



FortiAnalyzer v4.0 MR3
Log Message Reference



March 07, 2012

05-432-165170-20120307

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Visit these links for more information and documentation for your Fortinet product:

Technical Documentation - <http://docs.fortinet.com>

Knowledge Base - <http://kb.fortinet.com>

Technical Support - <https://support.fortinet.com>

Training Services - <http://training.fortinet.com>



Introduction	5
Customer service & technical support.....	5
Training	5
Documentation	6
Fortinet Tools and Documentation CD 6	
Fortinet Knowledge Base 6	
Comments on Fortinet technical documentation 6	
Conventions.....	6
IP addresses	6
Cautions, Notes and Tips	6
Typographical conventions.....	7
Command syntax conventions	7
Log types, IDs, & display styles	10
Formatted vs. raw display	10
Log types and subtypes	10
Event logs	10
Network analyzer logs.....	11
Network scan logs	11
Log ID numbers	11
Log headers vs. bodies	12
Event logs: admin subtype	13
0104000001	13
0104000002	14
0104000003	16
0104000004	16
0104000005	17
0104000008	18
0104000009	18
0104000010	18
0104000011	19
0104000013	19
0104000015	20
0104000016	21
0104000017	21
0104000018	22
0104000019	23
Event logs: config subtype	25
0100000000	26
0100000001	26

0100000003	27
0100000004	28
0100000005	28
0100000006	29
0100000007	29
0100000008	30
0100000009	31
0100000010	31
0100000011	32
0100000012	32
0100000013	33
0100000015	33
0100000016	34
0100000029	34
0100000030	35
0100000031	36
0100000032	36
0100000033	37
0100000034	37
0100000035	38
0100000036	38
0100000037	39
0100000038	39
0100000039	40
0100000040	40
0100000041	41
0100000042	41
0100000043	42
0100000044	43
0100000045	44
0100000046	44
0100000047	45
0100000048	45
0100000049	46
0100000050	47
0100000052	47
0100000053	48
0100000054	48
0100000069	49
0100000070	49
0100000071	50
0100000072	50
0100000073	51

0100000074	51
0100000075	52
0100000076	52
0100000077	53
0100000078	53
0100000079	54
0100000080	54
0100000083	55
0100000084	55
0100000086	56
0100000088	56
0100000090	57
0100000091	57
0100000092	58
0100000093	58
0100000094	59
0100000096	59
0100032120	60
0100032122	60
0100032132	61
0100032133	61
0100032134	62
0100032150	62
0100065535	63
Event logs: ipsec subtype	65
Event logs: system subtype	67
0106000001	67
0106000005	68
0106000006	68
0106000007	69
0106000009	70
0106000010	71
0106000012	72
0106000014	74
0106000016	75
0106000017	77
0106000018	78
0106000019	79
0106000021	79
0106000023	81
0106000024	81
0106000025	82
0106000028	84

0106000029	85
0106000030	87
0106000035	90
0106000036	91
0106000037	92
0106000038	93
0106000040	93
0106131090	94
0106131091	94
Network Analyzer logs	96
Netscan logs: discovery subtype	97
1100000097	97
1100000099	97
1100000100	98
1100000102	98
1100000104	99
1100000105	99
Netscan logs: vulnerability subtype	100
1101000096	100
1101000098	101
1101000101	101
1101000103	102



Welcome and thank you for selecting Fortinet products for your network protection.

This document provides information about FortiAnalyzer log messages.

It assumes that you have already enabled and configured local storage of system event and/or network analyzer logs on your FortiAnalyzer unit, and need to know what those log messages mean.

This document does **not** cover physical deployment or initial configuration. For information on physical deployment and installation, see the *FortiAnalyzer Install Guide*. For information on configuring local event and network analyzer log storage, see the *FortiAnalyzer Administration Guide* or the *FortiAnalyzer CLI Reference*.

Also, this document does **not** cover the log messages of other network devices that may connect to the FortiAnalyzer unit in order to store their log messages. For those devices, see the reference specific to each device. For example, for information on FortiGate log messages, see the *FortiOS Log Message Reference*.

This chapter introduces you to concepts you may need in order to use this document, and includes the following topics:

- [Customer service & technical support](#)
- [Training](#)
- [Documentation](#)
- [Conventions](#)

Customer service & technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate 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 [Technical Support Requirements](#).

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://campus.training.fortinet.com>, or email training@fortinet.com.

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.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For 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, 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 technical document to techdoc@fortinet.com.

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 notes, tips and cautions.



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



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



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

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 <i>VPN > IPSEC > Auto Key (IKE)</i> .
Publication	For details, see the <i>FortiGate Administration Guide</i> .

Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 2: Command syntax notation

Convention	Description
Square brackets []	A non-required word or series of words. For example: <pre>[verbose {1 2 3}]</pre> indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <pre>verbose 3</pre>

Table 2: Command syntax notation (Continued)

<p>Angle brackets < ></p>	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example:</p> <pre><retries_int></pre> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> • <xxx_name>: A name referring to another part of the configuration, such as <code>policy_A</code>. • <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. • <xxx_email>: An email address, such as <code>admin@mail.example.com</code>. • <xxx_url>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet.com/</code>. • <xxx_ipv4>: An IPv4 address, such as <code>192.168.1.99</code>. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. • <xxx_ipv6>: A colon (:)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>. • <xxx_v6mask>: An IPv6 netmask, such as <code>/96</code>. • <xxx_ipv6mask>: An IPv6 address and netmask separated by a space. • <xxx_str>: A string of characters that is not another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the FortiAnalyzer CLI Reference. • <xxx_int>: An integer number that is not another data type, such as 15 for the number of minutes.
<p>Curly braces { }</p>	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.</p> <p>You must enter at least one of the options, unless the set of options is surrounded by square brackets [].</p>

Table 2: Command syntax notation (Continued)

Options delimited by vertical bars 	Mutually exclusive options. For example: <code>{enable disable}</code> indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: <code>{http https ping snmp ssh telnet}</code> indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: <code>ping https ssh</code> Note: To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: <code>ping https snmp ssh</code> If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

2. Log types, IDs, & display styles



When local logging is enabled, and the FortiAnalyzer unit performs an activity or a local event occurs, an event log message is recorded. The network analyzer feature may also record local log messages if you have enabled it.

Each of these log messages has a specific type, subtype, and log ID number.



Note: Device log messages are not covered in this document. Instead, see the log message reference for each device. For example, for FortiGate log information, see the [FortiOS Log Message Reference](#).

This topic includes:

- [Formatted vs. raw display](#)
- [Log types and subtypes](#)
- [Log ID numbers](#)
- [Log headers vs. bodies](#)

Formatted vs. raw display

Log messages are initially displayed in *Formatted* (columnar) format. Columnar format permits you to filter the display, including hiding some log messages and fields of those messages.

Because columnar format may not display the complete log message, this document assumes you are viewing log messages in *Raw* format, which displays complete log messages.

To display all fields and all log message, click *Raw*.

Log types and subtypes

On FortiAnalyzer units, local log messages' *Type* is one of:

- *network analyzer* (`type=sniffer`)
- *event* (`type=event`)
- *network scan* (`type=netscan`)



Note: In this document, chapters are organized by the log type and subtype.

Event logs Event log messages record local system events. Event logs have the following subtypes:

- *admin* (`sybtype=admin`): Administrator console, GUI, or CLI logins and logouts.
- *config* (`subtype=config`): Configuration changes.

- *ipsec* (subtype=ipsec): IPsec VPN subsystem events, such as security association (SA) installation and connection negotiation.
- *system* (subtype=system): RAID level changes and other subsystem events, except for IPsec VPN subsystem events.

To log each subtype, you must enable it. For more information on configuring local logging, see the [FortiAnalyzer Administration Guide](#) or the [FortiAnalyzer CLI Reference](#).

To view event log messages that are stored locally, go to *Log & Archive > Log Access > Event Log*, then select *LocalLogs* in the Show drop-down menu.



Tip: If you do not see any logs in this menu location, verify that you have enabled local log storage. The Web-based Manager cannot display log messages that are stored on a remote Syslog server or another FortiAnalyzer unit. For details on configuring local log storage, see the [FortiAnalyzer Administration Guide](#) or the [FortiAnalyzer CLI Reference](#).

Network analyzer logs

Network analyzer logs record packets observed by the network interface that is configured to act as a sniffer, rather than local system events. Sniffer logs have no subtypes.

To log observed packets, you must deploy the FortiAnalyzer unit in your topology where you want to capture packets, then enable the network analyzer feature. For more information, see the [FortiAnalyzer Administration Guide](#) and the [FortiAnalyzer CLI Reference](#).

To view network analyzer log messages, go to *Tools > Network Analyzer > Historical*.

Network scan logs

Netscan logs have two subtypes: discovery and vulnerability.

Log ID numbers

Log messages are identified by their *Log ID* (`log_id=`) number, which is a ten-digit number. Each part of the number indicates something about the nature of the log message.

- **First two digits:** Log type. For FortiAnalyzer units, only the “event” type exists, indicating that all local log messages are categorized as local system events.
- **Second two digits:** Log subtype. The “admin” subtype uses 04, the “config” subtype uses 00, the “ipsec” subtype uses 01, and the “system” subtype uses 06. For more information, see “[Log types and subtypes](#)” on page 10.
- **Last six digits:** An identifier for the specific event which caused the log message, such as a configuration item being deleted. The exact form of the message recorded in the *Message* (`msg=`) field can sometimes vary. However, message permutations sharing the same ID are generally related to the same event. For example, if a log message is too long to fit on one standard-size line, it could be split into multiple log messages with an identical log ID number.



Note: In this document, you can look up the meaning and permutations of a log message by its log ID number.

For example, if a log identification number is 0100000045:

- 01 indicates that it is of the “event” log type
- 00 indicates that it is of the “config” log subtype
- 000045 indicates that its *Message* (msg=) is one of those that is recorded specifically whenever a device configuration item is deleted
- You could look up information about that log message in “0100000045” on [page 44](#).

Log headers vs. bodies

All log messages’ fields belong to one of two parts: the log header or the log body.

The log header contains the date, time, the log identification number, log type, subtype, and severity (priority) level. The log body contains the rest of the log message, which includes the message but can also contain other fields that vary by the specific event.

For example, for this log message:

```
date=2009-12-22 time=13:15:01 log_id=0100000045 type=event
  subtype=config pri=warning device_id=FL800B3908000420
  user=admin ui=GUI(172.20.120.46) action=config msg="User
  deleted device 'FGT5002803033050'"
```

its log header is:

```
date=2009-12-22 time=13:15:01 log_id=0100000045 type=event
  subtype=config pri=warning
```

and its log body is:

```
device_id=FL800B3908000420 user=admin ui=GUI(172.20.120.46)
  action=config msg="User deleted device 'FGT5002803033050'"
```



Note: In this document, for each log ID’s reference table, the *Format* row contains only the log body in order to focus on fields that contain identifying characteristics of that specific log message. It does **not** contain the log header.

3. Event logs: admin subtype



Event log messages of the *admin* subtype record administrative login and logout events.

Log ID numbers of this type and subtype include:

0104000001	0104000008	0104000015
0104000002	0104000009	0104000016
0104000003	0104000010	0104000017
0104000004	0104000011	0104000018
0104000005	0104000013	0104000019

0104000001

Log ID	0104000001
Meaning	The specified administrator attempted to log in to the web-based manager (GUI) or CLI (SSH or telnet or local serial console). The <code>status=</code> field indicates whether the attempt was successful or not. If not successful, the <code>reason=</code> field indicates the cause of the failure. Note: CLI sessions via the JavaScript console widget in the web-based manager are <i>not</i> logged. Such sessions use the same access method as when the administrator logged in to the web-based manager, and therefore you should instead look for the log message that indicates the GUI login.
Severity Level	Alert (attempt failed) or Information (attempt succeeded)
Format	<code>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=login status={failure success} reason={none name_invalid passwd_invalid} msg="User <administrator_name> login {failed successfully} from {console GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)}"</code>

Log ID	010400001
Examples	date=2009-12-22 time=17:01:57 log_id=0104000001 type=event subtype=admin pri= information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=login status= success reason= none msg="User admin login successfully from GUI (172.16.1.20) "
	date=2009-12-21 time=15:55:00 log_id=0104000001 type=event subtype=admin pri= alert device_id=FLG8002704000076 user=amdin ui=GUI(172.20.110.44) action=login status= failure reason= name_invalid msg="User ' amdin ' login failed from GUI(172.20.110.44)"
	date=2009-12-23 time=10:54:51 log_id=0104000001 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=SSH(172.16.1.20) action=login status=success reason=none msg="User admin login successfully from SSH (172.16.1.20) "
	date=2009-12-23 time=11:25:01 log_id=0104000001 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=telnet(172.16.1.20) action=login status=success reason=none msg="User admin login successfully from telnet (172.16.1.20) "
	date=2009-12-23 time=11:11:18 log_id=0104000001 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=console action=login status=success reason=none msg="User admin login successfully from console "

See also

- [0100032120](#)
- [0100032150](#)
- [0100000093](#)

010400002

Log ID	010400002
Meaning	The specified administrator either manually logged out, or the system automatically logged out that administrator because: <ul style="list-style-type: none"> • his or her session was idle for a time which exceeded the idle timeout • in the case of the JavaScript console widget in the web-based manager, the administrator terminated the session implicitly by navigating to a different page
Severity Level	Information

