76
35025	76
35026	76

35027	77
Service logs	77
35030	77
35031	78
35032	78
Suspicious URL rule logs.	79
35035	79
35036	79
35037	80
Virtual server logs	80
35040	80
35041	81
35042	81
Protection	82
Allow method exception logs	82
36000	82
36001	82
36002	83
Authentication rule logs	83
36005	83
36006	84
36007	84
Authentication policy logs	85
36010	85
36011	85
36012	86
Auto learning profile logs	86
36015	86
36016	87
36017	87
Brute force login logs	88
36020	88
36021	88
36022	89
Custom data type logs	89
36025	89
36026	90
36027	90
Custom protection group logs	91
36030	91
Custom protection rule logs	91
36035	91
36036	92
36037	92
Custom robot logs	93
36040	93

36041	93
36042	94
Suspicious URL rule logs.	94
36045	94
36046	95
36047	95
Custom suspicious URL logs.	96
36050	96
36051	96
36052	97
Custom suspicious URL rule logs	97
36055	97
36056	98
36057	98
Hidden fields protection logs	99
36060	99
36061	99
36062	100
Hidden fields rule logs	100
36065	100
36066	101
36067	101
HTTP protocol constraint logs	102
36070	102
36071	102
36072	103
Inline protection profile logs	103
36075	103
36076	104
36077	104
Input rule logs	105
36080	105
36081	105
36082	106
IP blacklist logs.	106
36085	106
36086	107
36087	107
IP trust list logs	108
36090	108
36091	108
36092	109
Offline protection profile logs	109
36095	109
36096	110

36097	110
Page access rule logs	111
36100	111
36101	111
36102	112
Parameter validation rule logs	112
36105	112
36106	113
36107	113
Robot control logs	114
36110	114
36111	114
36112	115
Robot group logs	115
36115	115
36116	116
36117	116
Server protection exception logs	117
36120	117
Server protection rule logs	117
36125	117
36126	118
36127	118
Start page logs	119
36130	119
36131	119
36132	120
URL access policy logs	120
36135	120
36136	121
36137	121
URL access rule logs	122
36140	122
36141	122
36142	123
URL rewriting policy logs	123
36145	123
URL rewriting rule logs	124
36150	124
Web vulnerability scan policy logs	124
36155	124
36156	125
36157	125
Web vulnerability scan profile logs	126
36160	126
36161	126

36162	127
Web vulnerability scan schedule logs	127
36165	127
36166	128
36167	128
Attack logs - 04	129
Attack log message content	133
Traffic - 00	135
Traffic log message content	135

Introduction

This reference provides detailed information about all log messages that are recorded by the FortiWeb unit. It is intended for administrators that are already logging FortiWeb features and require information about a specific log message that was recorded.

This chapter includes the following topics:

- [Before you begin](#)
- [Document conventions](#)
- [Registering your Fortinet product](#)
- [Customer service and technical support Training](#)
- [Fortinet documentation](#)

Before you begin

Before you begin using this guide, take a moment to note the following:

- The information in this reference applies to all FortiWeb units and models running FortiWeb v4.0 MR2 and higher application software.
- You have enabled logging of FortiWeb features. If you have not chosen a log device, or have not enabled logging of FortiWeb features, see the Log & Report chapter in the *FortiWeb 4.0 MR2 Administration Guide*.
- Each log message is written similarly to how it appears in the log access table, based on the Formatted view.
- This reference contains detailed information for each log message field; however, this reference contains only information gathered at publication and as a result, not every log message field contains detailed information. More detailed information will be available in future releases of this reference.

How this log reference is organized

This document describes what log messages are recorded by the FortiWeb unit. This document contains the following chapters:

- [FortiWeb logging overview](#)
- [Event logs - 01](#)
- [Attack logs - 04](#)
- [Traffic - 00](#)

[FortiWeb logging overview](#) provides an overview of the composition of FortiWeb logs, and a detailed example explaining the different fields within a log message.

The remainder of the chapters describe each log message generated by FortiWeb, grouped by log type and subtype.

Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.



Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.



Note: Presents useful information, usually focused on an alternative, optional method, such as a shortcut, to perform a step.



Tip: Highlights useful additional information, often tailored to your workplace activity.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input*	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are not secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <code>VPN > IPSEC > Auto Key (IKE)</code> .
Publication	For details, see the FortiGate Administration Guide . Note: Links typically go to the most recent version. To access earlier releases, go to http://docs.fortinet.com/ . This link appears at the bottom of each page of this document.

Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article [What does Fortinet Technical Support require in order to best assist the customer?](#)

Training

Fortinet Training Services provides a variety of training programs to serve the needs of our customers and partners world-wide. Visit the Fortinet Training Services web site at <http://training.fortinet.com>, or email training@fortinet.com.

Fortinet documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Tools and Documentation CD

The documentation for your product is available on the Fortinet Tools and Documentation CD shipped with your product. The documents on this CD are current at shipping time. For the most current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

FortiWeb logging overview

FortiWeb has logging and reporting functions that provide historical and current analysis of network activity. This section explains the composition of FortiWeb log messages. Other sections in this document provide information about the specific log messages generated by FortiWeb.

The topics covered in this section include:

- [Anatomy of a FortiWeb log message](#)
- [Log types](#)
- [Log subtypes](#)
- [Log priority level](#)

For detailed information about configuring, viewing, managing and generating FortiWeb log messages and reports, see the Log & Report chapter in the *FortiWeb Administration Guide*. The FortiWeb Administration Guide is located on the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

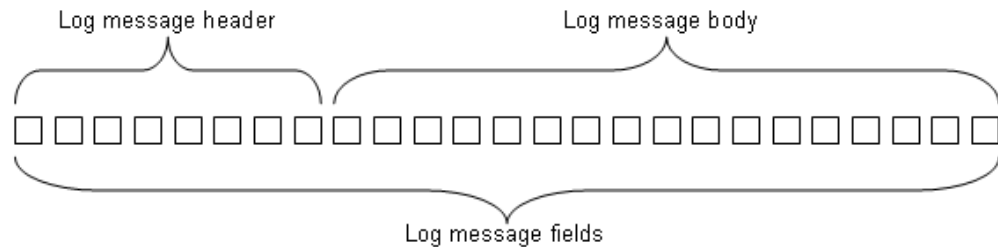
Anatomy of a FortiWeb log message

FortiWeb log message provide detailed information on network activity that helps identify system and security issue, reducing network misuse and abuse.

For a description of each field in a log message, see [Table 2 on page 18](#).

Log messages are composed of a number of fields. The fields are organized into two parts: a message header and a message body.

Figure 1: Log message anatomy



The log message header includes general information about the log message itself, including: the time and date the log originated, a log identifier, a message identifier, the type of log, the priority level and where the log message originated. The fields that comprise the log message header are the same for every log.

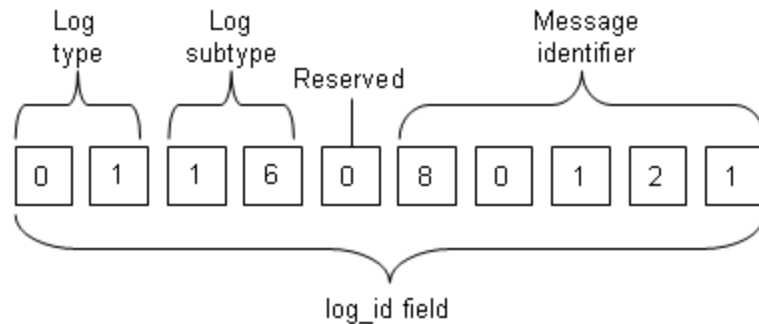
The log message body fields describe the specific situation for which the log was created, including the reason that the activity was recorded and details about the activity. The fields that comprise the log message body vary according to log type.

log_id field

The **log_id** is a 10-digit field located in the log message header, immediately following the time and date fields. The log_id field has a static numbering sequence that uniquely identifies each individual log message. Understanding the composition of the log_id field will simplify identification of log message and the situations they represent.

