FortiADC Log Reference

VERSION 5.1.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, October 4, 2018

FortiADC Log Reference

Initial Release

TABLE OF CONTENTS

Change Log

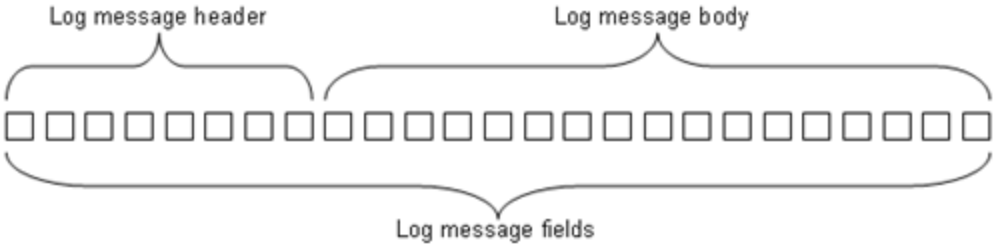
Date	Change Description
2018-08-04	Initial publication.

Introduction

This document discusses the various types of logs that FortiADC appliance generates, describing the log formats and the data contained in the logs. The goal is to help system administrators better understand the log messages so that they can have a better idea about their network traffic and system performance.

Anatomy of a log message

The diagram below illustrates the formation of a FortiADC log message. This section discusses the composition of a log message.



Log message header vs. log message body

As illustrated above, a log message consists of a number of message fields, which can be separated into two part: log message header and log message body.

- Log message header—The log message header shows a log's date, time, log ID, administrative domain, type, sub-type, and priority. *These fields exist in all log types.*
- Log message body—The log message body describes the reason that the log was generated and the action that the FortiADC appliance took in response. *These fields vary by log type.*

Example log messages

The log messages below are provided to help you understand the composition of FortiADC log messages. Note that these are raw log messages that you see from the FortiADC Console or when log file you opened in a text editor. Some of the fields may look slightly different from the formatted log messages that you see on the GUI.

Note: The log message body in the following example log messages is intentionally marked in **BOLD** to help distinguish it from the log message header.

Event log

```
date=2018-01-23 time=16:18:15 log_id=0000000100 type=event subtype=config
pri=information vd=root msg_id=39242021 user=admin ui=GUI(172.30.16.64)
action=add cfgpath=global-load-balance data-center cfgobj=name cfgattr=dc1
```

logdesc=Change the configuration msg=added a new entry 'dc1' for "global-load-balance data-center" on domain "root"

Traffic log

date=2018-01-20 time=15:27:40 log_id=0101008001 type=traffic subtype=slb_http pri=information vd=root **msg_id=39233799 duration=0 ibytes=150 obytes=258 proto=6 service=http src=192.168.1.10 src_port=50758 dst=192.168.1.141 dst_port=80 trans_src=2.2.2.1 trans_src_port=23992 trans_dst=2.2.2.10 trans_dst_port=80 policy=test11111111111111111111111111111111 action=none http_method=get http_host=192.168.1.141 http_agent=Wget/1.16.3 (linux-gnu) http_url=/index.html http_qry=none http_referer=none http_cookie=none http_retcode=200 user=none usrgrp=none auth_status=none srccountry=Reserved dstcountry=Reserved real_server=s1**

Security log

date=2018-01-11 time=09:13:21 log_id=0201006003 type=attack subtype=synflood pri=alert vd=root **msg_id=38284198 count=18287 severity=high proto=6 service=tcp src=0.0.0.0 src_port=0 dst=192.168.1.141 dst_port=0 policy=l7vs action=deny srccountry=Reserved dstcountry=Reserved**

Script log

date=2018-02-08 time=19:31:45 log_id=0300010000 type=script subtype=slb pri=information vd=priceminister **msg_id=3291 obj_name=Virtual Server obj_value=VIP_narcisse_443 msg="agent iphone matches UA mobile "**

Log types and sub-types

FortiADC log messages fall into four major types or categories, each of which has a number of sub-types or sub-categories.

Major log types

The table below lists the four major log types and their functions.