Log ID	0104000002
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>) jsconsole SSH(<ip_address>) telnet(<ip_address>)} action=logout status=success reason={none user_exit} msg="User <administrator_name> {time out logout terminates the session} from {console GUI(<ip_address>) jsconsole ssh(<ip_address>) telnet(<ip_address>)}"
Examples	<p>date=2009-12-23 time=01:03:33 log_id=0104000002 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=logout status=success reason=none msg="User admin time out from GUI(172.16.1.20)"</p> <p>date=2009-12-23 time=10:55:09 log_id=0104000002 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=ssh(172.16.1.20) action=logout status=success reason=user_exit msg="User admin logout from ssh(172.16.1.20)."</p> <p>date=2009-12-23 time=11:25:07 log_id=0104000002 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=telnet(172.16.1.20) action=logout status=success reason=user_exit msg="User admin logout from telnet(172.16.1.20)."</p> <p>date=2009-12-23 time=10:56:59 log_id=0104000002 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=logout status=success reason=user_exit msg="User admin logout from jsconsole."</p> <p>date=2009-12-23 time=01:07:42 log_id=0104000002 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=jsconsole action=logout status=success reason=user_exit msg="User admin terminates the session from jsconsole"</p> <p>date=2009-12-23 time=11:09:00 log_id=0104000002 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=console action=logout status=success reason=user_exit msg="User admin logout from console."</p>

0104000003

Log ID	0104000003
Meaning	An administrator attempted to download a backup copy of the configuration to his or her computer, or upload a backup copy of the configuration to a server. The <code>status</code> field indicates whether the attempt succeeded or failed.
Severity Level	Information
Formats	<pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=backup_config status=success reason=none msg="User <administrator_name> backed up the configuration from GUI(<ip_address>) successfully."</pre> <pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={jsconsole SSH(<ip_address>) telnet(<ip_address>)} action=backup_config status=success reason=none msg="User <administrator_name> backed up the configuration from {jsconsole ssh(<ip_address>) telnet(<ip_address>)} {successfully failed}."</pre>
Examples	<pre>date=2009-08-30 time=20:54:00 log_id=0104000003 type=event subtype=admin pri=information device_id=FLG8002704000076 user=unknown ui=unknown action=backup_config status=success reason=none msg="User unknown backed up the configuration from unknown successfully."</pre> <pre>date=2010-01-12 time=10:57:13 log_id=0104000003 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=backup_config status=success reason=none msg="User admin backed up the configuration from jsconsole successfully."</pre> <pre>date=2010-01-12 time=10:58:15 log_id=0104000003 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=backup_config status=failure reason=none msg="User admin backed up the configuration from jsconsole failed."</pre>

0104000004

Log ID	0104000004
Meaning	An administrator enabled migration mode and, because this FortiAnalyzer unit is configured to act as the destination, it is receiving configuration changes from the source FortiAnalyzer unit.
Severity Level	Information

Log ID	0104000004
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=import_lang status=success reason=none msg="User <administrator_name> changed the configuration from {GUI(<ip_address>) ssh(<ip_address>)} by starting migration."
Example	date=2009-07-22 time=21:30:21 log_id=0104000004 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=ssh(172.16.1.20) action=restore_config status=success reason=none msg="User admin changed the configuration from ssh(172.16.1.20) by starting migration."

See also

- [0100000083](#)

0104000005

Log ID	0104000005
Meaning	An administrator attempted to back up data leak prevention (DLP) archives to an FTP server. The status= field indicates whether the attempt was successful or not.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console ssh(<ip_address>) telnet(<ip_address>)} action=backup_logs status={success failure} reason=none msg="User <administrator_name> backed up <device_name> logs with DLP archives from {console ssh(<ip_address>) telnet(<ip_address>)} to ftp server (<ip_address>) {successfully failed}."
Example	date=2010-01-15 time=16:08:46 log_id=0104000005 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=ssh(172.20.110.77) action=backup_logs status=failure reason=none msg="User admin backed up FGT4002803033146 logs with DLP archives from ssh(172.16.1.20) to ftp server(192.168.1.5) failed."

0104000008

Log ID	0104000008
Meaning	An administrator restored report files from a backup on an FTP server.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console ssh(<ip_address>) telnet(<ip_address>)} status=success reason=none action=restore_reports msg="User <administrator_name> restored reports from {console ssh(<ip_address>) telnet(<ip_address>)} (ftp) successfully."
Example	date=2010-01-15 time=16:31:52 log_id=0104000008 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=ssh(172.16.1.20) action=restore_reports status=success reason=none msg="User admin restored reports from ssh(172.16.1.20) (ftp) successfully."

0104000009

Log ID	0104000009
Meaning	An administrator imported a device log file.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=import_lang status=success reason=none msg="User <administrator_name> imported log file '<file_name>' from GUI(<ip_address>) successfully"
Example	date=2010-01-11 time=15:44:31 log_id=0104000009 type=event subtype=admin pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=import_log status=success reason=none msg="User 'admin' imported log file 'tlog.1263242601.log' from 'GUI(172.16.1.20)' successfully"

0104000010

Log ID	0104000010
Meaning	An administrator imported a report language.
Severity Level	Information

Log ID	0104000010
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=import_lang status=success reason=none msg="User <administrator_name> add language '<language_name>' from {SSH(<ip_address>) GUI(<ip_address>)}"
Example	date=2009-12-23 time=11:38:57 log_id=0104000010 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=import_lang status=success reason=none msg="User admin add language 'British_English' from GUI(172.16.1.20)"

0104000011

Log ID	0104000011
Meaning	An administrator deleted a report language.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=delete_lang status=success reason=none msg="User <administrator_name> delete language '<language_name>' from {SSH(<ip_address>) GUI(<ip_address>)}"
Example	date=2010-01-11 time=16:41:50 log_id=0104000011 type=event subtype=admin pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=delete_lang status=success reason=none msg="User admin delete language 'British_English' from GUI(172.16.1.20)"

0104000013

Log ID	0104000013
Meaning	
Severity Level	Information

Log ID	0104000013
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={SSH(<ip_address>) telnet(<ip_address>)} action=view_certificate status=success reason=none msg="User <administrator_name> import server certificate from {SSH(<ip_address>) telnet(<ip_address>)} {successfully failed}{ftp tftp}."
Example	date=2009-04-21 time=20:29:56 log_id=0104000013 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=telnet(172.16.1.20) action=restore_certificate status=success reason=none msg="User admin import server certificate from telnet(172.16.1.20) successfully(ftp)."

See also

- [0104000015](#)

0104000015

Log ID	0104000015
Meaning	An administrator reset the FortiAnalyzer unit's server certificate to the default certificate included with the currently installed firmware.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={SSH(<ip_address>) telnet(<ip_address>)} action=view_certificate status=success reason=none msg="User <administrator_name> reset the server certificate to its factory state from {SSH(<ip_address>) telnet(<ip_address>)} successfully."
Example	date=2009-04-21 time=18:46:44 log_id=0104000015 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=telnet(172.16.1.20) action=view_certificate status=success reason=none msg="User admin reset the server certificate to its factory state from telnet(172.16.1.20) successfully."

See also

- [0104000013](#)

0104000016

Log ID	0104000016
Meaning	An administrator acknowledged messages in the <i>Alert Message Console</i> widget on the dashboard of the web-based manager. After acknowledgement, log messages are hidden from the <i>Alert Message Console</i> . However, you can still view them in the device and/or local log files.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=ack_alert status=success reason=none msg="Alert messages are acknowledged by <administrator_name>."
Example	date=2010-01-07 time=09:49:36 log_id=0104000016 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=ack_alert status=success reason=none msg="Alert messages are acknowledged by admin."

0104000017

Log ID	0104000017
Meaning	An administrator conducted a migration test.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=migration status=success reason=none msg="User <administrator_name> performed migration test from {GUI(<ip_address>) ssh(<ip_address>) telnet(<ip_address>)}"
Example	date=2009-12-23 time=11:40:07 log_id=0104000017 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=migration status=success reason=none msg="User admin performed migration test from GUI(172.16.1.20)."

0104000018

Log ID	0104000018
Meaning	An administrator executed the command <code>diagnose email parse</code> . This command detects email that cannot be properly parsed for display in content archives, and uploads them to a server. For details, see the FortiAnalyzer CLI Reference .
Severity Level	Information
Formats	<pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=upload_email status=success reason=none msg="User <administrator_name> parsed <total> email(s) of device <device_name> from {GUI(<ip_address>) ssh(<ip_address>) telnet(<ip_address>)}, no emails uploaded."</pre> <pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) SSH(<ip_address>) telnet(<ip_address>)} action=upload_email status=success reason=none msg="User <administrator_name> parsed <total> email(s) of device <device_name> device from {GUI(<ip_address>) ssh(<ip_address>) telnet(<ip_address>)}, <number>/<total> email(s) failed parsing uploaded to ftp server <ftp_server_address> under <folder_path> directory."</pre>
Examples	<pre>date=2009-05-29 time=03:12:10 log_id=0104000018 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=telnet(172.16.1.20) action=upload_email status=success reason=none msg="User admin parsed 5 email(s) of device all device from telnet(172.16.1.20) successfully, no emails uploaded.</pre> <pre>date=2009-05-29 time=15:03:39 log_id=0104000018 type=event subtype=admin pri=information device_id=FLG8002704000076 user=admin ui=telnet(172.16.1.20) action=upload_email status=success reason=none msg="User admin parsed 7 email(s) of all device from telnet(172.16.1.20), 2/2 email(s) failed parsing uploaded to ftp server 192.168.1.50 under home directory."</pre>

0104000019

Log ID	0104000019
Meanings	An administrator created a folder for e-Discovery search results.
	An administrator deleted a folder for e-Discovery search results.
	An administrator added an e-Discovery search task. Results, when complete, will be located in the specified folder.
	An e-Discovery search task finished. Results are located in the specified folder.
	An administrator deleted a set of e-Discovery search results.
Severity Level	Information
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=e_discovery status=success reason=none msg="User <administrator_name> (GUI(<ip_address>)) create ediscovery folder <folder_name>."
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=e_discovery status=success reason=none msg="User <administrator_name> (GUI(<ip_address>)) deleted ediscovery folder <folder_name>."
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=e_discovery status=success reason=none msg="User <administrator_name> (GUI(<ip_address>)) succeeded creating ediscovery task <search_results_name> under folder <folder_name>."
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=e_discovery status=success reason=none msg="Ediscovery task <search_results_name> under folder <folder_name> created by User <administrator_name> (GUI(<ip_address>)) finished."
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=e_discovery status=success reason=none msg="User <administrator_name> (GUI(<ip_address>)) deleted ediscovery task <search_results_name> under folder <folder_name>."
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=e_discovery status=success reason=none msg="User <administrator_name> (GUI(<ip_address>)) deleted ediscovery task <search_results_name> under folder <folder_name>."

Log ID	0104000019
Examples	<p>date=2010-01-06 time=12:22:36 log_id=0104000019 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=e_discovery status=success reason=none msg="User admin (GUI(172.16.1.20)) create ediscovery folder ediscoveryfolder1."</p> <p>date=2010-01-06 time=12:22:57 log_id=0104000019 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=e_discovery status=success reason=none msg="User admin (GUI(172.16.1.20)) deleted ediscovery folder ediscoveryfolder1."</p> <p>date=2010-01-06 time=12:24:38 log_id=0104000019 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=e_discovery status=success reason=none msg="User admin (GUI(172.16.1.20)) succeeded creating ediscovery task search-task1 under folder folder1."</p> <p>date=2010-01-06 time=12:24:45 log_id=0104000019 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=e_discovery status=success reason=none msg="Ediscovery task search-task1 under folder folder1 created by User admin (GUI(172.16.1.20)) finished."</p> <p>date=2010-01-06 time=16:21:40 log_id=0104000019 type=event subtype=admin pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=e_discovery status=success reason=none msg="User admin (GUI(172.16.1.20)) deleted ediscovery task search-task1 under folder ediscovery-folder1."</p>

4. Event logs: config subtype



Event log messages of the *config* subtype record changes that administrators make to the configuration of the FortiAnalyzer unit.

Log ID numbers of this type and subtype include:

010000000	010000038	010000076
010000001	010000039	010000077
010000003	010000040	010000078
010000004	010000041	010000079
010000005	010000042	010000080
010000006	010000043	010000083
010000007	010000044	010000084
010000008	010000045	010000086
010000009	010000046	010000088
010000010	010000047	010000090
010000011	010000048	010000091
010000012	010000049	010000092
010000013	010000050	010000093
010000015	010000052	010000094
010000016	010000053	010000096
010000029	010000054	0100032120
010000030	010000069	0100032122
010000031	010000070	0100032132
010000032	010000071	0100032133
010000034	010000072	0100032134
010000035	010000073	0100032150
010000036	010000074	0100065535
010000037	010000075	

010000000

Log ID	010000000
Meaning	An administrator added, changed, or deleted an administrative access profile.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' {added deleted changed the setting of} access profile <access_profile_name> from GUI(<ip_address>)"
Examples	<pre>date=2010-01-06 time=12:01:19 log_id=0100000000 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' deleted access profile reports_only2 from GUI(172.16.1.20) "</pre> <pre>date=2010-01-06 time=12:01:11 log_id=0100000000 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' added new access profile reports_only from GUI(172.16.1.20) "</pre> <pre>date=2010-01-11 time=13:58:55 log_id=0100000000 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed the setting of access profile read_only from GUI(172.16.1.20) "</pre>

See also

- [0100032120](#)

010000001

Log ID	010000001
Meaning	An administrator added a device to the device list.
Severity Level	Information

Log ID	010000001
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="Device <device_name> added"
Example	date=2010-01-05 time=13:10:50 log_id=0100000001 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="Device FortiWeb-1000B added"

See also

- [0106000028](#)
- [0100000043](#)
- [0100065535](#)

010000003

Log ID	010000003
Meanings	An administrator enabled or disabled network file sharing (NFS). An administrator changed the time zone.
Severity Level	Information
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="NFS network sharing has been turned {on off}" device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the time zone to '<time_zone>'"
Examples	date=2010-01-06 time=12:07:35 log_id=0100000003 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="NFS network sharing has been turned on" date=2010-01-08 time=15:25:07 log_id=0100000003 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed the time zone to '(GMT-5:00) Bogota, Lima, Quito'"