Figure 2 on page 16 illustrates the composition of the log_id field.

Figure 2: log_id field



The log_id field provides the following information:

- the first two digits represent the **log type**.
 - 00 = traffic logs
 - 01 = event logs
 - 04 = attack logs
- the second two digits represent the **log subtype**
 - 00 = accept traffic subtype
 - 01 = deny traffic subtype
 - 10 = system event subtype
 - 11 = admin event subtype
 - 12 = HA event subtype
 - 13 = router event subtype
 - 14 = user event subtype
 - 15 = policy event subtype
 - 16 = protection event subtype
 - 20 thru 60 = attack subtypes
- the fifth digit is reserved for future use and is always set to 0 (zero)
- the last five digits form a **message identifier**. A defined range of numbers is assigned to each subtype, and a static number within that range is associated with each message
 - 10000 = traffic log messages
 - 20000 = attacks logs
 - 30000 = event messages

msg_id field

The msg_id field is an incremental 12-digit number assigned to each individual log message generated by the FortiWeb unit. The msg_id number is unique to each log message, and is used only for administration and management of log message data.

Log message syntax

Below are examples showing the syntax of event, attack and traffic log messages. Depending on the method used to view the log messages, the message is presented in raw format, typically used for download, or formatted into columns for display in FortiWeb web-based management tool.

In these examples, the log message header is shown in `plain` typeface, and the log message body in ***bold-italic*** typeface.

Event log message syntax

Example event log, in raw format.

```
date=2010-08-16 time=17:30:23 log_id=0104012345 type=event subtype=admin
pri=information msg_id=000044866169 device_id=FV1AA2B34567890 timezone="(GMT-12:00)Eniwetok,Kwajalein"
user=admin ui=GUI(10.0.0.22) action=login
status=success reason=none msg="User admin login successfully from
GUI(10.0.0.22)"
```

Attack log message syntax

Example attack log, in raw format.

```
date=2010-08-12 time=14:02:00 log_id=0430067890 type=attack
subtype=waf_common_exploits pri=alert msg_id=000044866169
device_id=FV1AA2B34567890 timezone="(GMT-12:00)Eniwetok,Kwajalein"
proto=tcp service=http src=10.0.0.33 src_port=59474 dst=10.0.0.11 dst_port=80
policy=1 action=alert http_method=get http_url="/" http_host="10.0.0.11"
http_agent="Wget/1.10.2 (Red Hat modified)" http_session_id=unknown
severity_level=1 trigger_policy=xhwang msg="Common Exploits: Command
Injection"
```

Traffic log message syntax

Example traffic log, in raw format.

```
date=2010-08-12 time=14:02:00 log_id=0090024680 type=traffic
subtype=accept pri=notice msg_id=000044866169
device_id=FV1AA2B34567890 timezone="(GMT-12:00)Eniwetok,Kwajalein"
proto=tcp service=http src=10.0.0.33 src_port=59474 dst=10.0.0.11 dst_port=80
policy=1 action="alert" http_host="10.0.0.11" http_agent="Wget/1.10.2 (Red Hat
modified)" http_url="/" attack_type="" msg="HTTP request from 10.0.0.33:59474 to
10.0.0.11:80 ,protocol:HTTP"
```

Log message field descriptions

[Table 2 on page 18](#) describes each of the fields that comprise a FortiWeb log message and identifies the log type for which the field is used. The table also includes an example of the raw data associated with each field.

Table 2: Log message field description

Field name	Field description	Used in log type			Field example (raw format)
		Event	Attack	Traffic	
Log message header					
date	The date that the log message was recorded.	x	x	x	2010-09-03
time	The time that the log message was recorded.	x	x	x	15:38:01
log_id	A 10-digit number that identifies the log message. The log message number consists of: <ul style="list-style-type: none"> the first two digits represent the log type. See Table 3 on page 20 the second two digits represent the log subtype. See Table 4 on page 20 the fifth digit is reserved for future use and is always set to 0 (zero) the last five digits is a static identifier assigned to each individual log message. 	x	x	x	log_id=0116080121
msg_id	A unique 12-digit number assigned to each individual log message generated by the FortiWeb unit.	x	x	x	msg_id=000044866169
type	The type of log that occurred: event, attack or traffic. See Table 3 on page 20 .	x	x	x	type=event type=attack type=traffic
subtype	The log subtype, which provides additional information to identify the cause of the log message. See Table 4 on page 20 .	x	x	x	subtype=waf_information
pri	The log priority level (log level) associated with the situation for which the log message was created. See Table 5 on page 22	x	x	x	pri=alert
device_id	The identification number of the device from which the log message originated.	x	x	x	device_id=FV-1AA2B34567890
timezone	The timezone in which the device is located.	x	x	x	timezone="(GMT-5:00)Eastern Time(US & Canada)"
Log message body					
user	The login name of the user that performed the action that caused the event log to be created.	x			user=admin
ui	The type of user interface used when the log was created.	x			ui=GUI(10.0.0.22)

Table 2: Log message field description

Field name	Field description	Used in log type			Field example (raw format)
		Event	Attack	Traffic	
action	The action associated with the log.	x			action=login
status	The result of the action.	x			status=failure
reason	The reason for the status.	x			reason=name_invalid
proto	The protocol used by the web traffic		x	x	proto=tcp
service	The IP network service that defines the TCP port number on which the virtual server receives traffic.		x	x	service=http
src	The web traffic source IP address.		x	x	src=10.0.0.0
src_port	The web traffic source port number.		x	x	src_port=3471
dst	The web traffic destination IP address.		x	x	dst=10.0.0.1
dst_port	The web traffic destination port number.		x	x	dst_port=8080
policy	The name of the policy in use when the log was created.		x	x	policy="policy_name"
duration	The duration of the HTTP session.			x	duration=0
http_method	The http request method which are allowed to pass through the FortiWeb unit.		x		http_method=get
http_url	The URL address for the HTTP request.		x	x	http_url="/image/example"
http_host	The host home page of the HTTP request.		x	x	http_host="example.com"
http_agent	The web browser used for the HTTP request.		x	x	http_agent="web_browser_information"
http_session_id	The serial number of the session associated with the HTTP request (if known).		x		http_session_id=1ABC123ABC123
action	The action that was specified within the policy.		x	x	action=alert/deny
severity_level	The severity level associated with an attack. Severity level is user-defined per violation.		x		severity_level=1
trigger_policy	The name of the trigger policy used for email alerts and syslog.		x		trigger_policy=trigger_action
msg	The detail message describing the reason that the log message was created.	x	x	x	

Log types

The FortiWeb unit can record and store three types of logs: event logs, attack logs and traffic logs. Logs are recorded on a per occurrence basis, in a separate database for each type of log.

FortiWeb log types are described in [Table 3 on page 20](#).