Table 1: Major log types and their functions

Log type	Description
Event Log	Records system or administrative events, such as downloading a backup copy of the configuration or daemon activities
Traffic Log	Records network traffic information, such as HTTP or HTTPS requests and responses, etc.
Security Log	Records attack or intrusion attempts.
Script Log	Records the use of server load-balance scripts.

Log Sub-types

The table below lists the sub-types of each major log type.

Table 2: Major log types and their sub-types

Log type	Sub-type
Event Log	• Configuration • System • Admin • User • Health Check • SLB • LLB • GLB • Firewall
Traffic Log	• SLB Layer 4 • SLB HTTP • SLB TCPS • SLB RADIUS • GLB • SLB SIP • SLB RDP • SLB DNS • SLB RTSP • SLB SMTP • SLB RTMP • SLB DIAMETER • SLB MySQL • LLB
Security Log	• IP Reputation • Synflood • WAF • GEO • AV
Script Log	• SLB

Note: You can see all the log types and their sub-types from the GUI by clicking Log & Report >Log Browsing.

Log ID schema

The FortiADC log ID `(log_id)` is a 10-digit number. The first two digits stand for the major log type, the second two digits stand for the sub-type of a major log type, and the remaining six digits are specific to log content.

Log Type ID

The table below lists FortiADC's major log types and sub-types, along with their corresponding IDs numbers.

Type	Type ID	Sub-type	Sub-type ID
Event	**00**		
		Configuration	00
		Admin	01
		Health Check	02
		System	03
		User	04
		SLB	05
		LLB	06
		GLB	07
		Firewall	08
Traffic	**01**		
		SLB Layer 4	00
		SLB HTTP	01
		SLB TCPS	02
		SLB RADIUS	03
		GLB	04
		SLB SIP	06

Type	Type ID	Sub-type	Sub-type ID
		SLB RDP	07
		SLB DNS	08
		SLB RTSP	09
		SLB SMTP	10
		SLB RTMP	11
		SLB MySQL	12
		SLB DIAMETER	13
		LLB	14
Security	**02**		
		IP Reputation	00
		Synflood	01
		WAF	02
		GEO	03
		AV	04
Script	**03**		
		SLB	00

Event logs

This chapter covers various types of event logs, which fall into the following subcategories:

- Configuration change
- Admin
- Health check
- system
- User authentication
- Server load balancing
- Link load balancing
- Global load balancing
- Firewall

Configuration

This section describes log messages involving FortiADC configuration change.

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
user	string(64)
ui	string(64)
action	string(64)
cfgpath	string(255)

Field	Type
cfgobj	string(255)
cfgattr	string(255)
logdesc	string(255)
msg	string(1024)

0000000100 (configuration change)

This log ID represents a subtype of the event log. It could mean any changes made to the configuration of your FortiADC unit. The actions (changes) could be edit, delete, add, or backup.

All 000000100 (configuration change) log messages include the following fields:

- `cofgobj` —configuration object
- `cfgpath` —configuration path
- `cfgattr`—configuration attribute

For instance, if the administrator has changed the IP address for Port 1 from 192.168.1.99/24 to 172.30.154,141, the event will be logged as below:

```
date=2018-01-23 time=16:18:15 log_id=0000000100 type=event subtype=config
pri=information vd=root msg_id=39242021 user=admin ui=GUI(172.30.16.64)
action=add cfgpath=global-load-balance data-center cfgobj=name cfgattr=dc1
logdesc=Change the configuration msg=added a new entry 'dc1' for "global-load-
balance data-center" on domain "root"
```

Admin

This section describes log messages involving FortiADC system administration, which are a subcategory of the event log.

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)

Field	Type
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
user	string(64)
ui	string(64)
action	string(64)
status	string(64)
reason	string(64)
logdesc	string(255)
msg	string(1024)

0001001000 (admin login)

These log messages relate to administration login events to your FortiADC unit. The same log ID could cover any of the following events:

Admin login failed

Message: `User [name] login failed from [GUI|ssh|console]`

Meaning: Login attempt by (user name) from the GUI/SSH/Console failed.

Priority: Notification

Admin login failed for 3 times

Message: `User [name] from [GUI|ssh|console]has been tried more than 3 times.`

Meaning: Login attempts by (user name) from the GUI/SSH/Console failed for three times

Priority: Notification

Admin login failed for blockip

Message: `User [name] login failed from blocked ip [ip address]`

Meaning: Login attempt by (user name) from (IP address) was denied because this IP address was blocked.