See also

- [0100000041](#)
- [0100000004](#)
- [0100000005](#)
- [0100000008](#)

0100000004

Log ID	0100000004
Meanings	An administrator changed the interval in minutes between each time that the FortiAnalyzer unit connects to the NTP server in order to synchronize its system time.
	An administrator manually changed the system time.
Severity Level	Information
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the NTP server sync interval to <minutes>"
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="System time has been changed"
Example	date=2010-01-11 time=11:19:51 log_id=0100000004 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed the NTP server sync interval to 61"
	date=2010-01-16 time=14:49:49 log_id=0100000004 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=config msg=" System time has been changed"

See also

- [0100000003](#)
- [0100000005](#)
- [0100000008](#)

0100000005

Log ID	0100000005
Meaning	An administrator enabled or disabled synchronization of the FortiAnalyzer unit's system time with a network time protocol (NTP) server.
Severity Level	Information

Log ID	0100000005
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' {enabled disabled} NTP server synchronization"
Example	date=2010-01-08 time=15:26:34 log_id=0100000005 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' enabled NTP server synchronization"

See also

- [0100000003](#)
- [0100000004](#)
- [0100000008](#)

0100000006

Log ID	0100000006
Meaning	An administrator changed the display language of the web-based manager.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the system global language to '<language_name>'"
Example	date=2010-01-06 time=12:02:48 log_id=0100000006 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed the system global language to 'English'"

0100000007

Log ID	0100000007
Meanings	An administrator changed the idle timeout for administrative connections.
	An administrator changed the allocated disk space in megabytes (MB) for e-Discovery.
Severity Level	Information

Log ID	010000007
Formats	<p>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the system timeout from <old_timeout> to <new_timeout> minutes"</p> <p>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the system e-discovery disk quota from <old_megabytes> to <new_megabytes> percentage of reserved space"</p>
Examples	<pre>date=2009-12-22 time=11:16:06 log_id=0100000007 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the system timeout from 5 to 480 minutes"</pre> <pre>date=2010-01-06 time=14:29:30 log_id=0100000007 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed the system e-discovery disk quota from 20480 to 2000 percentage of reserved space"</pre>

010000008

Log ID	010000008
Meaning	An administrator changed which NTP server the FortiAnalyzer unit will use to synchronize its system time.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the sync NTP server from '<old_NTP_server>' to '<new_NTP_server>'"
Example	<pre>date=2010-01-08 time=15:26:34 log_id=0100000008 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed sync NTP server from '' to 'pool.ntp.org'"</pre>

See also

- [010000003](#)
- [010000004](#)
- [010000005](#)

010000009

Log ID	010000009
Meaning	An administrator changed the FortiAnalyzer unit's host name.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User '<administrator_name>' changed the system global hostname from '<old_host_name>' to '<new_host_name>'"
Example	date=2010-01-11 time=11:32:03 log_id=010000009 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' changed the system global hostname from 'FortiAnalyzer-800B' to 'FortiAnalyzer-800B-1'"

010000010

Log ID	010000010
Meaning	An administrator changed the configuration of a network interface.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) msg="Changed system interface from 'name=<port_number> ip=<ip_address_netmask> status={up down} fdp={enable disable} allowaccess={ping https ssh http telnet aggregator webservice} lockout={enable disable}' to 'name=<port_number> ip=<ip_address_netmask> status={up down} fdp={enable disable} allowaccess={ping https ssh http telnet aggregator webservice} lockout={enable disable}' "
Example	date=2009-12-23 time=11:24:37 log_id=010000010 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="Changed system interface from 'name=port1, ip=172.20.120.138 255.255.255.0, status=up, fdp=disable, allowaccess=ping https ssh http , lockout=enable' to 'name=port1, ip=172.20.120.138 255.255.255.0, status=up, fdp=disable, allowaccess=ping https ssh http telnet aggregator we bservice , lockout=enable'"

See also

- [010600037](#)

010000011

Log ID	010000011
Meaning	An administrator added an IP alias.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User added new alias '<alias_name>' ip_range '<ip_alias_addresses>'"
Example	date=2010-01-06 time=11:57:26 log_id=010000011 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User added new alias 'alias1' ip_range '192.168.1.20'"

See also

- [010000013](#)

010000012

Log ID	010000012
Meaning	An administrator changed the local log settings.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="Log Policy has been modified"
Example	date=2010-01-07 time=15:45:12 log_id=010000012 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="Log Policy has been modified"

See also

- [010000083](#)

0100000013

Log ID	0100000013
Meaning	An administrator deleted an IP alias.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=config msg="User added new alias '<alias_name>' ip_range '<ip_alias_addresses>'"
Example	date=2010-01-06 time=11:57:39 log_id=0100000013 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User deleted alias 'alias1' ip_range '192.168.1.20'"

See also

- [0100000011](#)

0100000015

Log ID	0100000015
Meaning	An administrator changed the primary and/or secondary DNS server.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console jsconsole SSH (<ip_address>) telnet(ip_address)} action=config msg="User changed DNS server from '<old_DNS_addresses>' to '<new_DNS_addresses>'"
Example	date=2009-09-04 time=15:59:21 log_id=0100000015 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=config msg="User changed DNS server from 'prim=0.0.0.0, sec=0.0.0.0' to 'prim=192.168.1.10, sec=172.16.1.1'"

See also

- [0106000016](#)

0100000016

Log ID	0100000016
Meaning	<p>An administrator changed the baud rate of local console connections to the CLI.</p> <p>The form of the log message varies by whether the administrator used a <code>set baudrate</code> command in order to specify the new value, or entered <code>unset baudrate</code> to reset that field to its default value.</p> <p>This log message is not recorded if the administrator changed the paged output mode within the same sub-command.</p>
Severity Level	Information
Formats	<pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console jsconsole SSH(<ip_address>) telnet(ip_address)} action=config msg="User changed the console baudrate from '<old_baud_rate>' to '<new_baud_rate>'"</pre> <pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console jsconsole SSH(<ip_address>) telnet(ip_address)} action=config msg="User changed the console baudrate from '<old_baud_rate>' to default '<default_baud_rate>'"</pre>
Examples	<pre>date=2010-01-11 time=14:21:27 log_id=0100000016 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=config msg="User changed the console baudrate from '57600' to '9600'"</pre> <pre>date=2010-01-11 time=14:30:51 log_id=0100000016 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=config msg="User changed the console baudrate from '38400' to default '9600'"</pre>

See also

- [0100000088](#)

0100000029

Log ID	0100000029
Meaning	An administrator added or changed a static route.
Severity Level	Information

Log ID	0100000029
Formats	<pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User edited route from 'seqnum=<route_index>, gateway=<old_ip_address>, dst=<old_ip_range>, device=<old_port>' to 'seqnum=<route_index>, gateway=<new_ip_address>, dst=<old_ip_range>, device=<new_port>'"</pre> <pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User created new route 'seqnum=<route_index>, gateway=<old_ip_address>, dst=<old_ip_range>, device=<old_port>'"</pre>
Examples	<pre>date=2009-12-10 time=08:59:37 log_id=0100000029 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=console action=config msg="User edited route from 'seqnum=1, gateway=192.168.1.1, dst=0.0.0.0-0.0.0.0, device=port1' to 'seqnum=1, gateway=172.20.140.2, dst=0.0.0.0-0.0.0.0, device=port2'"</pre> <pre>date=2010-01-08 time=14:16:07 log_id=0100000029 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=config msg="User created new route 'seqnum=2, gateway=10.10.1.1, dst=10.0.0.0- 255.0.0.0, device=port1'"</pre>

See also

- [0100000030](#)

0100000030

Log ID	0100000030
Meaning	An administrator deleted a static route.
Severity Level	Warning
Format	<pre>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User deleted route 'seqnum=<route_index>, gateway=<ip_address>, dst=<ip_range>, device=<port>'"</pre>
Example	<pre>date=2009-08-05 time=11:41:09 log_id=0100000030 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User deleted route 'seqnum=2, gateway=10.1.110.2, dst=0.0.0.0- 0.0.0.0, device=port1'"</pre>

See also

- [0100000029](#)

0100000031

Log ID	0100000031
Meaning	An administrator changed a network share user account.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=system-built-in ui={console GUI(<ip_address>)} action=config msg="User 'system-built-in' changed the NAS user '<share_user_name>' settings"
Example	date=2010-01-06 time=12:06:36 log_id=0100000031 type=event subtype=config pri=information device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.10) action=config msg="User 'system-built-in' changed the NAS user 'share-user3' settings"

See also

- [0100000032](#)
- [0100000033](#)

0100000032

Log ID	0100000032
Meaning	An administrator added a network share user account.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new NAS user '<share_user_name>' from 'GUI(<ip_address>)'"
Example	date=2009-12-20 time=21:15:05 log_id=0100000032 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new NAS user 'share-user1' from 'GUI(172.16.1.10)'"

See also

- [0100000031](#)
- [0100000033](#)
- [0100000034](#)

0100000033

Log ID	0100000033
Meaning	An administrator deleted a network share user account.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted NAS user '<share_user_name>' "
Example	date=2010-01-06 time=12:06:35 log_id=0100000033 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User deleted NAS user 'share-user2' "

See also

- [0100000031](#)
- [0100000032](#)

0100000034

Log ID	0100000034
Meaning	An administrator changed a network share user group.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the NAS group '<share_group_name>' from 'GUI(<ip_address>)' "
Example	date=2009-07-29 time=07:43:07 log_id=0100000034 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the NAS group 'grp' from 'GUI(172.16.1.10)' "

See also

- [0100000035](#)
- [0100000036](#)

0100000035

Log ID	0100000035
Meaning	An administrator added a network share user group.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new NAS group '<share_group_name>' from 'GUI(<ip_address>)'"
Example	date=2009-07-29 time=07:43:07 log_id=0100000035 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new NAS group 'grp' from 'GUI(172.16.1.10)'"

See also

- [0100000032](#)
- [0100000034](#)
- [0100000036](#)

0100000036

Log ID	0100000036
Meaning	An administrator deleted a network share user group.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=system-built-in ui={console GUI(<ip_address>)} action=config msg="User deleted NAS group '<share_group_name>'"
Example	date=2010-01-06 time=12:07:05 log_id=0100000036 type=event subtype=config pri=warning device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.20) action=config msg="User deleted NAS group 'share-group2'"

See also

- [0100000034](#)
- [0100000035](#)

0100000037

Log ID	0100000037
Meaning	An administrator changed a Windows network share.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the NAS share '<share_name>' from 'GUI(<ip_address>)'"
Example	date=2009-12-20 time=21:18:14 log_id=0100000037 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the NAS share 'report-share' from 'GUI(172.16.1.10)'"

See also

- [0100000038](#)
- [0100000039](#)

0100000038

Log ID	0100000038
Meaning	An administrator added a Windows network share.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new NAS share '<share_name>' from 'GUI(<ip_address>)'"
Example	date=2009-12-20 time=21:13:46 log_id=0100000038 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new NAS share 'report-share' from 'GUI(172.16.1.10)'"

See also

- [0100000037](#)
- [0100000039](#)

0100000039

Log ID	0100000039
Meaning	An administrator deleted a Windows network share.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted NAS share '<share_name>'"
Example	date=2009-07-27 time=13:29:57 log_id=0100000039 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' deleted NAS share 'report-share'"

See also

- [0100000037](#)
- [0100000038](#)

0100000040

Log ID	0100000040
Meaning	An administrator changed an NFS network share.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the NFS sharing '<share_name>' settings"
Example	date=2009-12-20 time=21:41:56 log_id=0100000040 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the NFS sharing 'report-share' settings"

See also

- [0100000041](#)
- [0100000042](#)

0100000041

Log ID	0100000041
Meaning	An administrator added an NFS network share.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new NFS sharing '<share_name>' from 'GUI(<ip_address>)'"
Example	date=2009-12-20 time=21:18:36 log_id=0100000041 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new NFS sharing 'report-share' from 'GUI(172.16.1.10)'"

See also

- [0100000003](#)
- [0100000040](#)
- [0100000042](#)

0100000042

Log ID	0100000042
Meaning	An administrator deleted an NFS network share.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted NFS sharing '<share_name>'"
Example	date=2009-12-20 time=21:18:48 log_id=0100000042 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' deleted NFS sharing 'report-share'"

See also

- [0100000040](#)
- [0100000041](#)

0100000043

Log ID	0100000043
Meaning	An administrator or the system itself (depending on the setting for automatic device list handling) added, renamed, or reconfigured a device in the device list. •
Severity Level	Warning (if the FortiAnalyzer model might not be powerful enough to support the device's maximum log rate) or Information
Formats	<p>device_id=<fortianalyzer_serial_number> user=system ui={data_upgrader fortilogd oftp system} action=config msg="User 'system' added new device '<device_name>'"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui={system} action=config msg="User 'system' changed device '<device_name>'"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui={oftp} action=config msg="User 'system' renamed device '<old_device_name> to <new_device_name>'"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=config msg="The FortiAnalyzer {added new changed} device '<device_serial_number>' automatically."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=fortilogd action=config msg="A higher end FortiAnalyzer is recommended for this model of FortiGate (<device_name>)"</p>