Table 3: FortiWeb log types

Log type name	Log type ID number	File name	Description
Event	01	elog.log	Event logs record administrative, management and system activity events that occur on the FortiWeb unit. Administrative and management activity events include system configuration changes and administrator log in and log out activity. System activity events include instances such as equipment failures.
Attack	04	alog.log	Attack log messages are recorded when attacks are made against your network and detected by FortiWeb protection rules. Attack log messages provide details about the attack, such as the type of attack, the severity level of the attack as well as source and destination information that can be used to isolate the attack.
Traffic	00	tlog.log	Traffic log messages record the network traffic going through the FortiWeb unit.

Log subtypes

Each FortiWeb log type is further subdivided into subtypes. Subtypes identify the specific area that an activity occurred, which resulted in a log message.

FortiWeb log subtypes are described in [Table 4 on page 20](#).



Note: Arbitrary Subtype ID numbers are used in the table below. on the subtype numbering scheme from FortiGate 4.0 MR2.

Table 4: FortiWeb log subtypes

Log type	Subtype	Subtype ID number	Common name (used in log msg field)
Event logs - 01	System	10	system
	Admin	11	admin
	HA	12	ha
	Router	13	route
	User	14	user
	Policy	15	policy
	Protection	16	protection

Table 4: FortiWeb log subtypes

Log type	Subtype	Subtype ID number	Common name (used in log msg field)
Attack logs - 04	waf_allow_method	20	HTTP Method Violation
	allow_host	21	HTTP Host Violation
	waf_page_rule	22	Page Access Rule Violation
	waf_start_page	23	Start Page Violation
	waf_cookie_poison	24	Cookie Poisoning
	waf_parameter_rule	25	Parameter Validation Violation
	waf_url_access	26	URL Access Violation
	waf_xss_attack	27	Cross Site Scripting
	waf_sql_injection	28	SQL Injection
	waf_information	29	Information Disclosure
	waf_common_exploits	30	Common Exploits
	waf_bad_robot	31	ROBOT Violation
	waf_allow_robot	32	
	waf_malicious_robot	33	Malicious Robot Violation
	waf_brute_login	34	Brute Force Login Violation
	waf_hidden_fields	35	Hidden Field Manipulation
	waf_custom_protection	36	Custom Attack Violation
	waf_header_overflow	37	Header Length Exceeded
	waf_headline_overflow	38	Header Length Line Exceeded
	waf_body_overflow	39	Body Length Exceeded
	waf_content_overflow	40	Content Length Exceeded
	waf_parameter_overflow	41	Parameter Length Exceeded
	waf_request_overflow	42	Request Length Exceeded
	waf_url_parameter_overflow	43	Parameter Length Exceeded
	waf_illegal_http_version	44	Illegal HTTP Version
	waf_cookiecount_overflow	45	Too Many Cookies in Request
	waf_req_headline_overflow	46	Too Many Headers In Request
	waf_illegal_http_method	47	Illegal HTTP Method
	waf_url_parameter_count_overflow	48	Too Many Parameters in Request
	waf_illegal_hostname	49	Illegal Host Name
	xml_intrusion	50	xml_intrusion
	xml_filter	51	xml_filter
	xml_wsdL_operation	52	xml_wsdL_operation
	xml_schema	53	xml_schema
	xml_wsdL_schema	54	xml_wsdL_schema
	xml_decrypt	55	xml_decrypt
	xml_sigverify	56	xml_sigverify
	xml_nonxml	57	xml_nonxml
xml_sql_injection	58	xml_sql_injection	

Table 4: FortiWeb log subtypes

Log type	Subtype	Subtype ID number	Common name (used in log msg field)
Traffic - 00	accept	00	accept
	deny	01	deny

Log priority level

Each FortiWeb log has is assigned a log priority level, also called a log level. The log level appears in the log *pri* field. Table 5 on page 22 describes the log levels.

The log level is used to configure FortiWeb to record logs whose priority equals or exceeds the specified log level. For example, if storing logs on the FortiWeb local disk or Syslog, and the log level is set to Warning, all logs at that priority level and higher are recorded on the disk and Syslog and lower priority level logs are not stored.

Table 5: FortiWeb log priority level

Levels	Description	Generated by
0-Emergency	The system has become unstable	Emergency messages
1-Alert	Immediate action is required	Attack log message
2-Critical	Function is affected	System
3-Error	An error condition exists and functionally could be affected	Error messages
4-Warning	Functionality could be affected	Web attack
5-Notice	Information about normal events	Web attack
6-Information	General information about system operation	Event log messages
7-Debug	Debug information	All system daemons

Event logs - 01

Event log messages record the actions performed by administration users on the FortiWeb unit, and the activities that occur on the FortiWeb unit as a result of those actions.

To locate a description for a particular event log message, match the last five digits of the 10-digit **log_id** number in the event log message with that shown in [Table 6](#), then proceed to the section in this document that describes the specific log_id.

For general information on the fields and composition of log messages, see [“Anatomy of a FortiWeb log message”](#) on page 15.

Table 6: Event logs by subtype and log_id

Subtype	Subtype number	log_id (last 5 digits, starting at)	Log message category
System	10	30000	Administrator logs
		30005	Auto update logs
		30020	Certificate - CA logs
		30025	Certificate - CA group logs
		30030	Certificate - CRL logs
		30035	Certificate - Intermediate CA logs
		30040	Certificate - Intermediate CA group logs
		30045	Certificate - Local logs
		30050	Certificate - Remote logs
		30055	Certificate - verify logs
		30060	DNS logs
		30065	DOS protection logs
		30070	HA-config logs
		30080	RAID logs
		30090	SNMP logs
30095	Vzone logs		
Admin	11	31000	Access profile logs
		31005	Backup and restore logs
		31010	Fail-open logs
		31015	Interface logs
		31020	Mode of operation logs
		31025	Settings logs
		31030	Status logs
		31035	System time logs
		31040	Update signature logs
		31045	Web Site with Anti-Defacement logs
HA	12	32000	HA logs
Router	13	33000	Route logs

Subtype	Subtype number	log_id (last 5 digits, starting at)	Log message category
User	14	34000	LDAP user logs
		34002	Local user logs
		34003	NTLM user logs
		34004	User group logs
Policy	15	35000	Data type group logs
		35002	Physical Server logs
		35003	Policy logs
		35004	Protected server logs
		35005	Server farm logs
		35006	Server health check logs
		35007	Service logs
		35008	Suspicious URL rule logs
		35009	Virtual server logs
Protection	16	36000	Allow method exception logs
		36005	Authentication rule logs
		36010	Authentication policy logs
		36015	Auto learning profile logs
		36020	Brute force login logs
		36025	Custom data type logs
		36030	Custom protection group logs
		36035	Custom protection rule logs
		36040	Custom robot logs
		36045	Suspicious URL rule logs
		36150	Custom suspicious URL logs
		36055	Custom suspicious URL rule logs
		36060	Hidden fields protection logs
		36065	Hidden fields rule logs
		36070	HTTP protocol constraint logs
		36075	Inline protection profile logs
		36080	Input rule logs
		36085	IP blacklist logs
		36090	IP trust list logs
		36095	Offline protection profile logs
		36100	Page access rule logs
36105	Parameter validation rule logs		
36110	Robot control logs		
36115	Robot group logs		
36120	Server protection exception logs		
36125	Server protection rule logs		
36130	Start page logs		

Subtype	Subtype number	log_id (last 5 digits, starting at)	Log message category
		36135	URL access policy logs
		36140	URL access rule logs
		36145	URL rewriting policy logs
		36150	URL rewriting rule logs
		36155	Web vulnerability scan policy logs
		36160	Web vulnerability scan profile logs
		36165	Web vulnerability scan schedule logs

System

System log messages record events that occur in the FortiWeb system, and the results of those events.