Priority: Notification

Admin login success

Message: `User [name] login successfully from [GUI|ssh|console]`

Meaning: (User name) successfully logged into the unit from the GUI/SSH/Console.

Priority: Information

0001001001 (admin logout)

These log messages relate to administration logout events from your FortiADC unit. The same log ID could cover either of the following events:

Admin logout

Message: `User [name] logout from [GUI|ssh|console]`

Meaning: (User name) logged out from the GUI/SSH/Console.

Priority: Information.

Admin timeout

Message: `User [name] time out from [GUI|ssh|console]`

Meaning: (User name) was logged out from the GUI/SSH/Console because the session had been idle for too long.

Priority: Information.

Health check

This section describes log messages regarding health checks. They are a subcategory of the event log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)

Field	Type
msg_id	uint64(20)
module	string(64)
policy	string(64)
member	string(64)
attrtype	string(64)
attrname	string(64)
action	string(64)
status	string(64)
logdesc	string(255)
msg	string(1024)

0002001800 (health check llb)

These log messages relate to health check for link load balancing (LLB) configuration on your FortiADC unit. The same log ID could cover either of the following events:

LLB gateway change status

Message: `Gateway [name] is [up|down]`

Meaning: (Gateway name) is up/down.

Priority: Alert.

LLB virtual tunnel change status

Message: `virtual tunnel [name] member [name] is [up|down]`

Meaning: (virtual tunnel name) (member name) is up/down.

Priority: Alert.

0002001801 (health check slb)

These log messages relate to health check for server load balancing (SLB) configuration on your FortiADC unit. The same log ID could cover either of the following events:

SLB VS change status

Message: `Virtual server [name], status is [up|down]`

Meaning: (virtual server name) is up/down.

Priority: Alert

SLB RS change status

Message: `Pool name [name] realserver name [name], ip [ip address] and port [port number] was detected as [up|down] by Health Check [name]`

Meaning: The health check found (server pool name) (real server name) with (IP address) and (port number) was up/down.

Priority: Alert.

0002001802 (health check glb)

This log ID relates to a health check result involving a remote server's virtual server and gateway.

Message: `GLB remote server change state`

Meaning: The remote server's virtual server or gateway health check state changed.

Priority: Alert

System

This section describes log messages involving various system events, which fall into the system sub-category of the event log.

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
user	string(64)
ui	string(64)

Field	Type
action	string(64)
status	string(64)
logdesc	string(255)
msg	string(1024)

0003000200 (certificate expired)

This log ID relate to the following event logs regarding the state of the local certificate on your FortiADC unit.

Local certificate to be expired

Message: `Local certificate [name] is going to expire in 1 week.`

Meaning: The local certificate will expire in one week.

Priority: Warning.

Local certificate expired

Message: `Local certificate [name] is expired !!`

Meaning: (Local certificate name) is expired!

Priority: Critical.

0003000201 (crl update)

This log ID relates to a system event involving the update of the CRL (certificate revocation List).

CRL update succeeded

Message: `Get/Update succeeded (CRL=[name] DP=[name])`

Meaning: (CRL name) from (DP) was successfully updated.

Priority: Information.

CRL update failed

Message: `Failed to save updated CRL[name] from DP [name]`

Meaning: The system failed to save the updated (CRL name) from (DP).

Priority: Information.

0003000202 (system reboot)

This event log ID indicates that your FortiADC unit was rebooted.

Message: `System has been restarted`

Meaning: An administrator restarted the unit using the CLI or web-based manager.

Priority: Warning

0003000203 (system shutdown)

This event log ID indicates that your FortiADC unit was shut down.

Message: `System has been shutdown`

Meaning: An administrator has shut down the unit.

Priority: Warning

0003000204 (clean isp address)

This log ID relates to a system event involving the clean-up of the restored ISP address book.

Message: `Clean restored ISP address-books`

Meaning: The restored ISP address book was cleaned.

Priority: Warning

0003000205 (configuration backup)

This log ID relates to the backup of system configuration on your FortiADC unit.