Log ID	010000043
Examples	date=2009-12-15 time=13:49:30 log_id=010000043 type=event subtype=config pri=information device_id=FLG8002704000076 user=system ui= fortilogd action=config msg=" User 'system' added new device 'FG36002804033057'"
	date=2009-12-15 time=13:49:30 log_id=010000043 type=event subtype=config pri=warning device_id=FLG8002704000076 user=system ui=fortilogd action=config msg=" A higher end FortiAnalyzer is recommended for this model of FortiGate (FG36002804033057) "
	date=2010-01-04 time=16:08:13 log_id=010000043 type=event subtype=config pri=information device_id=FL800B3908000420 user=system ui= oftp action=config msg="User 'system' added new device 'FMG40A3906500505'"
	date=2009-12-15 time=10:56:39 log_id=010000043 type=event subtype=config pri=information device_id=FLG8002704000076 user=system ui= oftp action=config msg="User 'system' renamed device 'FG36002804033057' to 'FortiGate-3600-Floor2'"
	date=2009-12-15 time=14:32:49 log_id=010000043 type=event subtype=config pri=information device_id=FLG8002704000076 user=system ui= system action=config msg=" The FortiAnalyzer changed device 'FG200A3907550170' automatically. "
	date=2009-12-15 time=14:32:49 log_id=010000043 type=event subtype=config pri=information device_id=FLG8002704000076 user=system ui=system action=config msg="The FortiAnalyzer added new device 'FG200A3907550170' automatically. "

See also

- 010000001
- 0100065535
- 0106000028

010000044

Log ID	010000044
Meaning	An administrator changed a device.
Severity Level	Information

Log ID	0100000044
Format	device_id=<fortianalyzer_serial_number> user=system ui={console GUI(<ip_address>)}ftp ssh(<ip_address>) telnet(ip_address)} action=config msg="User '<administrator_name>' changed device <device_name> settings"
Example	date=2009-12-08 time=05:42:48 log_id=0100000044 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=console action=config msg="User 'admin' changed device 'FGT-400-Floor2' settings"

See also

- [0100000043](#)

0100000045

Log ID	0100000045
Meaning	An administrator deleted a device.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User deleted device <device_name>"
Example	date=2009-12-15 time=14:32:41 log_id=0100000045 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User deleted device 'FG200A3907550170'"

See also

- [0100000046](#)
- [0100000047](#)

0100000046

Log ID	0100000046
Meaning	An administrator changed a device group.
Severity Level	Information

Log ID	0100000046
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the device group '<device_group_name>' settings"
Example	date=2009-12-22 time=12:00:01 log_id=0100000046 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the device group 'devicegroup1' settings"

See also

- [0100000045](#)
- [0100000047](#)
- [0100000048](#)

0100000047

Log ID	0100000047
Meaning	An administrator added a device group.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added device group '<device_group_name>' from '{console GUI(<ip_address>)}'"
Example	date=2009-12-22 time=11:59:38 log_id=0100000047 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added device group 'grp' from 'GUI(172.16.1.10)'"

See also

- [0100000045](#)
- [0100000046](#)
- [0100000048](#)

0100000048

Log ID	0100000048
Meaning	An administrator deleted a device group.
Severity Level	Warning

Log ID	0100000048
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name>ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted device group <device_group_name>"
Example	date=2010-01-06 time=12:20:49 log_id=0100000048 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User deleted device group 'devicegroup2'"

See also

- [0100000045](#)
- [0100000046](#)
- [0100000047](#)

0100000049

Log ID	0100000049
Meaning	An administrator changed the devices' default log settings.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>) SSH(<ip_address>) telnet(ip_address)} action=config msg="User '<administrator_name>' changed the {logs log rolling} settings"
Examples	<p>date=2009-12-18 time=10:16:16 log_id=0100000049 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI (172.16.1.10) action=config msg="User 'admin' changed the logs settings"</p> <p>date=2009-12-18 time=10:15:32 log_id=0100000049 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=telnet (172.16.1.10) action=config msg="User 'admin' changed the logs settings"</p> <p>date=2009-12-18 time=09:33:19 log_id=0100000049 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=console action=config msg="User 'admin' changed the logs settings"</p> <p>date=2009-11-26 time=16:45:53 log_id=0100000049 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the log rolling settings"</p>

0100000050

Log ID	0100000050
Meaning	An administrator changed the network area storage (NAS) settings.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the NAS protocol from 'nfs={enabled disabled}, share={enabled disabled}, workgroup=<old_workgroup_name>nfs={enabled disabled}, share={enabled disabled}, workgroup=<new_workgroup_name>"
Example	date=2009-12-20 time=21:15:46 log_id=0100000050 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the NAS protocol from 'nfs=enabled, share=enabled, workgroup=' settings to 'nfs=enabled, share=enabled, workgroup="

0100000052

Log ID	0100000052
Meaning	An administrator changed a report output, layout, or schedule.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' edited report {layout profile output profile schedule} '<profile_name>"
Examples	date=2009-12-22 time=15:03:51 log_id=0100000052 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' edited report layout profile 'report-layout1'" date=2009-12-22 time=15:12:56 log_id=0100000052 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' edited report output profile 'report-output1'"

See also

- [0100000053](#)
- [0100000054](#)

0100000053

Log ID	0100000053
Meaning	An administrator added a report output, layout, or schedule.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new report {output profile layout profile schedule} <profile_name>"
Examples	<pre>date=2009-12-23 time=15:42:07 log_id=0100000053 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new report schedule 'report-schedule1'" date=2009-12-23 time=15:41:59 log_id=0100000053 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new report layout profile 'report-layout1'"</pre>

See also

- [0100000052](#)
- [0100000054](#)

0100000054

Log ID	0100000054
Meaning	An administrator deleted a report layout or schedule.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted report schedule <schedule_name>"
Examples	<pre>date=2009-12-23 time=15:45:00 log_id=0100000054 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' deleted report schedule 'schedule1'"</pre>

See also

- [0100000052](#)
- [0100000053](#)

0100000069

Log ID	0100000069
Meaning	An administrator deleted an SNMP community.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted the snmp-trap '<snmp_community_name>'"
Example	date=2010-01-06 time=12:38:04 log_id=0100000069 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User deleted snmp-trap 'public'"

See also

- [0100000070](#)
- [0100000071](#)
- [0100065535](#)

0100000070

Log ID	0100000070
Meaning	An administrator changed an SNMP community.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the snmp-trap '<snmp_community_name>' settings"
Example	date=2009-12-22 time=16:52:18 log_id=0100000070 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the snmp-trap 'public' settings"

See also

- [0100000069](#)
- [0100000071](#)
- [0100065535](#)

0100000071

Log ID	0100000071
Meaning	An administrator added an SNMP community.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new snmp-trap '<snmp_trap_name>' settings"
Example	date=2009-12-22 time=16:52:18 log_id=0100000071 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new snmp-trap 'public' settings"

See also

- [0100000069](#)
- [0100000070](#)
- [0100065535](#)

0100000072

Log ID	0100000072
Meaning	An administrator deleted a Syslog alert server.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted syslog server '<syslog_alert_server>' configurations"
Example	date=2010-01-06 time=12:37:45 log_id=0100000072 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User deleted syslog server 'syslog-alerts2' configurations"

See also

- [0100000073](#)
- [0100000074](#)

0100000073

Log ID	0100000073
Meaning	An administrator changed a Syslog alert server.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=system-built-in ui={console GUI(<ip_address>)} action=config msg="User 'system-built-in' changed the syslog server '<syslog_alert_server>' settings"
Example	date=2010-01-06 time=12:37:43 log_id=0100000073 type=event subtype=config pri=information device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.20) action=config msg="User 'system-built-in' changed the syslog server 'syslog-alerts2' settings"

See also

- [0100000072](#)
- [0100000074](#)

0100000074

Log ID	0100000074
Meaning	An administrator added a Syslog alert server.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new syslog server '<syslog_alert_server>' settings"
Example	date=2009-12-22 time=16:53:28 log_id=0100000074 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new syslog server 'syslog-alerts1' settings"

See also

- [0100000072](#)
- [0100000073](#)

0100000075

Log ID	0100000075
Meaning	An administrator deleted an alert event.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User deleted alert-event '<alert_name>'"
Example	date=2009-12-18 time=13:49:24 log_id=0100000075 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User deleted alert-event 'alert1'"

See also

- [0100000076](#)
- [0100000077](#)

0100000076

Log ID	0100000076
Meaning	An administrator changed an alert event.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed the alert- event '<alert_name>' settings"
Example	date=2009-12-18 time=14:15:25 log_id=0100000076 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' changed the alert-event 'alert1' settings"

See also

- [0100000075](#)
- [0100000077](#)

0100000077

Log ID	0100000077
Meaning	An administrator added an alert event.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new alert-event '<alert_name>' settings"
Example	date=2009-12-18 time=14:15:25 log_id=0100000077 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="User 'admin' added new alert-event 'alert1'"

See also

- [0100000075](#)
- [0100000076](#)

0100000078

Log ID	0100000078
Meaning	An administrator deleted an alert email server.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User deleted mail server '<alert_mail_server>' settings "
Example	date=2010-01-06 time=12:34:55 log_id=0100000078 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User deleted mail server 'mail.example.com' settings "

See also

- [0100000079](#)
- [0100000080](#)

0100000079

Log ID	0100000079
Meaning	An administrator changed an alert email server.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=system-built-in ui={console GUI(<ip_address>)} action=config msg="User 'system-built-in' changed the mail server '<alert_mail_server>' settings"
Example	date=2010-01-06 time=12:34:53 log_id=0100000079 type=event subtype=config pri=information device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.20) action=config msg="User 'system-built-in' changed the mail server 'mail.example.com' settings"

See also

- [0100000078](#)
- [0100000080](#)

0100000080

Log ID	0100000080
Meaning	An administrator added an alert email server. Mail servers are required in order to deliver alert email messages.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added new mail server '<alert_server_name>' settings"
Example	date=2009-12-22 time=15:12:15 log_id=0100000080 type=event subtype=config pri=information device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' added new mail server 'mail.fortinet.com'"

See also

- [0106000036](#)
- [0100000078](#)
- [0100000079](#)

0100000083

Log ID	0100000083
Meanings	An administrator changed the local log settings' automatic log file deletion settings.
	An administrator enabled or disabled migration mode, with this FortiAnalyzer unit acting as either a source or destination.
Severity Level	Information
Formats	device_id=<fortianalyzer_serial_number> user=system-built-in ui= GUI(<ip_address>) action=config msg= "User 'system-built-in' changed the autodelete settings"
	device_id=<fortianalyzer_serial_number> user=system-built-in ui= GUI(<ip_address>) action=config msg= "User '<administrator_name>' {enabled disabled} '{source destination}' migration mode."
Examples	date=2010-01-07 time=15:45:12 log_id=0100000083 type=event subtype=config pri=information device_id=FL800B3908000420 user=system-built-in ui=GUI(172.16.1.20) action=config msg="User 'system-built-in' changed the autodelete settings "
	date=2010-01-11 time=15:08:03 log_id=0100000083 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' disabled 'destination' migration mode. "

See also

- [0100000012](#)
- [0104000004](#)
- [0106000040](#)

0100000084

Log ID	0100000084
Meaning	An administrator removed a disk from the RAID array.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui= GUI(<ip_address>) action=config msg= "User '<administrator_name>' delete disk<disk_number> from RAID array"

0100000086

Log ID	0100000086
Meaning	An administrator attempted to remove a device or device group, but the action failed because it was in use by another part of the configuration, such as a device group.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=console action=config msg="Unable to delete device[group] '<device_name>', it is used by <i>n</i> higher level object(s)
Example	date=2009-06-24 time=10:31:26 log_id=0100000086 type=event subtype=config pri=warning device_id=FLG8002704000076 user=admin ui=console action=config msg="Unable to delete device 'FGT60M2904400538', it is used by 1 higher level object(s) "

0100000088

Log ID	0100000088
Meaning	An administrator changed the CLI paged display option.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console jsconsole SSH(<ip_address>) telnet(ip_address)} action=config msg="User changed the console output option"
Example	date=2010-01-11 time=14:17:26 log_id=0100000088 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=config msg="User changed the console output option"

See also

- [0100000016](#)

0100000090

Log ID	0100000090
Meaning	An administrator deleted an LDAP server query.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="A ldap server is deleted"
Example	date=2010-01-06 time=11:58:25 log_id=0100000090 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="A ldap server is deleted"

See also

- [0100000091](#)
- [0100000092](#)

0100000091

Log ID	0100000091
Meaning	An administrator changed LDAP server query.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="A ldap server's setting is changed"
Example	date=2009-12-04 time=15:03:16 log_id=0100000091 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=config msg="A ldap server's setting is changed"

See also

- [0100000090](#)
- [0100000092](#)

0100000092

Log ID	0100000092
Meaning	An administrator added an LDAP server query.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="A new ldap server is added"
Example	date=2009-12-11 time=06:16:00 log_id=0100000092 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=config msg="A new ldap server is added"

See also

- [0100000090](#)
- [0100000091](#)

0100000093

Log ID	0100000093
Meaning	An administrator changed the maximum number of concurrently logged-in administrators. This setting is available only from the CLI. For more information, see the FortiAnalyzer CLI Reference .
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console jsconsole SSH(<ip_address>) telnet(ip_address)} action=config msg="User '<administrator_name>' changed the system max concurrent users from <old_limit> to <new_limit>"
Example	date=2010-01-11 time=11:37:30 log_id=0100000093 type=event subtype=config pri=information device_id=FL800B3908000420 user=admin ui=jsconsole action=config msg="User 'admin' changed the system max concurrent users from 10 to 20"

See also

- [0104000001](#)

0100000094

Log ID	0100000094
Meaning	An administrator added a new administrative domain (ADOM).
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>) telnet(ip_address)} action=config msg="User '<administrator_name>' added a domain <ADOM_name> from {console GUI(<ip_address>) telnet(ip_address)}"
Example	date=2009-12-08 time=10:36:26 log_id=0100000094 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=telnet(172.16.1.10) action=config msg="User 'admin' added a domain adom1 from telnet(172.16.1.10) "

See also

- [0100000094](#)

0100000096

Log ID	0100000096
Meaning	An administrator deleted an administrative domain (ADOM).
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>) telnet(ip_address)} action=config msg="User '<administrator_name>' deleted domain <ADOM_name> from {SSH(<ip_address>) GUI(<ip_address>)}"
Example	date=2009-12-08 time=11:23:39 log_id=0100000096 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=telnet(172.16.1.10) action=config msg="User 'admin' deleted domain adom1 from telnet(172.16.1.10) "