Administrator logs

30000

log_id	30000
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See “Anatomy of a FortiWeb log message” on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added administrator <administrator_name> from {GUI CLI console}
Meaning	An administrator setting is added.

30001

log_id	30001
Subtype	10 - System
Log type	01 - Event
Log level	information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name>deleted administrator <administrator_name> from {GUI CLI console}
Meaning	An administrator setting is deleted.

30002

log_id	30002
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified administrator <administrator_name> from {GUI CLI console}
Meaning	An administrator setting is changed.

Auto update logs

30005

log_id	30005
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update started
Meaning	update started

30006

log_id	30006
Subtype	10 - System
Log type	01 - Event
Log level	Error
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update failed, failed to connect fds server!
Meaning	update failed

30007

log_id	30007
Subtype	10 - System
Log type	01 - Event
Log level	Error
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update failed, send update request error
Meaning	update failed

30008

log_id	30008
Subtype	10 - System
Log type	01 - Event
Log level	Error
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update failed, couldn't receive a update package
Meaning	update failed

30009

log_id	30009
Subtype	10 - System
Log type	01 - Event
Log level	Error
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update failed, receive a bad update package
Meaning	update failed

30010

log_id	30010
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update failed, failed to connect any fds servers!
Meaning	update failed

30011

log_id	30011
Subtype	11 - Admin
Log type	01 - Event
Log level	Critical
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	Updated daemon reboot the device
Meaning	device is rebooted

30012

log_id	30012
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	fortiweb is already up-to-date
Meaning	fortiweb is already up-to-date

30013

log_id	30013
Subtype	10 - System
Log type	01 - Event
Log level	Error
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	fortiweb is unauthorized
Meaning	update failed of no contract

30014

log_id	30014
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update succeeded
Meaning	update succeeds

30015

log_id	30015
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	update install failed
Meaning	update failed

Certificate - CA logs**30020**

log_id	30020
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added certificate CA <cert_name> from GUI(<ip_address>).
Meaning	A certificate CA is added

30021

log_id	30021
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted certificate CA <cert_name> from {GUI CLI}.
Meaning	A certificate CA is

Certificate - CA group logs**30025**

log_id	30025
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added certificate CA group <cagroup_name> from {GUI CLI}.
Meaning	A certificate CA group is added

30026

log_id	30026
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted certificate CA group <cagroup_name> from {GUI CLI}.
Meaning	A certificate CA group is deleted

30027

log_id	30027
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified certificate CA group <cagroup_name> from {GUI CLI}.
Meaning	A certificate CA group is modified

Certificate - CRL logs

30030

log_id	30030
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added certificate CRL <crl_name> from GUI(<ip_address>).
Meaning	A intermediate CA group is added

30031

log_id	30031
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted certificate CRL <crl_name> from {GUI CLI}.
Meaning	A certificate CRL is deleted

30032

log_id	30032
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified certificate CRL <cri_name> from {GUI CLI}..
Meaning	A certificate CRL is modified

Certificate - Intermediate CA logs**30035**

log_id	30035
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added intermediate certificate CA <cert_name> from GUI(<ip_address>).
Meaning	A intermediate certificate CA is added

30036

log_id	30036
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted intermediate certificate CA <cert_name> from {GUI CLI}.
Meaning	A intermediate certificate CA is deleted

Certificate - Intermediate CA group logs**30040**

log_id	30040
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added intermediate CA group <inter_cagroup_name> from {GUI CLI}.
Meaning	A intermediate CA group is added

30041

log_id	30041
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted intermediate CA group <inter_cagroup_name> from {GUI CLI}.
Meaning	A intermediate CA group is deleted

30042

log_id	30042
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified intermediate CA group <inter_cagroup_name> from {GUI CLI}.
Meaning	A intermediate CA group is modified

Certificate - Local logs

30045

log_id	30045
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added local certificate <cert_name> from GUI(<ip_address>)
Meaning	A local certificate is added

30046

log_id	30046
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified local certificate <cert_name> from GUI(<ip_address>)
Meaning	A local certificate is changed

30047

log_id	30047
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted local certificate <cert_name> from {GUI CLI}.
Meaning	A local certificate is deleted

30048

log_id	30048
Subtype	11 - Admin
Log type	01 - Event
Log level	Warning
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	Local Cert(CSR) file has been downloaded by user <administrator_name> via GUI(<ip_address>).
Meaning	Users download a csr file

Certificate - Remote logs

30050

log_id	30050
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added remote certificate <cert_name> from GUI(<ip_address>).
Meaning	A remote certificate is added

30051

log_id	30051
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted remote certificate <cert_name> from {GUI CLI}.
Meaning	A remote certificate is deleted

Certificate - verify logs

30055

log_id	30055
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added certificate verify <verify_name> from {GUI CLI}..
Meaning	A certificate verify is added

30056

log_id	30056
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted certificate verify <verify_name> from {GUI CLI}.
Meaning	A certificate verify is deleted

30057

log_id	30057
Subtype	10 - System
Log type	01 - Event
Log level	
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified certificate verify <verify_name> from {GUI CLI}
Meaning	A certificate verify is modified

DNS logs**30060**

log_id	30060
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified DNS settings from {GUI CLI console}
Meaning	DNS settings is changed

DOS protection logs

30065

log_id	30065
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> enabled dos prevention from {GUI CLI console}..
Meaning	Dos prevention is enabled

30066

log_id	30066
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> disabled dos prevention from {GUI CLI console}.
Meaning	Dos prevention is disabled.

HA-config logs

30070

log_id	30070
Subtype	10 - System
Log type	01 - Event
Log level	
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

RAID logs

30080

log_id	30080
Subtype	10 - System
Log type	01 - Event
Log level	
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

SNMP logs

30090

log_id	30090
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified SNMP settings from {GUI CLI console}.
Meaning	SNMP settings is changed

Vzone logs

30095

log_id	30095
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added V-Zone <v-zone_name> from {GUI CLI console}
Meaning	A V-Zone setting is added

30096

log_id	30096
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified V-Zone <v-zone_name> from {GUI CLI console}
Meaning	A V-Zone setting is changed

30097

log_id	30097
Subtype	10 - System
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted V-Zone <v-zone_name> from {GUI CLI console}
Meaning	A V-Zone setting is deleted

Admin

Admin log messages record the actions performed by administration users when configuring FortiWeb, and the results of those actions.