Message: `Backup configuration [config name] to FortiADC disk [failed|successful]`

Meaning: The system configuration (file name) was successfully backed up or failed to be backed up onto the FortiADC disk.

Priority: Warning (when failed) or Notice (when succeeded)

Message: `Backup files reach [file number] and overwrite is disable`

Meaning: The number of configuration backup files has reached the set limit and the system is not allowed to overwrite previous configuration backups.

Priority: Warning

Message: `Total configuration file reach maximum size and overwrite is disable`

Meaning: The size of all configuration backup files combined has reached the set limit, and the system is not allowed to overwrite previous configuration backups.

Priority: Warning

Message: `Backup the configuration to tftp server [server ip] as [file name] [failed| successful]`

Meaning: The system configuration was successfully backed up or failed to be backed up onto the TFTP server (server IP).

Priority: Warning (when failed) or Notice (when succeeded)

Message: `Backup the configuration to sftp server [server ip] as [file name] [failed| successful]`

Meaning: Backing up the system configuration (file name) onto the TFTP server (server IP) failed or succeeded.

Priority: Warning (when failed) or Notice (when succeeded)

Message: `SFTP server [server ip] is unreachable`

Meaning: The SFTP server (server IP) could not be reached during configuration backup.

Priority: Warning

Message: `Login failed to sftp server [server ip]`

Meaning: Attempt to log into the SFTP server (server IP) failed when doing configuration backup.

Priority: Warning

Action: Make sure your username and password as valid.

Message: `Unable to write file in path [directory name] of sftp server [server ip]`

Meaning: The system was unable to write files to the path (directory name) on the SFTP server.

Priority: Warning

Action: Double-check the permission settings.

0003000206 (isp address book backup)

This log ID relates to a system event involving the backup of the ISP address books.

Message: `Backup ISP address-books to tftp server [server_name] as [file_name]`

Meaning: The ISP address book (file name) was backed up onto the TFTP server (server name).

Priority: Warning

0003000207 (log backup)

This log ID relates to a system event involving the backup of log files.

Message: `backup log to ftp server [server ip]`

Meaning: The logs were backed up on FTP server (server IP).

Priority: Warning.

0003000208 (generate local certificate by scep)

This event log ID relates to a system event involving the generation of a local certificate by SCEP.

Message: `Local certification generated by SCEP`

Meaning: A local certificate was generated by SCEP.

Priority: Information.

0003000209 (import ca certificate)

This event log ID relates to a system event involving the import of a CA certificate.

Message: `CA certification is retrieved from SCEP server"`

Meaning: A CA certificate was retrieved from the SCEP server.

Priority: Information.

0003000210 (import crl)

This event log ID relates to a system event involving the import of a CRL (Certificate Revocation List).

Message: `CRL is retrieved from SCEP server`

Meaning: A CRL was retrieved from the SCEP server.

Priority: Information.

0003000211 (import ocsp response)

This log ID relates to a system event involving the import of an OCSP (Online Certificate Status Protocol) response.

Message: `import OCSP response through ftp log`

Meaning: A new OCSP response was updated to system through FTP server.

Priority: Information

0003000212 (set system time)

This log ID relates to a system event involving the setting of system time.

Message: `set system time to [date][time].`

Meaning: The system time was set to (date) (time).

Priority: Warning.

0003000213 (system reset)

This log ID relates to a system event involving resetting FortiADC to its factory (default) settings.

Message: `system has been reset to factory default.`

Meaning: An administrator has reset the system to its factory default from the GUI, Console, or LCD.

Priority: Warning.

0003000214 (log rebuilt)

This log ID relates to a system event involving the rebuild of logs on the system.

Message: `log rebuild on [root vdom|domain [name]] db`

Meaning: The log was rebuilt on [root VDOM | (domain name)] database.

Priority: Warning.

0003000215 (log deleted)

This log ID relates to system events involving the delete of logs.

Message: `delete type [elog|tlog|alog|all type] log`

Or Delete log [log file name]

Meaning: The log type (event/traffic/security/all) were deleted.

Priority: Warning.

Or

Message: `delete log [log file name]`

Meaning: The (log file name) deleted.

Priority: Warning.

0003000216 (system reloaded)

This log ID relates to a system event involving reloading the system with applications.