See also

- [0100000096](#)

0100032120

Log ID	0100032120
Meaning	An administrator added an administrator account.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added an admin user <deleted_administrator_account> from {console GUI(<ip_address>)}"
Example	date=2010-01-06 time=12:00:20 log_id=0100032120 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' added an admin user admin3 from GUI(172.16.1.20) "

See also

- [0100000000](#)
- [0100032122](#)
- [0104000001](#)

0100032122

Log ID	0100032122
Meaning	An administrator deleted an administrator account.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted an admin user <deleted_administrator_account> from {console GUI(<ip_address>)}"
Example	date=2010-01-06 time=12:00:43 log_id=0100032122 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User 'admin' deleted an admin user admin4 from GUI(172.16.1.20) "

See also

- [0100032120](#)

0100032132

Log ID	0100032132
Meaning	An administrator added a RADIUS server.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' added radius server <radius_server_name> from {console GUI(<ip_address>)}"
Example	date=2010-01-06 time=12:02:19 log_id=0100032134 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User admin added radius server radius3 from GUI(172.16.1.20) "

See also

- [0100032133](#)
- [0100032134](#)

0100032133

Log ID	0100032133
Meaning	An administrator changed a RADIUS server.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' changed a radius server <radius_server_name> from {console GUI(<ip_address>)}.name=<radius_name> old_server=<old_ip_address> new_server=<new_ip_address> secret=<secret>"
Example	date=2010-01-06 time=12:02:17 log_id=0100032133 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User admin changed a radius server radius3 setting from GUI(172.16.1.20).name=radius3 old_server=192.168.1.10 new_server=192.168.1.20 secret=mysecret"

See also

- [0100032132](#)
- [0100032134](#)

0100032134

Log ID	0100032134
Meaning	An administrator deleted a RADIUS server.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="User '<administrator_name>' deleted radius server <radius_server_name> from {console GUI(<ip_address>)}"
Example	date=2010-01-06 time=12:02:20 log_id=0100032134 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=config msg="User admin deleted radius server radius3 from GUI(172.16.1.20)"

See also

- [0100032132](#)
- [0100032133](#)

0100032150

Log ID	0100032150
Meaning	An administrator changed the password of an administrator account.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={console GUI(<ip_address>)} action=config msg="Admin user <current_administrator_name> changed password of admin user <administrator_name>"
Example	date=2010-01-06 time=12:00:41 log_id=0100032150 type=event subtype=config pri=warning device_id=FL800B3908000420 user=admin1 ui=GUI(172.16.20) action=config msg="Admin user admin1 changed password of admin user admin4"

See also

- [0104000001](#)

0100065535

Log ID	0100065535
Meaning	An administrator added, changed, or deleted the settings of a configuration object.
Severity Level	Notification
Examples	<pre>date=2009-12-22 time=16:53:29 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of system.syslog(unix) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=16:53:08 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin changed settings of system.snmp.sysinfo from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=16:52:18 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of system.snmp.community(public) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=15:12:55 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of report.output(1) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=15:12:16 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of system.mail(mail.example.com) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=15:03:49 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of report.layout(New) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=14:51:13 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of vm.business-risk(DEFAULT) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=12:00:01 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin changed settings of log.device-group(grp) from GUI(172.16.1.10) "</pre> <pre>date=2009-12-22 time=11:59:39 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin added a new entry of log.device-group(grp) from GUI(172.16.1.10) "</pre>

Log ID	0100065535
	date=2009-12-22 time=11:20:55 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin changed settings of system.alert-console from GUI(172.16.1.10) "
	date=2009-12-22 time=11:16:06 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin changed settings of system.global from GUI(172.16.1.10) "
	date=2009-12-18 time=15:38:13 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=system ui=cmf action=config msg="Administrator system added a new entry of log.device(FG600D2423423) from cmf"
	date=2009-12-18 time=14:19:55 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=system ui=cmf action=config msg="Administrator system deleted an entry of vm.sensor(vcm_pci_sensor) from cmf"
	date=2009-12-18 time=14:19:55 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=system ui=cmf action=config msg="Administrator system deleted an entry of vm.scan-profile(vcm_pci_profile) from cmf"
	date=2009-12-16 time=15:00:20 log_id=0100065535 type=event subtype=config pri=notice device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=config msg="Administrator admin changed settings of system.interface(port2) from GUI(172.16.1.10) "
	date=2010-01-07 time=08:21:04 log_id=0100065535 type=event subtype=config pri=notice device_id=FL800B3908000420 user=admin ui=console action=config msg="Administrator admin changed settings of log.settings from console"

See also

- [0106000028](#)
- [0100000043](#)
- [0100000001](#)

5. Event logs: ipsec subtype

Event log messages of the *ipsec* subtype record IPsec VPN events

IPsec VPNs can be established with connecting devices in order to secure their log and/or DLP archive transmissions if you have configured both the FortiAnalyzer unit and the device to use a secure connection. For details, see the [FortiAnalyzer CLI Reference](#) and the [FortiAnalyzer Administration Guide](#).

Log ID	0101000000 or other subsequent numbers
Meanings	Quick mode messages in Phase I completed successfully. Aggressive mode encryption method negotiations in Phase I completed successfully. Phase I key exchange (IKE) negotiations completed successfully and the resulting security association (SA) was installed.
Severity Level	Notification
Formats	device_id=<fortianalyzer_serial_number> loc_ip=<fortianalyzer_ip_address> loc_port=500 rem_ip=<device_ip_address> rem_port=500 out_if=vpn_tunnel=<device_name> action={negotiate install sa} {init=remote mode={quick aggressive} stage={1 2} dir=outbound status=success} in_spi=<in_SPI> out_spi=<out_SPI>} msg="<IPSec_message>"

Log ID	0101000000 or other subsequent numbers
Examples	<pre> date=2009-12-22 time=16:51:28 log_id=0101000000 type=event subtype=ipsec pri=notice device_id=FL800B3908000420 loc_ip=172.16.1.20 loc_port=500 rem_ip=172.16.1.30 rem_port=500 out_if=vpn_tunnel=Gateway_Firewall action=negotiate init=remote mode=quick stage=1 dir=outbound status=success msg="Responder: sent 172.16.1.30 quick mode message #1 (OK)" date=2009-12-23 time=05:41:56 log_id=0101000000 type=event subtype=ipsec pri=notice device_id=FL800B3908000420 loc_ip=172.16.1.20 loc_port=500 rem_ip=172.16.1.30 rem_port=500 out_if=vpn_tunnel=Gateway_Firewall action=negotiate init=remote mode=aggressive stage=1 dir=outbound status=success msg="Responder: sent 172.16.1.30 aggressive mode message #1 (OK)" date=2009-12-23 time=05:41:56 log_id=0101000000 type=event subtype=ipsec pri=notice device_id=FL800B3908000420 loc_ip=172.16.1.20 loc_port=500 rem_ip=172.16.1.30 rem_port=500 out_if=vpn_tunnel=Gateway_Firewall action=negotiate init=remote mode=aggressive stage=2 dir=inbound status=success msg="Responder: parsed 172.16.1.30 aggressive mode message #2 (DONE)" date=2009-12-23 time=06:13:27 log_id=0101000000 type=event subtype=ipsec pri=notice device_id=FL800B3908000420 loc_ip=172.16.1.20 loc_port=500 rem_ip=172.16.1.30 rem_port=500 out_if=vpn_tunnel=Gateway_Firewall action=install_sa, in_spi=2975e37c out_spi=2c0edd2b msg="Responder: tunnel 172.16.1.20/172.16.1.30 install ipsec sa" </pre>

6. Event logs: system subtype



Event log messages of the *system* subtype record subsystem events such as reboots and RAID level changes.



Note: The system subtype does *not* include IPsec VPN subsystem events. For details on logs of the *ipsec* subtype, see “[Event logs: ipsec subtype](#)” on page 65.

Log ID numbers of this type and subtype include:

0106000001	0106000017	0106000030
0106000005	0106000018	0106000035
0106000006	0106000019	0106000036
0106000007	0106000021	0106000037
0106000009	0106000023	0106000038
0106000010	0106000024	0106000040
0106000012	0106000025	0106131090
0106000014	0106000028	0106131091
0106000016	0106000029	

0106000001

Log ID	0106000001
Meaning	An administrator rebooted the FortiAnalyzer unit.
Severity Level	Warning (administrator command) or Information (system-initiated action)
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=reboot status=success msg="System has been restarted by user '<administrator_name>' via GUI(<ip_address>)" device_id=<fortianalyzer_serial_number> user=system ui=system action=reboot status=success msg="The system is rebooting!"

Log ID	0106000001
Examples	date=2009-12-01 time=12:13:55 log_id=0106000001 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.20.140.52) action=reboot status=success msg="System has been restarted by user 'admin' via GUI(172.20.140.52) "
	date=2009-12-17 time=17:07:47 log_id=0106000001 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=reboot status=success msg="The system is rebooting!"

See also

- [0106131090](#)

0106000005

Log ID	0106000005
Meaning	An administrator reset the configuration to its default values for the currently installed firmware version.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=upgrade status=success msg="System has been reset to factory default by user '<administrator_name>' via GUI(<ip_address>)"
Example	date=2010-01-07 time=11:16:16 log_id=0106000005 type=event subtype=system pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=factory_reset status=success msg="System has been reset to factory default by user 'admin' via GUI(172.16.1.20) "

See also

- [0106000006](#)
- [0106000010](#)

0106000006

Log ID	0106000006
Meaning	An administrator restored the configuration using a configuration backup file.
Severity Level	Warning

Log ID	0106000006
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=upgrade status=success msg="System configuration file has been restored by user '<administrator_name>' via GUI(<ip_address>)"
Example	date=2010-01-07 time=08:28:58 log_id=0106000006 type=event subtype=system pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.20.120.104) action=restore status=success msg="System configuration file has been restored by user 'admin' via GUI(172.16.1.20)"

See also

- [0106000005](#)
- [0106000010](#)

0106000007

Log ID	0106000007
Meaning	An administrator attempted to install firmware that was a newer version than the currently installed firmware. Success or failure of the attempt is indicated by the <code>status</code> field.
Severity Level	Warning (administrator-initiated success or failure) or Information
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=upgrade status=success msg="System firmware has been upgraded by user <administrator_name> via GUI(<ip_address>)" device_id=<fortianalyzer_serial_number> user=system ui=system action=upgrade status=success msg="The system is upgrading!" device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=upgrade status=failure msg="Upgrade system firmware failed: incompatible image for this platform by user <administrator_name> via GUI(<ip_address>)"

Log ID	0106000007
Examples	date=2009-12-03 time=14:50:44 log_id=0106000007 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=upgrade status= success msg=" System firmware has been upgraded by user 'admin' via GUI(172.16.1.10) "
	date=2009-12-03 time=14:50:46 log_id=0106000007 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=upgrade status=success msg="The system is upgrading!"
	date=2009-11-27 time=15:29:18 log_id=0106000007 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=upgrade status= failure msg=" Upgrade system firmware failed: incompatible image for this platform by user 'admin' via GUI(172.16.1.10) "

See also

- [0106000014](#)

0106000009

Log ID	0106000009
Meaning	An administrator attempted to download an email attachment file, data leak prevention (DLP) archive file, a quarantine file, a log file, current log view, remote vulnerability scan (RVS) report file, packet log (Network Analyzer) file, or a report language file. The <code>status</code> field indicates whether the attempt succeeded or failed.
Severity Level	Warning
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=download status=success msg="{ Current log view Email attachment DLP archive Logging Packet Log Quarantine Report Language rvs } file has been downloaded by user <administrator_name> via GUI(<ip_address>)"
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=download status=failure msg="Download { Current log view eDiscovery result file Email attachment DLP archive Logging Packet Log Quarantine Report Language rvs } file failed by user <administrator_name> via GUI(<ip_address>)"

Log ID	0106000009
Examples	date=2009-12-23 time=11:38:19 log_id=0106000009 type=event subtype=system pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=download status=success msg="Report Language file has been downloaded by user 'admin' via GUI(172.16.1.20) "
	date=2009-12-22 time=14:40:25 log_id=0106000009 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=download status=success msg="DLP archive file has been downloaded by user 'admin' via GUI(172.16.1.10) "
	date=2010-01-07 time=09:40:08 log_id=0106000009 type=event subtype=system pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=download status=failure msg="Download eDiscovery result file failed by user 'admin' via GUI(172.16.1.20) "

See also

- [0106000010](#)

0106000010

Log ID	0106000010
Meanings	An administrator downloaded a configuration backup file.
	The FortiAnalyzer unit successfully uploaded a log file to an FTP, SFTP, or SCP server, according to schedule.
	The FortiAnalyzer unit failed to upload a log file to an FTP, SFTP, or SCP server, and, after 10 retries and 600 seconds, abandoned the attempt.
Severity Level	Error (upload failed), Warning, or Notification (upload succeeded)
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=upload status=success msg="System config file has been backed up by user '<administrator_name>' via GUI(<ip_address>)"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=upload status=success msg="Upload of log file <file_name> {succeeded failed}."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=upload status=failure msg="Too many failed attempts(<file_name>), deleting upload request for host <ip_address>."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=upload status=failure msg="SSH Fatal Error:fatal: Timeout before authentication for <ip_address>."