Access profile logs

31000

log_id	31000
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added new access profile <profile_name> from {GUI CLI console}
Meaning	A new access profile was added

31001

log_id	31001
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted new access profile <profile_name> from {GUI CLI console}
Meaning	An access profile was deleted

31002

log_id	31002
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed new access profile <profile_name> from {GUI CLI console}
Meaning	An access profile setting is changed

Backup and restore logs**31005**

log_id	31005
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	System config file has been downloaded by user <administrator_name> via {GUI CLI}.
Meaning	System config file has been downloaded

31006

log_id	31006
Subtype	11 - Admin
Log type	01 - Event
Log level	Critical
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> restored the image from {GUI CLI}.
Meaning	User restores the image

Fail-open logs**31010**

log_id	31010
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed the mode of failopen
Meaning	The mode of fail-open is changed

Interface logs

31015

log_id	31015
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added new interface <interface_name> from {GUI CLI console}
Meaning	A new interface is added

31016

log_id	31016
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed the ip setting of interface <interface_name> from {GUI CLI console}
Meaning	User changed the ip setting of the interface

31017

log_id	31017
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed the access setting of interface <interface_name> from {GUI CLI console}
Meaning	User changed the access setting of the interface

31018

log_id	31018
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted new interface <interface_name> from {GUI CLI console}
Meaning	An interface is deleted

Mode of operation logs

31020

log_id	31020
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed the mode of system from {reverse proxy offline protection true transparent proxy transparent inspection} to {reverse proxy offline protection true transparent proxy transparent inspection}
Meaning	system opmode is changed

Settings logs

31025

log_id	31025
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> {enabled disable} enable-strong-passwords global setting from {GUI CLI console}
Meaning	enable-strong-passwords global setting changed

31026

log_id	31026
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> {enabled disable} single-admin-mode global setting from {GUI CLI console}
Meaning	single-admin-mode global setting changed

31027

log_id	31027
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed timeout global setting to <integer>m from {GUI CLI console}
Meaning	Timeout global setting is changed

Status logs

31030

log_id	31030
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed hostname global setting to <host_name> from {GUI CLI}.
Meaning	User changes hostname

31031

log_id	31031
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> reset to the factory settings from {GUI CLI}.
Meaning	factory reset

31032

log_id	31032
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> shutdown the device from {GUI CLI}.
Meaning	shutdown device

31033

log_id	31033
Subtype	11 - Admin
Log type	01 - Event
Log level	Critical
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> rebooted the device from {GUI CLI}
Meaning	device is rebooted the alternative firmware

System time logs

31035

log_id	31035
Subtype	11 - Admin
Log type	01 - Event
Log level	Notice
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> changed time from <Time> to <Time> from {GUI CLI}.
Meaning	global time setting change

Update signature logs

31040

log_id	31040
Subtype	11 - Admin
Log type	01 - Event
Log level	Critical
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> loaded a wrong signature file from GUI(<ip addr>)
Meaning	loaded a wrong signature file

31041

log_id	31041
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> update signatures from GUI(<ip addr>)
Meaning	update signature

Web Site with Anti-Defacement logs**31045**

log_id	31045
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added a new website <name> from {GUI CLI}.
Meaning	a new website is added

31046

log_id	31046
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified a new website <name> from {GUI CLI}.
Meaning	a new website is modified

31047

log_id	31047
Subtype	11 - Admin
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted a new website <name> from {GUI CLI}.
Meaning	a new website is deleted

HA

HA log messages record events performed by administrative users when configuring High Availability (HA), and the results of those events.

HA logs

32000

log_id	32000
Subtype	12- HA
Log type	01 - Event
Log level	
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

Router

Router log messages record events performed by administrative users when configuring Router connections, and the results of those events.

Route logs

33000

log_id	33000
Subtype	13- Router
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added route <route_name> from {GUI CLI}.
Meaning	A route has been added

33001

log_id	33001
Subtype	13- Router
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified route <route_name> from {GUI CLI}.
Meaning	A route has been modified

33002

log_id	33002
Subtype	13- Router
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted route <route_name> from {GUI CLI}.
Meaning	A route has been deleted

User

User log messages record events as a result of actions performed by users,), and the results of those events.

LDAP user logs**34000**

log_id	34000
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added ldap user <user_name> from {GUI CLI}.
Meaning	A ldap user is added

34001

log_id	34001
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified ldap user <user_name> from {GUI CLI}.
Meaning	A ldap user is modified

34002

log_id	34002
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted ldap user <user_name> from {GUI CLI}
Meaning	A ldap user is deleted

Local user logs

34005

log_id	34005
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added local user <user_name> from {GUI CLI}.
Meaning	A local user is added

34006

log_id	34006
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified local user <user_name> from {GUI CLI}.
Meaning	A local user is modified

34007

log_id	34007
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted local user <user_name> from {GUI CLI}.
Meaning	A local user is deleted

NTLM user logs**34010**

log_id	34010
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added ntlm user <user_name> from {GUI CLI}.
Meaning	A ntlm user is added

34011

log_id	34011
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified ntlm user <user_name> from {GUI CLI}.
Meaning	A ntlm user is changed

34012

log_id	34012
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted ntlm user <user_name> from {GUI CLI}.
Meaning	A ntlm user is deleted

User group logs

34015

log_id	34015
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator> added user group <user_group_name> from {GUI CLI}.
Meaning	User Group is added.

34016

log_id	34016
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator> Modified user group <user_group_name> from {GUI CLI}.
Meaning	User Group is edited.

34017

log_id	34017
Subtype	14 - User
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted user group <user_group_name> from {GUI CLI}.
Meaning	User Group is deleted

Policy

Policy log messages record events performed by administrative users related to policy, and the results of those events.

Data type group logs**35000**

log_id	35000
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the data type group <group_name> from {GUI CLI}.
Meaning	a data type group has been added

35001

log_id	35001
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the data type group <group_name> from {GUI CLI}.
Meaning	a data type group has been changed

35002

log_id	35002
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the data type group <group_name> from {GUI CLI}.
Meaning	a data type group has been deleted

Physical Server logs

35005

log_id	35005
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added pserver <pserver_name> from {GUI CLI}.
Meaning	A pserver is added

35006

log_id	35006
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified pserver <pserver_name> from {GUI CLI}.
Meaning	A pserver is changed

35007

log_id	35007
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted pserver <pserver_name> from {GUI CLI}.
Meaning	A pserver is deleted

Policy logs**35010**

log_id	35010
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added policy <policy_name> from {GUI CLI}.
Meaning	Policy added

35011

log_id	35011
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified policy <policy_name> from {GUI CLI}.
Meaning	Policy modified

35012

log_id	35012
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted policy <policy_name> from {GUI CLI}.
Meaning	Policy deleted

Protected server logs

35015

log_id	35015
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the protected server <server_name> from {GUI CLI}.
Meaning	a protected server has been added

35016

log_id	35016
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the protected server <server_name> from {GUI CLI}.
Meaning	a protected server has been changed

35017

log_id	35017
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the protected server <server_name> from {GUI CLI}.
Meaning	a protected server has been deleted

Server farm logs**35020**

log_id	35020
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the server farm <server_farm_name> from {GUI CLI}.
Meaning	A server farm is added

35031

log_id	35031
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the server farm <server_farm_name> from {GUI CLI}.
Meaning	A server farm is changed

35022

log_id	35022
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the server farm <server_farm_name> from {GUI CLI}.
Meaning	A server farm is deleted

Server health check logs

35025

log_id	35025
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added server health <name> from {GUI CLI}.
Meaning	A server health is added

35026

log_id	35026
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified server health <name> from {GUI CLI}.
Meaning	A server health is modified

35027

log_id	35027
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted server health <name> from {GUI CLI}.
Meaning	A server health is deleted

Service logs**35030**

log_id	35030
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <user_name> Added the service <service_name> from {GUI CLI}.
Meaning	a service has been added

35031

log_id	35031
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <user_name> modified the service <service_name> from {GUI CLI}.
Meaning	a service has been changed

35032

log_id	35032
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <user_name> deleted the service <service_name> from {GUI CLI}.
Meaning	a service has been deleted

Suspicious URL rule logs

35035

log_id	35035
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the suspicious url rule <rule_name> from {GUI CLI}.
Meaning	a suspicious url rule has been changed

35036

log_id	35036
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the suspicious url rule <rule_name> from {GUI CLI}.
Meaning	a suspicious url rule has been changed

35037

log_id	35037
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the suspicious url rule <rule_name> from {GUI CLI}.
Meaning	a suspicious url rule has been deleted

Virtual server logs**35040**

log_id	35040
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added vserver <vserver_name> from {GUI CLI}.
Meaning	A vserver is added

35041

log_id	35041
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified vserver <vserver_name> from {GUI CLI}.
Meaning	A vserver is changed

35042

log_id	35042
Subtype	15 - Policy
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted vserver <vserver_name> from {GUI CLI}.
Meaning	A vserver is deleted

Protection

Protection log messages record events related to protection rules, and the results of those events.