Message: `system (version) has been reloaded`

Meaning: The administrator reloaded the system (version) using the GUI/Console.

Priority: Warning

0003000217 (firmware upgraded)

This log ID relates to a system event involving the system's firmware upgrade.

Message: `system firmware has been upraded from version1 to version2`

Meaning: An administrator has upgraded the system firmware from version 1 to version 2 using the GUI/Console.

Priority: Warning.

0003000218 (firmware downgraded)

This log ID relates to a system event involving the system's firmware downgrade.

Message: `System firmware has been downgraded from version2 to version1`

Meaning: An administrator has downgraded the system's firmware from version 2 to version 1 using the GUI/Console.

Priority: Warning

0003000219 (firmware error)

This log ID relates to a system event involving a firmware error on the system.

Message: `Check image error`

Meaning: The uploaded image was not a FortiADC firmware image.

Priority: Warning

0003000220 (crypto license upgraded)

This log ID relates to a system event involving the update of the system's cryptographic license.

Message: `crypto license has been updated`

Meaning: The system's crypto license has been updated.

Priority: Warning.

0003000221 (isp address-books updated)

This log ID relates to a system event regarding update of the ISP address book.

Message: `update restored ISP address-books`

Meaning: The restored ISP address-books were updated.

Priority: Warning

0003000222 (database reset)

This log ID relates to a system event involving the reset of the statistics database.

Message: `statistics db will be reset`

Meaning: The statistics database will be reset.

Priority: Warning.

0003000223 (database restore)

This log ID relates to a system event involving the restore of the statistics database.

Message: `statistics db will be restored`

Meaning: The statistics database will be restored.

Priority: Warning.

0003000224 (alert delete)

This log ID relates to a system event involving the removal of alert messages.

Message: `delete an alert alert_for_cpu_too_high with id 3,alertname,alertid`

Meaning: The alert "`alert_for_cpu_too_high with ID 3`" is deleted from the system.

Priority: Warning

0003000225 (ca retrieved)

This log ID relates to a system event involving the retrieval of a CA.

Message: `CA was successfully retrieved from SCEP server`

Meaning: (CA) was successfully retrieved from the SCEP server.

Priority: Information.

0003000226 (intermediate ca retrieved)

This log ID relates to a system event involving the retrieval of an intermediate CA.

Message: `intermediate CA was successfully retrieved from SCEP server`

Meaning: (Intermediate CA) was successfully retrieved from the SCEP server.

Priority: Information.

0003000227 (csr vdom)

This log ID relates to a system event to generate a CSR used to create a local certificate.

Message: `generate csr log`

Meaning: A Certificate Signing Request (CSR) certificate was generated to the system.

Priority: Information

0003000228 (generate local certificate)

This log ID relates to a system event involving the generation of a local certificate.

Message: `generate local certificate log`

Meaning: local certificate was generated.

Priority: Information

See Log 0003000208.

0003000229 (import certificate)

This log ID relates to a system event involving the import of a certificate.

Message: `import local certificate log`

Meaning: A certificate was uploaded to the system as a local certificate.

Priority: Information

0003000230 (remote certificate retrieved)

This log ID relates to a system event involving the retrieval of a remote certificate.

Message: `import remote certificate log.`

Meaning: A certificate was uploaded as an OCSP-signing certificate.

Priority: Information

0003000231 (log download)

This log ID relates to a system event involving log download.

Message: `Download log successfully.`

Meaning: An attempt to download the log was successful.

Priority: Warning

Or

Message: `Download log failed.`

Meaning: Attempt to download the log failed.

Priority: Warning

0003000232 (delete report)

This log ID relates to a system event involving deleting a report file.

Message: `report [filename] is deleted`

Meaning: The report (filename) was deleted.

Priority: Warning

0003000233 (delete log table)

This log ID relates to a system event involving deleting a log table.

Message: `Upgrade the log db since the log format is changed.`

Meaning: Due to log format change, the log index table was updated (rebuilt).

Priority: Warning

0003000234 (port status changed)

This log ID relates to a system event involving the change of port status.

Message: `[port name] status changed from [up|down] to [up|down]`

Meaning: The status of (Port number) changed from (up/down) to (down/up).