Log ID	0106000010
Examples	date=2010-01-07 time=11:15:57 log_id=0106000010 type=event subtype=system pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=upload status=success msg=" System config file has been backed up by user 'admin' via GUI(172.16.1.20) "
	date=2010-01-12 time=12:02:47 log_id=0106000010 type=event subtype=system pri=notice device_id=FL800B3908000420 user=system ui=system action=upload status=success msg=" Upload of log file FE-4002905500226-eelog.1255422385.log-2009-10-16-04-31-59.gz succeeded."
	date=2009-12-21 time=17:05:19 log_id=0106000010 type=event subtype=system pri=error device_id=FLG8002704000076 user=system ui=system action=upload status=failure msg=" Too many failed attempts (core file or crash log fortilogd.dbg.tgz), deleting upload request for host 172.16.1.20."
	date=2010-01-15 time=11:39:43 log_id=0106000010 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=upload status=failure msg="SSH Fatal Error:fatal: Timeout before authentication for 172.16.1.20."

See also

- [0106000005](#)
- [0106000006](#)
- [0106000009](#)

0106000012

Log ID	0106000012
Meaning	A log file or data leak prevention (DLP) archive, intrusion prevention system (IPS) packet log file, or report file was deleted or trimmed by a FortiAnalyzer administrator, or the FortiAnalyzer unit itself.
Severity Level	Warning (administrator-initiated), Notification (system-initiated to enforce disk space quota), or Information (device-initiated)
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name>} ui={GUI(<ip_address>)} action=del_log status=success msg="Device Log file <file_name> deleted by user '<administrator_name>' via GUI(<ip_address>)"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Deleted <number> log files of <device_name>, to enforce the device's space quota."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Device <device_name> Log file <file_name> deleted"

<p>Log ID</p>	<p>0106000012</p> <p>device_id=<fortianalyzer_serial_number> user=<administrator_name> ui={GUI(<ip_address>) jsconsole } action=del_log status=success msg="DLP summaries and archives for device <device_name> deleted by '<administrator_name>' via {GUI(<ip_address>) jsconsole}"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Trimmed <number> log files of <device_name> in total, to enforce the device's space quota"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Trimmed log file <file_name>, to enforce the device's space quota"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Deleted IPS content archive files of <device_name>[totally], which are older than <number> hour"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Deleted DLP archive files of <device_name>[totally], which are older than <number> hour"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_log status=success msg="Delete report [<report_name>], which is older than <number> month"</p>
<p>Examples</p>	<p>date=2009-12-10 time=03:41:53 log_id=0106000012 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.20.110.60) action=del_log status=success msg="Device Log file tlog.2.log deleted by user 'admin' via GUI(172.20.110.60) "</p> <p>date=2010-01-05 time=15:41:48 log_id=0106000012 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=del_log status=success msg="Deleted 2 log files of FGT4002803033148, to enforce the device's space quota."</p> <p>date=2009-12-22 time=15:29:29 log_id=0106000012 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=del_log status=success msg="Device FG200A3907550170 Log file tlog.1.log deleted"</p> <p>date=2009-12-22 time=16:43:50 log_id=0106000012 type=event subtype=system pri=information device_id=FL800B3908000420 user=system ui=system action=del_log status=success msg="Device .self Log file elog.log deleted"</p> <p>date=2009-12-22 time=16:43:58 log_id=0106000012 type=event subtype=system pri=information device_id=FL800B3908000420 user=system ui=system action=del_log status=success msg="Device .sniffer Log file xlog.log deleted"</p>

Log ID	0106000012
	date=2009-09-04 time=21:54:39 log_id=0106000012 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=jsconsole action=del_log status=success msg="DLP summaries and archives for device F60DSL2906500707 deleted by user 'admin' via jsconsole"
	date=2009-09-02 time=08:16:19 log_id=0106000012 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=del_log status=success msg="Trimmed log file tlog.log, to enforce the device's space quota"
	date=2009-07-11 time=14:48:00 log_id=0106000012 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=del_log status=success msg="Deleted IPS content archive files of FGT60M2904400538, which are older than 1 hour"
	date=2009-07-11 time=14:48:00 log_id=0106000012 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=del_log status=success msg="Deleted DLP archive files of FGT60M2904400538, which are older than 1 hour"
	date=2010-01-12 time=10:48:00 log_id=0106000012 type=event subtype=system pri=notice device_id=FL800B3908000420 user=system ui=system action=del_log status=success msg="Delete report [report1-2009-08-12-1404] , which is older than 1 month"

See also

- [0106000017](#)

0106000014

Log ID	0106000014
Meaning	An administrator installed firmware that was an older version than the currently installed firmware. Downgrading can cause configuration loss if a configured feature is not supported in the older firmware version.
Severity Level	Warning
Formats	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui= GUI(<ip_address>) action=downgrade status=success msg="System firmware has been downgraded by user <administrator_name> via GUI(<ip_address>)" device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=console action=downgrade status=success msg="Firmware has been downgraded."

Log ID	0106000014
Examples	date=2009-12-20 time=21:06:14 log_id=0106000014 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=downgrade status=success msg="System firmware has been downgraded by user 'admin' via GUI(172.16.1.10) "
	date=2009-04-16 time=14:30:23 log_id=0106000014 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=console action=downgrade status=success msg="Firmware has been downgraded."

See also

- [0106000007](#)

0106000016

Log ID	0106000016
Meanings	During startup, the FortiAnalyzer unit detected that the log disk has not recently been checked for errors.
	During startup, the FortiAnalyzer unit detected that the log disk was not unmounted properly during the previous shutdown.
	During startup, the FortiAnalyzer unit detected that the configured default route's gateway IP address is not valid.
	During startup, the FortiAnalyzer unit detected that one of the DNS servers is not reachable.
Actions	Log in to the CLI and enter the command <code>syntax diag sys file-system fsfix</code> to fix the errors. For more information, see the FortiAnalyzer CLI Reference .
	Log in to the CLI and enter the command <code>syntax diag sys file-system fsfix</code> to fix the errors. For more information, see the FortiAnalyzer CLI Reference .
	Change the default static route's gateway IP address so that it is on the same subnet as the network interface's IP address.
	Change the IP address of the primary and secondary DNS servers to ones that can be reliably reached. Alternatively, you can locate the source of connectivity issues using the CLI command <code>execute traceroute <gateway_ipv4></code> . For more information, see the FortiAnalyzer CLI Reference .
Severity Level	Warning (file system not checked, or unmounted improperly) or Alert (incorrect gateway or DNS server address)

Log ID	0106000016
Formats	<p>device_id=<fortianalyzer_serial_number> user=system ui=system action=bootup status=success msg="The log disk has not been checked for errors for <number> mounts. You should run 'diag sys file-system fsfix'. If unsuccessful, you can also try running 'diag sys file-system fsrebuild'."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=bootup status=success msg="The log disk was not unmounted properly. You should run 'diag sys file-system fsfix'."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=bootup status=success msg="The configured default gateway address is invalid. The gateway address must be on the same subnet as the interface address."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=bootup status=success msg="The configured {primary secondary} DNS server is not reachable. A valid DNS server is required for resolving IP addresses to hostnames in reports."</p>
Examples	<p>date=2009-12-18 time=15:38:07 log_id=0106000016 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=bootup status=success msg="The log disk has not been checked for errors for 184 mounts. You should run 'diag sys file-system fsfix'. If unsuccessful, you can also try running 'diag sys file-system fsrebuild'."</p> <p>date=2009-12-24 time=04:59:54 log_id=0106000016 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=bootup status=success msg="The log disk was not unmounted properly. You should run 'diag sys file-system fsfix'."</p> <p>date=2010-01-05 time=17:32:41 log_id=0106000016 type=event subtype=system pri=alert device_id=FL800B3908000420 user=system ui=system action=bootup status=success msg="The configured default gateway address is invalid. The gateway address must be on the same subnet as the interface address."</p> <p>date=2009-05-28 time=07:51:36 log_id=0106000016 type=event subtype=system pri=alert device_id=FLG8002704000076 user=system ui=system action=bootup status=success msg="The configured secondary DNS server is not reachable. A valid DNS server is required for resolving IP addresses to hostnames in reports."</p>

See also

- [0100000015](#)

0106000017

Log ID	0106000017
Meanings	The report generator started generating a report.
	The report generator finished generating a report.
	A report was deleted.
	The report generator encountered an error.
	The report generator encountered a DNS query timeout.
	The report generator is rebuilding a GUI dashboard widget's report.
Severity Level	Notification or Information (timeout or operations error)
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg="Start generating report [<name of report_yyyy-mm-dd-ss>] at <dayofweek> (<day>) <yyyy-mm-dd> <hh:mm:ss>"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg="Report [<name of report_yyyy-mm-dd-ss>] finished at <dayofweek> (<day>) <yyyy-mm-dd> <hh:mm:ss>"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg="Report [<name of report_yyyy-mm-dd-ss>] deleted at <dayofweek> (<day>) <yyyy-mm-dd> <hh:mm:ss>"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg="Operations error"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg="Timed out"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg="User deleted all dashboard widget's reports to be rebuilt. The system is rebuilding them."
Examples	date=2009-12-10 time=00:01:30 log_id=0106000017 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=report status=success msg=" Start generating report [Scheduled-54321-2009-12-10-0000] at Thu (4) 2009-12-10 00:01:30."
	date=2009-12-10 time=00:01:38 log_id=0106000017 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=report status=success msg=" Report [Scheduled-54321-2009-12-10-0000] finished at Thu (4) 2009-12-10 00:01:38."
	date=2009-12-23 time=10:00:08 log_id=0106000017 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=report status=success msg="Report [54321-2009-12-08-0818] deleted at Wed (3) 2009-12-23 10:00:08."

Log ID	0106000017
	date=2009-12-07 time=00:00:01 log_id=0106000017 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=report status=failure msg=" Operations error "
	date=2009-12-03 time=00:01:00 log_id=0106000017 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=report status=failure msg=" Timed out "
	date=2009-11-18 time=20:18:58 log_id=0106000017 type=event subtype=system pri=notice device_id=FLG8002704000076 user=admin ui=jsconsole action=report status=success msg="User deleted all dashboard widget's reports to be rebuilt . The system is rebuilding them."
	date=2010-01-12 time=10:48:00 log_id=0106000017 type=event subtype=system pri=notice device_id=FL800B3908000420 user=system ui=system action=report status=success msg=" Delete 3 reports totally, which are older than 1 month "

See also

- [0106000012](#)
- [0106000018](#)

0106000018

Log ID	0106000018
Meaning	An administrator renamed a report.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=ren_log status=success msg="<old_report_name> has been renamed as <new_report_name> by user '<administrator_name>' via GUI(<ip_address>)"
Example	date=2010-01-06 time=12:27:38 log_id=0106000018 type=event subtype=system pri=warning device_id=FL800B3908000420 user=admin ui=GUI(172.16.1.20) action=ren_log status=success msg="Report Bandwidth_Analysis_Copy_003-2010-01-06- 1227 has been renamed as Bandwidth_Analysis_Copy_1 by user 'admin' via GUI(172.16.1.20)"

See also

- [0106000017](#)

0106000019

Log ID	0106000019
Meaning	An administrator deleted a quarantine file.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=quarantine status=success msg="n quarantine file(s) deleted by user '<administrator_name>' via GUI(<ip_address>)"
Example	date=2010-01-14 time=16:36:07 log_id=0106000019 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.20) action=quarantine status=success msg="1 quarantine file(s) deleted by user 'admin' via GUI(172.16.1.20) "

0106000021

Log ID	0106000021
Meanings	A vulnerability management package upload and installation was started or finished.
	A vulnerability management package download from the FDN was started or finished.
	A scheduled vulnerability scan was started or finished.
	An administrator cancelled a scheduled vulnerability management scan.
Severity Level	Information
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=scan status=success msg="VM package initial installation {started finished}."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=scan status=success msg="rvsagent {start finish} copy so file: <file_id>"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=scan status=success msg="VM {map scan} schedule (<scan_name>) has been {started finished} by system."
	device_id=<fortianalyzer_serial_number> user=system ui=GUI action=scan status=success msg="VM job (<rvs_schedule_name>) has been {started stopped} manually by <administrator_name> via GUI."
	device_id=<fortianalyzer_serial_number> user=system ui=GUI action=scan status=success msg="VM schedule (<rvs_schedule_name>) has been {started stopped} manually by <administrator_name> via CLI."

Log ID	0106000021
Examples	<p>date=2009-12-16 time=11:10:51 log_id=0106000021 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=scan status=success msg="VM package initial installation started."</p> <p>date=2009-12-16 time=11:11:14 log_id=0106000021 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=scan status=success msg="VM package initial installation finished."</p> <p>date=2009-12-15 time=13:49:16 log_id=0106000021 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=scan status=success msg="rvsagent start copy so file: 1260884956"</p> <p>date=2009-12-15 time=13:49:28 log_id=0106000021 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=scan status=success msg="rvsagent finish copy so file: 1260884967"</p> <p>date=2009-12-30 time=10:55:05 log_id=0106000021 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=scan status=success msg="VM scan schedule (assetsch) has been started by system."</p> <p>date=2009-12-30 time=16:33:14 log_id=0106000021 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=scan status=success msg="VM scan schedule (assetsch) has been finished by system."</p> <p>date=2010-01-06 time=12:43:43 log_id=0106000021 type=event subtype=system pri=information device_id=FL800B3908000420 user=system ui=GUI action=scan status=success msg="VM job (rvs-schedule1) has been stopped manually by admin via GUI."</p> <p>date=2010-01-13 time=15:40:18 log_id=0106000021 type=event subtype=system pri=information device_id=FL800B3908000420 user=system ui=CLI action=scan status=success msg="VM schedule (rvs-schedule1) has been started by admin via CLI."</p>

See also

- [0106000038](#)

0106000023

Log ID	0106000023
Meanings	A vulnerability management scan or network map report has been generated.
	A vulnerability management scan, compliance, or network map report has been deleted.
Severity Level	Notification (report deleted) or Information (report created)
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg= "VM{map scan} report (<vm_report_name><yyyy-mm-dd_<yyyy-mm-dd>_<hh:mm:ss>_<yyyy-mm-dd>_<hh:mm:ss>) has been created by system."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=report status=success msg= "Report [<report_name>] has been deleted."
	device_id=<fortianalyzer_serial_number> user=system ui=CLI action=report status=success msg= "Clear Reports: <number> reports of [{map scan compliance}] have been deleted."
Examples	date=2009-12-30 time=16:33:14 log_id=0106000023 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=report status=success msg="VM scan report (assetsch-2009-12-30-1055_2009-12-30_10:55:03_2009-12-30_16:32:54) has been created by system."
	date=2010-01-13 time=15:03:44 log_id=0106000023 type=event subtype=system pri=notice device_id=FL800B3908000420 user=system ui=GUI(172.16.1.20) action=report status=success msg="Report [rvs-schedule1-2010-01-13-1502-A] has been deleted ."
	date=2010-01-13 time=15:55:03 log_id=0106000023 type=event subtype=system pri=notice device_id=FL800B3908000420 user=system ui=CLI action=report status=success msg="Clear Reports: 1 reports of [map] have been deleted."