Allow method exception logs

36000

log_id	36000
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Allow Method Exception <name> from {GUI CLI}.
Meaning	An Allow Method Exception rule is added

36001

log_id	36001
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Allow Method Exception <name> from {GUI CLI}
Meaning	An Allow Method Exception rule is changed

36002

log_id	36002
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Allow Method Exception <name> from {GUI CLI}.
Meaning	An Allow Method Exception rule is deleted

Authentication rule logs**36005**

log_id	36005
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added the authenticate rule <name> from {GUI CLI}.
Meaning	An authenticate rule has been added

36006

log_id	36006
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified the authenticate rule <name> from {GUI CLI}.
Meaning	An authenticate rule has been changed

36007

log_id	36007
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the authenticate rule <name> from {GUI CLI}.
Meaning	An authenticate rule has been deleted

Authentication policy logs

36010

log_id	36010
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Authentication Policy <name> from {GUI CLI}.
Meaning	An Authentication Policy rule is added

36011

log_id	36011
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Authentication Policy <name> from {GUI CLI}.
Meaning	An Authentication Policy rule is changed

36012

log_id	36012
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Authentication Policy <name> from {GUI CLI}.
Meaning	An Authentication Policy rule is deleted

Auto learning profile logs**36015**

log_id	36015
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Auto Learn <name> from {GUI CLI}.
Meaning	An Auto Learn rule is added

36016

log_id	36016
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Auto Learn <name> from {GUI CLI}.
Meaning	An Auto Learn rule is modified

36017

log_id	36017
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Auto Learn <name> from {GUI CLI}.
Meaning	An Auto Learn rule is deleted

Brute force login logs

36020

log_id	36020
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Brute Force Login <name> from {GUI CLI}.
Meaning	A Brute Force Login rule is added

36021

log_id	36021
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified Brute Force Login <name> from {GUI CLI}.
Meaning	A Brute Force Login rule is modified

36022

log_id	36022
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted Brute Force Login <name> from {GUI CLI}.
Meaning	A Brute Force Login rule is deleted

Custom data type logs**36025**

log_id	36025
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the custom data type <type_name> from {GUI CLI}.
Meaning	A custom data type has been added

36026

log_id	36026
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the custom data type <type_name> from {GUI CLI}.
Meaning	A custom data type has been changed

36027

log_id	36027
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the custom data type <type_name> from {GUI CLI}.
Meaning	A custom data type has been deleted

Custom protection group logs

36030

log_id	36030
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

Custom protection rule logs

36035

log_id	36035
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the custom protection rule <rule_name> from {GUI CLI}.
Meaning	a custom protection rule has been added

36036

log_id	36036
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the custom protection rule <rule_name> from {GUI CLI}.
Meaning	A custom protection rule has been changed

36037

log_id	36037
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the custom protection rule <rule_name> from {GUI CLI}.
Meaning	A custom protection rule has been deleted

Custom robot logs

36040

log_id	36040
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added custom robot <name> from {GUI CLI}.
Meaning	A custom robot is added

36041

log_id	36041
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified custom robot <name> from {GUI CLI}.
Meaning	A custom robot is modified

36042

log_id	36042
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted custom robot <name> from {GUI CLI}.
Meaning	A custom robot is deleted

Suspicious URL rule logs**36045**

log_id	36045
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the suspicious url rule <rule_name> from {GUI CLI}.
Meaning	A suspicious url rule has been added

36046

log_id	36046
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the suspicious url rule <rule_name> from {GUI CLI}.
Meaning	A suspicious url rule has been changed

36047

log_id	36047
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the suspicious url rule <rule_name> from {GUI CLI}.
Meaning	A suspicious url rule has been deleted

Custom suspicious URL logs

36050

log_id	36050
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the custom suspicious url <url_name> from {GUI CLI}.
Meaning	A custom suspicious url has been added

36051

log_id	36051
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the custom suspicious url <url_name> from {GUI CLI}.
Meaning	A custom suspicious url has been changed

36052

log_id	36052
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the custom suspicious url <url_name> from {GUI CLI}.
Meaning	A custom suspicious url has been

Custom suspicious URL rule logs**36055**

log_id	36055
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the custom suspicious url rule <rule_name> from {GUI CLI}.
Meaning	A custom suspicious url rule has been added

36056

log_id	36056
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the custom suspicious url rule <rule_name> from {GUI CLI}.
Meaning	A custom suspicious url rule has been changed

36057

log_id	36057
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the custom suspicious url rule <rule_name> from {GUI CLI}.
Meaning	A custom suspicious url rule has been deleted

Hidden fields protection logs

36060

log_id	36060
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Hidden Fields Protection <name> from {GUI CLI}.
Meaning	A Hidden Fields Protection rule is added

36061

log_id	36061
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Hidden Fields Protection <name> from {GUI CLI}.
Meaning	A Hidden Fields Protection rule is changed

36062

log_id	36062
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Hidden Fields Protection <name> from {GUI CLI}.
Meaning	A Hidden Fields Protection rule is deleted

Hidden fields rule logs**36065**

log_id	36065
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Hidden Fields Rule <name> from {GUI CLI}.
Meaning	A Hidden Fields Rule is added

36066

log_id	36066
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Hidden Fields Rule <name> from {GUI CLI}.
Meaning	A Hidden Fields Rule is changed

36067

log_id	36067
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Hidden Fields Rule <name> from {GUI CLI}.
Meaning	A Hidden Fields Rule is deleted

HTTP protocol constraint logs

36070

log_id	36070
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Parameter Validation <name> from {GUI CLI}.
Meaning	A Parameter Validation rule is added

36071

log_id	36071
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Parameter Validation <name> from {GUI CLI}.
Meaning	A Parameter Validation rule is changed

36072

log_id	36072
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Parameter Validation <name> from {GUI CLI}.
Meaning	A Parameter Validation rule is deleted

Inline protection profile logs**36075**

log_id	36075
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Inline Profile <name> from {GUI CLI}.
Meaning	An Inline Profile rule is added

36076

log_id	36076
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Inline Profile <name> from {GUI CLI}.
Meaning	An Inline Profile rule is changed

36077

log_id	36077
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Inline Profile <name> from {GUI CLI}.
Meaning	An Inline Profile rule is deleted

Input rule logs

36080

log_id	36080
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the input rule <rule_name> from {GUI CLI}.
Meaning	An input rule has been added

36081

log_id	36081
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the input rule <rule_name> from {GUI CLI}.
Meaning	An input rule has been changed

36082

log_id	36082
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the input rule <rule_name> from {GUI CLI}.
Meaning	a input rule has been deleted

IP blacklist logs**36085**

log_id	36085
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added IP Black List rule <rule_name> from {GUI CLI}.
Meaning	A IP Black List rule is added

36086

log_id	36086
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified IP Black List rule <rule_name> from {GUI CLI}.
Meaning	A IP Black List rule is changed