0106000024

Log ID	0106000024
Meanings	The FortiAnalyzer successfully upgraded its vulnerability modules.
	When connecting to the FortiGuard Distribution Network (FDN), the FortiAnalyzer unit did not have a valid license for the vulnerability module upgrade service.
Severity Level	Error (for failure) or Information (for success)

Log ID	0106000024
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=upgrade status=success msg= "VM Upgrade: Package installed ok, Object type [VMPL]"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=upgrade status=failure msg= "VM upgrade: Invalid VM license."
Examples	date=2010-01-13 time=04:53:57 log_id=0106000024 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=upgrade status=success msg="VM Upgrade: Package installed ok, Object type [VMPL]"
	date=2010-01-06 time=12:18:27 log_id=0106000024 type=event subtype=system pri=error device_id=FL800B3908000420 user=system ui=system action=upgrade status=failure msg="VM upgrade: Invalid VM license."

0106000025

Log ID	0106000025
Meanings	An unregistered device was added to the unregistration device list.
	The logging daemon, fortilogd, is starting.
	The logging daemon is recording the total log volume for the day.
	The logging daemon is saving the local, Network Analyzer, or device's current log file according to the date, and starting a new log file ("rolling").
	The new firmware image has a valid RSA signature.
	The logging daemon will soon stop accepting new content archive and quarantine files from one of the devices because it is about to consume its allotted disk space quota.
	The logging daemon will resume accepting new content archive and quarantine files from one of the devices because some files have been removed, and it now has some available disk space within its disk space quota.
	A device whose logs were initialled received indirectly, via log aggregation from another FortiAnalyzer unit, is now logging directly to this FortiAnalyzer unit.
Severity Level	Warning (log disk space has been freed, or logs are being received from an aggregated device), Alert (log disk quota is almost consumed), Notification, or Information (total log volume for the day)
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=log status=success msg="Add unregistered device <device_name> to unregistered table"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=log status=success msg="Fortilogd is starting."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=log status=success msg="Log volume for <mm> <dd>, <yyyy>: <volme_number>MB, <day_number> average: <number>MB."

Log ID	0106000025
	device_id=<fortianalyzer_serial_number> user=system ui=system action=log status=success msg="Roll <roll_number_sequential> log files of device [<i><device_name></i> <i>Network Analyzer</i> <i>Local</i>]."
	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=GUI(<ip_address>) action=log status=success msg="The new image does have a valid RSA signature. by user ' <i><administrator_name></i> ' via <i>GUI(<ip_address>)</i> "
	device_id=<fortianalyzer_serial_number> user=system ui=system action=log status=success msg="Device files reach 95% of the space quota of the device: <i><device_name></i> . The system will stop accepting new content archive and quarantine files"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=log status=success msg="Device files is below quota: <i><device_name></i> . The system will resume receiving content archive and quarantine files"
	The device FGT4002803033220, aggregated from FAZ:FLG8002704000042, is now logging directly to this FAZ.
Examples	date=2009-12-15 time=09:30:37 log_id=0106000025 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=log status=success msg="Add unregistered device SYSLOG-172.20.110.78 to unregistered table"
	date=2009-12-24 time=04:59:48 log_id=0106000025 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=log status=success msg=" Fortilogd is starting "
	date=2009-12-30 time=00:00:06 log_id=0106000025 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=log status=success msg=" Log volume for Dec 29, 2009: 289.24 MB, 7 day average: 290.72 MB"
	date=2009-12-29 time=23:57:25 log_id=0106000025 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=log status=success msg=" Rolled 1 log file of device[FGT4002803033149]"
	date=2009-12-18 time=14:17:01 log_id=0106000025 type=event subtype=system pri=warning device_id=FLG8002704000076 user=admin ui=GUI(172.16.1.10) action=log status=success msg="The new image does have a valid RSA signature . by user 'admin' via GUI(172.16.1.10) "
	date=2010-01-12 time=11:01:41 log_id=0106000025 type=event subtype=system pri=notice device_id=FL800B3908000420 user=system ui=system action=log status=success msg=" Rolled 1 log file of device[NetworkAnalyzer]"

Log ID	0106000025
	date=2009-09-02 time=12:40:08 log_id=0106000025 type=event subtype=system pri=alert device_id=FLG8002704000076 user=system ui=system action=log status=success msg="Device files reach 95% of the space quota of the device: FG500A0000000001. The system will stop accepting new content archive and quarantine files"
	date=2009-09-02 time=07:30:34 log_id=0106000025 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=log status=success msg="Device files is below quota : FG500A0000000001. The system will resume receiving content archive and quarantine files"
	date=2009-06-09 time=21:16:05 log_id=0106000025 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=log status=success msg="The device FGT4002803033220, aggregated from FAZ:FLG8002704000042, is now logging directly to this FAZ."

See also

- [0106000028](#)

0106000028

Log ID	0106000028
Meanings	The specified device was automatically registered to the device list, or (for generic Syslog devices) was added to the unregistered device table. The specified device could not be automatically registered because there was not enough disk space left to allocate to it.
Severity Level	Warning
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=add_device status=success msg="Log device <device_serial_number> is registered automatically." device_id=<fortianalyzer_serial_number> user=system ui=system action=add_device status=success msg="Added unregistered device SYSLOG-<ip_address> to unregistered table" device_id=<fortianalyzer_serial_number> user=system ui=system action=add_device status=success msg="Log device <device_serial_number> can not be registered automatically due to no disk quota available."

Log ID	0106000028
Examples	date=2010-01-05 time=14:24:39 log_id=0106000028 type=event subtype=system pri=warning device_id=FL800B3908000420 user=system ui=system action=add_device status=success msg="Log device FMG3KB3F09000109 is registered automatically. "
	date=2009-12-24 time=04:59:47 log_id=0106000028 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=add_device status=success msg=" Added unregistered device SYSLOG-172.16.1.20 to unregistered table"
	date=2010-01-15 time=12:01:20 log_id=0106000028 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=add_device status=success msg="Log device FGT4002803033886 can not be registered automatically due to no disk quota available."

See also

- [0100065535](#)
- [0100000043](#)
- [0100000001](#)

0106000029

Log ID	0106000029
Meanings	The RAID subsystem is started rebuilding the array.
	The RAID subsystem has synchronized the array.
	The RAID subsystem has finished rebuilding the array.
	The RAID subsystem has corrected an error on the array.
	The RAID subsystem has detected that the array is missing a disk.
	The RAID subsystem status is now OK.
Severity Level	Alert, Warning, or Error
Format	device_id=<fortianalyzer_serial_number> user=system ui=system action=RAID status=success msg="<RAID_message>"

Log ID	0106000029
Examples	<pre>date=2009-07-21 time=12:46:56 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="RAID rebuilding process started."</pre>
	<pre>date=2009-07-21 time=12:46:56 log_id=0106000029 type=event subtype=system pri=error device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="md: md0: raid array is not clean -- starting background reconstruction"</pre>
	<pre>date=2009-07-21 time=12:47:12 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="md: syncing RAID array md0"</pre>
	<pre>date=2009-07-21 time=12:47:16 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="md: resuming recovery of md0 from checkpoint."</pre>
	<pre>date=2009-07-22 time=07:10:59 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="md: md0: sync done."</pre>
	<pre>date=2009-07-22 time=07:11:27 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="RAID rebuilding process finished."</pre>
	<pre>date=2009-07-22 time=07:11:27 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="RAID status changes to OK."</pre>
	<pre>date=2009-08-17 time=16:34:06 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="raid10: raid set md0 active with 0 out of 4 devices"</pre>
	<pre>date=2009-07-23 time=12:43:41 log_id=0106000029 type=event subtype=system pri=error device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="raid10: hdel: rescheduling sector 120"</pre>
	<pre>date=2009-07-23 time=12:43:41 log_id=0106000029 type=event subtype=system pri=error device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="raid10: hdel: redirecting sector 120 to another mirror"</pre>

Log ID	0106000029
Examples	date=2009-07-24 time=13:14:54 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="raid10:md0: read error corrected (8 sectors at 0 on hde1)"
	date=2009-08-17 time=16:34:05 log_id=0106000029 type=event subtype=system pri=warning device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="raid10: disk01 Missing (2) "
	date=2009-08-16 time=05:47:09 log_id=0106000029 type=event subtype=system pri=alert device_id=FLG8002704000089 user=system ui=system action=RAID status=success msg="md: kicking non-fresh hde1 from array!"
	date=2010-01-07 time=11:40:23 log_id=0106000029 type=event subtype=system pri=warning device_id=FL800B3908000420 user=system ui=system action=RAID status=success msg="raid1: raid set md0 active with 4 out of 4 mirrors"

0106000030

Log ID	0106000030
Meanings	The FortiAnalyzer unit has started, is in progress, or has finished a log aggregation session.
	The FortiAnalyzer unit rejected an aggregation request from a client because it is not configured for log aggregation.
	The FortiAnalyzer unit accepted an aggregation request from a client.
	The FortiAnalyzer unit aborted a log aggregation session from a client in order to enforce the disk space quota.
	The FortiAnalyzer unit could not aggregate logs because the server was not reachable, or the password was incorrect.
	The FortiAnalyzer unit's log aggregation session was aborted by the server in order to enforce the disk space quota.
	The FortiAnalyzer unit's log aggregation session was rejected because the server is not configured for log aggregation.
Severity Level	Warning (any log aggregation failure) or Notification

Log ID	0106000030
Formats	<p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation is starting"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation to the remote FortiAnalyzer(<aggregation_server_address>) starts for device <device_name>."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation for device <device_serial_number> is finished."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="No log files to be aggregated for device FG1KBD2423423"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation session completed."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation is exiting."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation request from FortiAnalyzer <client_serial_number> for device <device_name> is rejected because this device is not an aggregated device."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation request from FortiAnalyzer <client_serial_number> for device <device_name> is accepted."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation request from FortiAnalyzer <client_serial_number> for device <device_name> is aborted, because the disk quota for this device will be used up with more aggregation."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation failed. The password was incorrect or the server was unreachable."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation from <aggregation_client_address> failed because password was incorrect."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg="Log aggregation for device <device_name> is aborted, because the disk quota for this device on the remote FortiAnalyzer(<server_ip_address>) will be used up with more aggregation."</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=aggregation status=success msg=Log aggregation for device <device_name> fails because it is not an aggregated device on remote FortiAnalyzer(<server_ip_address>)."</p>

Log ID	0106000030
Examples	<p>date=2010-01-08 time=00:00:01 log_id=0106000030 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation is starting"</p> <p>date=2010-01-08 time=00:00:02 log_id=0106000030 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation to the remote FortiAnalyzer(192.168.1.30) starts for device All_FortiClients."</p> <p>date=2010-01-08 time=00:00:12 log_id=0106000030 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation for device FortiClient is finished."</p> <p>date=2010-01-08 time=00:00:50 log_id=0106000030 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="No log files to be aggregated for device FG1KBD2423423"</p> <p>date=2010-01-08 time=00:34:51 log_id=0106000030 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation session completed."</p> <p>date=2010-01-08 time=00:34:51 log_id=0106000030 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation is exiting."</p> <p>date=2009-12-15 time=14:33:30 log_id=0106000030 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation request from FortiAnalyzer FLG8002704000046 for device SYSLOG-172.16.1.50 is rejected because this device is not an aggregated device."</p> <p>date=2009-12-15 time=18:57:08 log_id=0106000030 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation request from FortiAnalyzer FLG8002704000046 for device FGT60M2904400348 is accepted"</p>

Log ID	0106000030
	date=2009-12-15 time=18:57:08 log_id=0106000030 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation from FortiAnalyzer FLG8002704000046 for device FGT60M2904400348 is aborted, because the disk quota for this device will be used up with more aggregation."
	date=2010-01-08 time=13:47:27 log_id=0106000030 type=event subtype=system pri=warning device_id=FL800B3908000420 user=system ui=system action=aggregation status=success msg="Log aggregation failed. The password was incorrect or the server was unreachable. "
	date=2009-12-18 time=03:01:07 log_id=0106000030 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=aggregation status=success msg="Log aggregation from 192.168.1.20 failed because password was incorrect. "
	date=2010-01-08 time=13:47:27 log_id=0106000030 type=event subtype=system pri=warning device_id=FL800B3908000420 user=system ui=system action=aggregation status=success msg="Log aggregation for device SYSLOG-172.16.1.50 is aborted, because the disk quota for this device on the remote FortiAnalyzer(192.168.1.30) will be used up with more aggregation. "
	date=2010-01-08 time=13:47:27 log_id=0106000030 type=event subtype=system pri=warning device_id=FL800B3908000420 user=system ui=system action=aggregation status=success msg="Log aggregation for device SYSLOG-172.16.1.50 fails because it is not an aggregated device on remote FortiAnalyzer (192.168.1.30)."

0106000035

Log ID	0106000035
Meanings	Because an administrator deleted a log file that had associated content archive files, the FortiAnalyzer unit automatically deleted the associated content archive files in order to reclaim disk space. The FortiAnalyzer unit automatically deleted some of the oldest content archive files in order to enforce disk space quota.
Severity Level	Notification (automatic deletion to enforce quota) or Information

Log ID	0106000035
Formats	<p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_archive status=success msg="{IPS packet log Quarantined} files related to <log_file_name> for device <device_name> deleted"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_archive status=success msg="{IPS packet log Quarantined} files for device <device_name> deleted"</p> <p>device_id=<fortianalyzer_serial_number> user=system ui=system action=del_archive status=success msg="Deleted all {IPS packet log quarantine content archive} files of <device_name>, to enforce the device's space quota."</p>
Examples	<p>date=2009-10-07 time=07:07:25 log_id=0106000035 type=event subtype=system pri=information device_id=FLG8002704000076 user=system ui=system action=del_archive status=success msg="Quarantined files related to vlog.1250600801.log for device FG400A2905500095_CID deleted"</p> <p>date=2009-05-13 time=14:12:14 log_id=0106000035 type=event subtype=system pri=notice device_id=FLG8002704000076 user=system ui=system action=del_archive status=success msg="Deleted all content archive and quarantine files of FG500A2904559391, to enforce the device's space quota."</p>

0106000036

Log ID	0106000036
Meanings	<p>The FortiAnalyzer unit successfully sent an alert email using the SMTP server.</p> <p>The FortiAnalyzer unit could not send an alert email using the SMTP server.</p> <p>The FortiAnalyzer unit was able to initiate a session with the SMTP server in order to begin sending an alert email, but the session then timed out due to being idle, and the alert email was not successfully sent.</p>
Action	<p>Verify that the FortiAnalyzer unit can reliably reach the alert mail server, and that the SMTP protocol is permitted along that path. Also, if the mail server requires SMTP authentication, configure the FortiAnalyzer unit to authenticate with a user name and password. For details on using <code>execute traceroute</code> to locate connectivity failures, see the FortiAnalyzer CLI Reference.</p>
Severity Level	Warning

Log ID	0106000036
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=send_mail status=failure msg="Send mail to SMTP server <alert_mail_server> failed."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=send_mail status=failure msg="Sending-mail session is closed by SMTP server."
	device_id=<fortianalyzer_serial_number> user=system ui=system action=send_mail status=failure msg="Sending mail proceed more than 300 seconds, time out."
Examples	date=2009-08-07 time=00:33:21 log_id=0106000036 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=send_mail status=failure msg="Sending-mail session is closed by SMTP server. "
	date=2010-01-06 time=12:34:48 log_id=0106000036 type=event subtype=system pri=warning device_id=FL800B3908000420 user=system ui=system action=send_mail status=failure msg=" Send mail to SMTP server mail.example.com failed. "
	date=2010-01-16 time=14:48:21 log_id=0106000036 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=send_mail status=failure msg="Sending mail proceed more than 300 seconds, time out. "

See also

- [0100000080](#)

0106000037

Log ID	0106000037
Meanings	An administrator brought up (enabled) or brought down (disabled) a network interface.
	To preserve system stability, the FortiAnalyzer unit automatically killed a daemon because it was consuming too much memory.
Action	If a daemon is terminated automatically, please contact Fortinet Technical Support .
Severity Level	Warning
Formats	device_id=<fortianalyzer_serial_number> user=system ui=system action=monitor status=success msg="Network Interface (<network_interface_name>) is {up down}"
	device_id=<fortianalyzer_serial_number> user=system ui=system action=monitor status=failure msg="Killing process <daemon_name> due to high memory usage [RSS:n KB, VM:m KB]"

Log ID	0106000037
Examples	date=2009-11-27 time=09:15:57 log_id=0106000037 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=monitor status=success msg="Network Interface (port 1) is up"
	date=2009-10-30 time=19:09:36 log_id=0106000037 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=monitor status=failure msg="Killing process httpsd due to high memory usage [RSS:271044 KB, VM:730440 KB]."

See also

- [0100000010](#)

0106000038

Log ID	0106000038
Meaning	An administrator started or stopped, via the CLI, a vulnerability scan report based upon a network map.
Severity Level	Information
Format	device_id=<fortianalyzer_serial_number> user=system ui=CLI action=map status=success msg="VM map-config (<rvs_map_name>) has been {started stopped} by <administrator_name> via CLI."
Example	date=2010-01-13 time=15:42:44 log_id=0106000038 type=event subtype=system pri=information device_id=FL800B3908000420 user=system ui=CLI action=map status=success msg="VM map-config (vuln-map1) has been started by admin via CLI."

See also

- [0106000021](#)

0106000040

Log ID	0106000040
Meaning	Authentication with the destination FortiAnalyzer unit for migration mode failed.
Severity Level	Warning

Log ID	0106000040
Format	device_id=<fortianalyzer_serial_number> user=system ui=system action=migration status=failure msg="Error: Authentication on peer failed."
Example	date=2009-07-22 time=21:47:43 log_id=0106000040 type=event subtype=system pri=warning device_id=FLG8002704000076 user=system ui=system action=migration status=failure msg="Error: Authentication on peer failed."

0106131090

Log ID	0106131090
Meaning	An administrator halted the operating system and shut down the FortiAnalyzer unit.
Severity Level	Warning
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=ssh(<ip_address>) action=unknown status=success msg=" '<administrator_name>' is shutting down the system from 'ssh(<ip_address>)'"
Example	date=2010-01-15 time=20:22:59 log_id=0106131090 type=event subtype=system pri=warning device_id=FL100B3107000276 user=admin ui=ssh(172.16.1.20) action=unknown status=success msg=" 'admin' is shutting down the system from 'ssh(172.16.1.20)'"

See also

- [0106000001](#)

0106131091

Log ID	0106131091
Meaning	An administrator reloaded the configuration using the CLI command <code>execute reload</code> .
Severity Level	Warning

Log ID	0106131091
Format	device_id=<fortianalyzer_serial_number> user=<administrator_name> ui=ssh(<ip_address>) action=unknown status=success msg=" '<administrator_name>' is reloading system configurations from the ssh(<ip_address>)"
Example	date=2010-01-15 time=20:38:56 log_id=0106131091 type=event subtype=system pri=warning device_id=FL100B3107000276 user=admin ui=ssh(172.16.1.20) action=unknown status=success msg=" 'admin' is reloading system configurations from the ssh(172.16.1.20) "

See also

- [0106000001](#)

7. Network Analyzer logs



Network Analyzer log messages are recorded only when Network Analyzer is enabled. The Network Analyzer feature can be used as an enhanced local network traffic sniffer to diagnose areas of the network where firewall policies may require adjustment, or where traffic anomalies occur.

Network Analyzer log files are located on the web-based manager in *Tools > Network Analyzer > Browse*. Network Analyzer logs have their own log file name, `xlog.log`. For more information about how to enable and use the network analyzer, see the *FortiAnalyzer Administration Guide*.

Network Analyzer log messages do not contain a logsubtype, and they also do not contain a log ID number.

The following is an example of a network analyzer log message:

```
itime=1269272053 type=sniffer src=172.16.1.50 dst=172.16.1.20
src_port=80 dst_port=4115 proto=tcp msg="HTTP -> 4115 [ ACK ]
Ack=2296376837"
```

Table 3: Explanation of the network analyzer log message example

itime=1269272053	The time in milliseconds.
type=sniffer	Indicates that the log message is related to packets observed by a network interface used by the network analyzer, rather than one caused by local system events.
src=172.16.1.50	The source IP address.
dst=172.22.1.20	The destination IP address.
src_port=80	The source port number.
dst_port=4115	The destination port number.
proto=tcp	The protocol that was used. In this example, the protocol was TCP. The protocol may be another, however, such as Fortinet Discovery Protocol (FDP), UDP or ARP.
msg="HTTP -> 4115 [ACK] Ack=2296376837"	The message whose contents vary by the protocol. In this example, the application protocol was HTTP, whose message contains TCP transmission control signals such as FIN, ACK and PSH, but not the HTTP payload, such as HTML or GIF files. For UDP, the message indicates the length, such as <code>UDP length=599</code> . For ARP, the message indicates the query or reply, such as <code>arp reply 172.20.120.138 is-at 0:1d:92:a1:82:aa</code> . For FDP, the message indicates the protocol action, such as <code>FDP HELLO from device FortiAnalyzer</code> .

8. Netscan logs: discovery subtype



Netscan log messages of the *discovery* subtype record network scanning activities performed by the FortiGate unit.

The action field can contain one of the following values:

- scan
- host-detection
- vuln-detection
- service-detection
- port-detection
- os-scan
- vuln-count

Log ID numbers of this type and subtype include:

1100000097	1100000100	1100000104
1100000099	1100000102	1100000105

1100000097

Log ID	1100000097
Meaning	A network scan was performed.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> action=<action> ip=<ip_address> start=<start_time> end=<end_time> status=<scan_status> engine=<netscan_engine_version> plugin=<netscan_plugin_version>

1100000099

Log ID	1100000099
Meaning	A network scan was performed.
Severity Level	Notification

Log ID	1100000099
Format	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> action=<action> ip=<ip_address> os=<os_name> os_family=<os_family> os_gen=<os_gen> os_vendor=<os_company>
Example	date=2012-02-21 time=15:41:40 log_id=4099 type=netscan subtype=discovery pri=notice device_id=FL100B3107004729 vd=root scan_name="Allen_PC" action="os-scan" ip="172.16.79.170" os="Linux 2.6.9 - 2.6.29 (likely FC 9/10/11)" os_family="Linux" os_gen="2.6.X" os_vendor="Linux"

1100000100

Log ID	1100000100
Meaning	A network scan was performed.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> action=<action> ip=<ip_address> service=<detected_service> proto=<protocol> port=<port_number>

1100000102

Log ID	1100000102
Meaning	A network scan was performed.
Severity Level	Notification
Formats	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> action=<action> msg=<log_message_info>

1100000104

Log ID	1100000104
Meaning	A network host was detected. The method field can contain one of the following values: <ul style="list-style-type: none"> • ARP • ICMP • TCP • UDP
Severity Level	Notification
Formats	device_id=<fortianalyzer_serial_number> vd=<administrator_name> scan_name=<device> action=host-detection ip=<ip_address> method=<discovery_method> asset_id=<asset_definition> asset_name=<asset_definition_name> vuln=<total_vulns>
Example	date=2012-02-21 time=15:41:25 log_id=4104 type=netscan subtype=discovery pri=notice device_id=FL100B3107004729 vd=root scan_name="Allen_PC" action="host-detection" ip="172.16.79.170" method="ARP" asset_id=1 asset_name="Allen_PC"

1100000105

Log ID	1100000105
Meanings	A netscan port was detected.
Severity Level	Notification
Formats	device_id=<fortianalyzer_serial_number> vd=<administrator_name> scan_name=<device> action=port-detection ip=<ip_address> proto=<protocol> port=<port_number>
Examples	date=2012-02-21 time=15:41:28 log_id=4105 type=netscan subtype=discovery pri=notice device_id=FL100B3107004729 vd=root scan_name="Allen_PC" action="port-detection" ip="172.16.79.170" proto="tcp" port=22

9. Netscan logs: vulnerability subtype



Netscan log messages of the *vulnerability* subtype record network scanning activities performed by the FortiGate unit.

The `action` field can contain one of the following:

- scan
- host-detection
- vuln-detection
- service-detection
- port-detection
- os-scan
- vuln-count

Log ID numbers of this type and subtype include:

1101000096 1101000101
1101000098 1101000103

1101000096

Log ID	1101000096
Meaning	A network scan was performed. The status field can contain one of the following values: <ul style="list-style-type: none">• start• stop• pause• resume• complete
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> action=<action> ip=<ip_address> start=<start_time> end=<end_time> status=<scan_status> engine=<netscan_engine_version> plugin=<netscan_plugin_version>

1101000098

Log ID	1101000098
Meaning	A network scan vulnerability was detected. The severity field can contain one of the following values: <ul style="list-style-type: none"> • cirticial • high • medium • low • info
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> scan_name=<device> action=<action> ip=<ip_address> vuln=<detected_vuln> vuln_cat=<vuln_category> vuln_id=<vuln_id_number> vuln_ref=<link_to_vuln_page> severity=<severity> proto=<protocol> port=<port_number>
Examples	<pre>date=2012-02-21 time=15:41:46 log_id=4098 type=netscan subtype=vulnerability pri=notice device_id=FL100B3107004729 vd=root scan_name="Allen_PC" action="vuln-detection" ip="172.16.79.170" vuln="SSH.Server.Type.Version" vuln_cat="Remote Access" vuln_id=8 vuln_ref="http://www.fortinet.com/ids/VID18300" severity="low" vuln_score=0.0 proto="tcp" port=22</pre> <pre>date=2012-02-21 time=15:41:56 log_id=4098 type=netscan subtype=vulnerability pri=notice device_id=FL100B3107004729 vd=root scan_name="Allen_PC" action="vuln-detection" ip="172.16.79.170" vuln="GNU.Tar.rmt.Client.Implementation.Buffer.Overflow.Vuln" vuln_cat="Applications" vuln_id=22692 vuln_ref="http://www.fortinet.com/ids/VID25510" severity="medium" vuln_score=7.5 proto="tcp" port=0</pre>

1101000101

Log ID	1101000101
Meaning	A network scan notification.
Severity Level	Notification
Format	device_id=<fortianalyzer_serial_number> vd=<virtual_domain_name> action=<action> msg=<log_message_info>

1101000103

Log ID	1101000103
Meaning	The number of vulnerabilities that netscan detected.
Severity Level	Notification
Formats	device_id=< <i>fortianalyzer_serial_number</i> > vd=< <i>virtual_domain_name</i> > action=< <i>action</i> > ip=< <i>ip_address</i> > vuln_count=< <i>total_vulns</i> >

FORTINET®