36087

log_id	36087
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted IP Black List rule <rule_name> from {GUI CLI}.
Meaning	A IP Black List rule is deleted

IP trust list logs

36090

log_id	36090
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Trust IP list from {GUI CLI}.
Meaning	An IP trust list has been added

36091

log_id	36091
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified Trust IP list from {GUI CLI}.
Meaning	An IP trust list has been changed

36092

log_id	36092
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Trust IP list from {GUI CLI}.
Meaning	An IP trust list has been deleted

Offline protection profile logs**36095**

log_id	36095
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Offline Profile <name> from {GUI CLI}.
Meaning	An Offline Profile rule is added

36096

log_id	36096
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified Offline Profile <name> from {GUI CLI}.
Meaning	A Offline Profile rule is changed

36097

log_id	36097
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Offline Profile <name> from {GUI CLI}.
Meaning	A Offline Profile rule is deleted

Page access rule logs

36100

log_id	36100
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the page access rule <rule_name> from {GUI CLI}.
Meaning	A page access rule has been added

36101

log_id	36101
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the page access rule <rule_name> from {GUI CLI}.
Meaning	A page access rule has been changed

36102

log_id	36102
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the page access rule <rule_name> from {GUI CLI}.
Meaning	A page access rule has been deleted

Parameter validation rule logs

36105

log_id	36105
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the parameter validation rule <rule_name> from {GUI CLI}.
Meaning	A parameter validation rule has been added

36106

log_id	36106
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the parameter validation rule <rule_name> from {GUI CLI}.
Meaning	A parameter validation rule has been changed

36107

log_id	36107
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the parameter validation rule <rule_name> from {GUI CLI}.
Meaning	A parameter validation rule has been deleted

Robot control logs

36110

log_id	36110
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Robot Control <name> from {GUI CLI}.
Meaning	A Robot Control rule is added

36111

log_id	36111
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified Robot Control <name> from {GUI CLI}.
Meaning	A Robot Control rule is changed

36112

log_id	36112
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Robot Control <name> from {GUI CLI}.
Meaning	A Robot Control rule is deleted

Robot group logs**36115**

log_id	36115
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added Robot Group rule <name> from {GUI CLI}.
Meaning	A Robot Group rule is added

36116

log_id	36116
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified Robot Group rule <name> from {GUI CLI}.
Meaning	A Robot Group rule is changed

36117

log_id	36117
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted Robot Group rule <name> from {GUI CLI}.
Meaning	A Robot Group rule is deleted

Server protection exception logs

36120

log_id	36120
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

Server protection rule logs

36125

log_id	36125
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the server protection rule <rule_name> from {GUI CLI}.
Meaning	A server protection rule has been added

36126

log_id	36126
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the server protection rule <rule_name> from {GUI CLI}.
Meaning	A server protection rule has been changed

36127

log_id	36127
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the server protection rule <rule_name> from {GUI CLI}.
Meaning	A server protection rule has been deleted

Start page logs

36130

log_id	36130
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Added the start page rule <rule_name> from {GUI CLI}.
Meaning	A start page rule has been added

36131

log_id	36131
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified the start page rule <rule_name> from {GUI CLI}.
Meaning	A start page rule has been changed

36132

log_id	36132
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted the start page rule <rule_name> from {GUI CLI}.
Meaning	a start page rule has been deleted

URL access policy logs**36135**

log_id	36135
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added URL Access Policy <policy_name> from {GUI CLI}.
Meaning	A URL Access Policy is added

36136

log_id	36136
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified URL Access Policy <policy_name> from {GUI CLI}.
Meaning	A URL Access Policy is changed

36137

log_id	36137
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Deleted URL Access Policy <policy_name> from {GUI CLI}.
Meaning	A URL Access Policy is deleted

URL access rule logs

36140

log_id	36140
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added URL Access Rule <rule_name> from {GUI CLI}.
Meaning	A URL Access Rule is added

36141

log_id	36141
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> Modified URL Access Rule <rule_name> from {GUI CLI}.
Meaning	A URL Access Rule is changed

36142

log_id	36142
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted URL Access Rule <rule_name> from {GUI CLI}.
Meaning	A URL Access Rule is deleted

URL rewriting policy logs

36145

log_id	36145
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

URL rewriting rule logs

36150

log_id	36150
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	<A unique message describing the event that occurred when this log was created.>
Meaning	

Web vulnerability scan policy logs

36155

log_id	36155
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added the wvs policy<name> from {GUI CLI}.
Meaning	A wvs policy has been added

36156

log_id	36156
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified the wvs policy <name> from {GUI CLI}.
Meaning	A wvs policy has been changed

36157

log_id	36157
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the wvs policy <name> from {GUI CLI}.
Meaning	A wvs policy has been deleted

Web vulnerability scan profile logs

36160

log_id	36160
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added the wvs profile <name> from {GUI CLI}.
Meaning	A wvs profile has been added

36161

log_id	36161
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified the wvs profile <name> from {GUI CLI}.
Meaning	A wvs profile has been changed

36162

log_id	36162
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the wvs profile <name> from {GUI CLI}.
Meaning	A wvs profile has been deleted

Web vulnerability scan schedule logs

36165

log_id	36165
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> added the wvs schedule <name> from {GUI CLI}.
Meaning	A wvs schedule has been added

36166

log_id	36166
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> modified the wvs schedule <name> from {GUI CLI}.
Meaning	A wvs schedule has been changed

36167

log_id	36167
Subtype	16 - Protection
Log type	01 - Event
Log level	Information
FortiWeb version	4.2
Fields	Field Description
Log header	See " Anatomy of a FortiWeb log message " on page 15 for a description of the log header fields.
user	The identification (login name) of the user that performed the action that caused the log to be created.
ui	The type of interface the user was using at the time the log was created. The possible values are: gui, telnet, ssh or console.
action	The action performed that caused the log to be created.
status	The result of the action performed.
reason	The reason for the result (status) of the action.
msg	User <administrator_name> deleted the wvs schedule <name> from {GUI CLI}.
Meaning	A wvs schedule has been deleted

Attack logs - 04

Attack log messages are recorded when attacks are made against your network. These log messages provide details about the attack, such as the severity level of the attack, the type of attack and the source and destination of the attack.

To locate a description for a particular attack log message, match the last five digits of the 10-digit **log_id** field in the attack log message with that shown in [Table 7](#), and then proceed to “[Attack log message content](#)” on page 133.

For general information on the structure and content of an attack log message, see “[Anatomy of a FortiWeb log message](#)” on page 15.

Table 7: Attack log subtypes and log_id

Subtype	Subtype number	log_id (last 5 digits)	Log message
allow_host	20	20000	HTTP Host Violation
waf_allow_method	21	20005	HTTP Method Violation
waf_allow_robot	22	20010	Allow Robot: Google
		20011	Allow Robot: Yahoo
		20012	Allow Robot: MSN
		20013	Allow Robot: Baidu
		20014	Allow Robot: Scooter
		20015	Allow Robot: Lycos
		20016	Allow Robot: Alltheweb
		20017	Allow Robot: Inktomi
		20018	Allow Robot: Looksmart
		20019	Allow Robot: Excite
		20020	Allow Robot: Askjeeves
		20021	Allow Robot: Teoma
20022	Allow Robot: Wisenut		
20023	Allow Robot: Bing		
waf_bad_robot	23	20030	ROBOT Violation
waf_body_overflow	24	20035	Body Length Exceeded
waf_brute_login	25	20040	Brute Force Login Violation

Subtype	Subtype number	log_id (last 5 digits)	Log message
waf_common_exploits	26	20045	Common Exploits: File Injection
		20046	Common Exploits: Command Access
		20047	Common Exploits: Command Injection
		20048	Common Exploits: Coldfusion Injection
		20049	Common Exploits: LDAP Injection
		20050	Common Exploits: SSI Injection
		20051	Common Exploits: PHP Injection
		20052	Common Exploits: Email Injection
		20053	Common Exploits: Response Splitting
		20054	Common Exploits: Injection Flaw
		20055	Common Exploits: SRC Disclosure
	20056	Common Exploits: Trojans	
waf_content_overflow	27	20060	Content Length Exceeded
waf_cookie_poison	28	20065	Cookie Poisoning
waf_cookiecount_overflow	29	20070	Too Many Cookies in Request
waf_custom_protection	30	20075	Custom Attack Violation: <name>, where <name> is the name of the custom protection rule that triggered the log.
waf_header_overflow	31	20080	Header Length Exceeded
waf_headline_overflow	32	20085	Header Line Length Exceeded
waf_hidden_fields	33	20090	Hidden Field Manipulation
waf_illegal_hostname	34	20095	Illegal Host Name
waf_illegal_http_method	35	20100	Illegal HTTP Method
waf_illegal_http_version	36	20105	Illegal HTTP Version

Subtype	Subtype number	log_id (last 5 digits)	Log message
waf_information	37	20110	Information Disclosure: Statistics Pages Revealed
		20111	Information Disclosure: SQL Errors Leakage
		20112	Information Disclosure: IIS Errors Leakage
		20113	Information Disclosure: Zope Information Leakage
		20114	Information Disclosure: CF Information Leakage
		20115	Information Disclosure: PHP Information Leakage
		20116	Information Disclosure: ISA Server Existence Revealed
		20117	Information Disclosure: MS Doc Properties Leakage
		20118	Information Disclosure: Directory Listing
		20119	Information Disclosure: ASP/JSP Source Code Leakage
		20120	Information Disclosure: PHP Source Code Leakage
		20121	Information Disclosure: CF Source Code Leakage
		20122	Information Disclosure: IIS Default Location
		20123	Information Disclosure: Application Not Available
		20124	Information Disclosure: Weblogic Info Disclosure
		20125	Information Disclosure: File Or Dir Names Leakage
		20126	Information Disclosure: HTTP Retcode 4XX
20127	Information Disclosure: HTTP Retcode 5XX		
waf_malicious_robot	38	20130	Malicious Robot Violation

Subtype	Subtype number	log_id (last 5 digits)	Log message
waf_page_rule	39	20135	Page Access Rule Violation
waf_parameter_overflow	40	20140	Parameter Length Exceeded
waf_parameter_rule	41	20145	Parameter Validation Violation
waf_req_headline_overflow	42	20150	Too Many Headers In Request
waf_request_overflow	43	20155	Request Length Exceeded
waf_sql_injection	44	20160	SQL Injection: SQL Injection <number>, where <number> is an integer in the range of 1 to 10 that defines the specific SQL injection type
waf_start_page	45	20165	Start Page Violation
waf_url_access	46	20170	URL Access Violation
waf_url_parameter_count_overflow	47	20175	Too Many Parameters in Request
waf_url_parameter_overflow	48	20180	Parameter Length Exceeded
waf_xss_attack	49	20185	Cross Site Scripting : XSS Signature <number>, where <number> is an integer in the range of 1 to 9 that defines the specific XSS signature type
xml_intrusion	50	20190	xml_intrusion
xml_filter	51	20195	xml_filter
xml_wsd_operation	52	20200	xml_wsd_operation
xml_schema	53	20205	xml_schema
xml_wsd_schema	54	20210	xml_wsd_schema
xml_decrypt	55	20215	xml_decrypt
xml_sigverify	56	20220	xml_sigverify
xml_nonxml	57	20225	xml_nonxml
xml_sql_injection	58	20230	xml_sql_injection

Attack log message content

All attack logs provide detailed information that describes the attack. The content of an attack log message is defined below.

log_id	A 10-digit number, of which the last 5 digits identify the specific log message. For more information, see log_id in Table 7, "Attack log subtypes and log_id," on page 129
log type	Attack
subtype	See Table 7, "Attack log subtypes and log_id," on page 129
severity_level	The severity level associated with the specific attack. Severity level is user-defined per violation (subtype). Possible severity values are 0, 1, 2 or 3: <ul style="list-style-type: none"> • 0, a severity level has not yet been assigned to the violation subtype • 1, the subtype is defined as a high severity violation • 2, the subtype is defined as a medium severity violation • 3, the subtype is defined as a low severity violation For more information, see rule violation severity in the FortiWeb Administration Guide .
FortiWeb version	4.2
Fields	Field Description
Log header	See "Anatomy of a FortiWeb log message" on page 15 for a description of the log header fields.
proto	The protocol used by the web traffic. Always set to tcp
service	The service associated with the log. Options are http https
src	The web traffic source IP address
src_port	The web traffic source port
dst	The web traffic destination IP address
dst_port	The web traffic destination port
policy_name	The name of the policy in use
action	The action associated with the log
http_method	The http request method which are allowed to pass through the FortiWeb unit. Options are: get post head delete put options trace connect others
http_url	The HTTP request URL
http_host	The HTTP request host
http_agent	The HTTP request User-Agent
http_session_id	The HTTP session ID
msg	A unique message associated with each subtype, describing the attack. See Log message in Table 7, "Attack log subtypes and log_id," on page 129

Traffic - 00

Traffic log messages record the network traffic going through the FortiWeb unit.

To locate a description for a particular traffic log message, match the last five digits of the 10-digit **log_id** field in the traffic log message with that shown in [Table 8](#), then proceed to [“Traffic log message content” on page 135](#).

For general information on the fields and composition of log messages, see [“Anatomy of a FortiWeb log message” on page 15](#).

Table 8: Traffic log subtypes and log_id

Subtype	Subtype number	log_id (last 5 digits)	Log message
Accept	00	10001	accept traffic
Deny	01	10002	deny traffic

Traffic log message content

All traffic logs provide detailed information that describes the traffic passing through the FortiWeb unit. The content of an traffic log message are defined below

log_id	A 10-digit number, of which the last 5 digits identify the specific log message. For more information, see log_id in Table 8, “Traffic log subtypes and log_id,” on page 135
log type	Traffic
subtype	The subtype associated with the traffic log message. Options are accept deny.
FortiWeb version	4.2
Fields	Field Description
Log header	See “Anatomy of a FortiWeb log message” on page 15 for a description of the log header fields.
proto	The protocol used by the web traffic. Always set to tcp
service	The service associated with the log. Options are http https
src	The web traffic source IP address
src_port	The web traffic source port
dst	The web traffic destination IP address
dst_port	The web traffic destination port
policy_name	The name of the server policy in use at the time that the traffic log was created
duration	The duration of the HTTP session (not currently measured - always set to zero)
action	The action associated with the log. Options are accept deny. Based on the policy in use at the time the traffic log was created, accept means the traffic is allowed by FortiWeb, and deny means the traffic was blocked by FortiWeb
http_url	The HTTP request URL
http_host	The HTTP request host
http_agent	The HTTP request User-Agent
msg	An accept or deny message associated with each traffic log, depending on the action performed by the FortiWeb unit.



www.fortinet.com



www.fortinet.com