Priority: Notification

0003000235 (vm license update)

This log ID relates to a system event involving the update of VM licenses.

Message: `vm license has been updated`

Meaning: The administrator has updated the VM license.

Priority: Warning

0003000236 (log db failed to start)

This log ID relates to a system event involving a failed attempt to launch the log database.

Message: `The DB server can not start correctly ...`

Meaning: The database server could not be started correctly.

Priority: Warning

0003000237 (get log version failed)

This log ID relates to a system event involving a failed attempt to get the log version.

Message: `Can not get the log file 1.admin.elog version and create new log file`

Meaning: The system could not get the version of the log file "1.admin.elog" in the file's header to create a new log file.

Priority: Critical

0003000238 (create log file)

This log ID relates to a system event involving the creation of a log file.

Message: `Create new log file 2.admin.elog for upgrade the log.`

Meaning: A new log file `"2.admin.elog"` was created when upgrading the log.

Priority: Warning

Message: `Create new log file 2.admin.elog for checking msgid wrongly.`

Meaning: A new log file `"2.admin.elog"` was created when checking the message ID of the log.

Priority: Warning

0003000239 (generate self-signed certificate)

This log ID relates to a system event involving the generation of a self-signed certificate.

Message: `generate the self signed certificate log.`

Meaning: A self-signed certificate was generated.

Priority: Information

0003000240 (temperature high)

This log ID relates a system event involving the temperature of the system's CPU.

Message: `Temperature of [CPU] is high: [number] C`

Meaning: The temperature of the CPU is high.

Priority: Critical

0003000241 (temperature critical)

This log ID relates to a system event involving extremely high CPU temperature.

Message: `[CPU ID | Device Sensor ID | PSU R/L] temperature [number] C hits threshold.`

Meaning: The temperature (digit in centigrade) of the (CPU ID | Device Sensor ID | PSU R/L) is over the threshold.

Priority: Critical

0003000242 (temperature normal)

This log ID relates to a system event involving normal CPU temperature.

Message: `Temperature of [CPU ID | Device Sensor ID | PSU R/L] back to normal`

Meaning: The temperature of the (CPU ID | Device Sensor ID | PSU R/L) is back to normal (cooling down).

Priority: Critical

0003000243 (fan bad)

This log ID relates to a system event involving the poor condition of the system cooling fan.

Message: [name] Device FAN id [number] is bad

Meaning: The system cooling fan is not working properly.

Priority: Error

0003000244 (fan slow)

This log ID relates to a system event involving the slow rotation of the system cooling fan.

Message: `[name] Device FAN id [number] is slow`

Meaning: The system (name) cooling fan (ID number) is slow.

Priority: Error

0003000245 (input voltage high)

This log ID relates to a system event involving high input voltage.

Message: `[device name] Input Voltage [device ID] is high:[number]`

Meaning: (Device name)'s input voltage is high: (numeric value).

Priority: Critical

0003000246 (input voltage low)

This log ID relates to a system event involving low input voltage.

Message: `[device name] Input Voltage [device ID] is low:[number]`

Meaning: (Device name)'s input voltage (device ID) is high: (numeric value)

Priority: Critical

0003000247 (hdd unhealthy)

This log ID relates to a system event involving the health state of the system hard disk drive.

Message: `Hard disk is NOT healthy`

Meaning: The hard disk drive is not healthy

Priority: Critical

0003000248 (ssd reached end of life)

This log ID relates to a system event involving the SSD reaching the end of its life.

Message: `SSD life reached threshold`

Meaning: The SSD has reached the end of its life.

Priority: Critical

0003000249 (ssd near end of life)

This log ID relates to a system event involving the SSD approaching the end of its life.

Message: `SSD life near threshold, has [number] left]`

Meaning: The SSD is approaching the end of its life.

Priority: Critical

0003000250 (device usage)

This log ID relates to a system event regarding FortiADC's disk usage.

Message: `device usage hit [number]percent`

Meaning: The FortiADC appliance's disk usage reached (percentage) of its capacity.

Priority: Warning

0003000251 (hdd mount status)

This log ID relates to a system event regarding the mount status of the hard disk drive.

Message: `device is not mounted`

Meaning: The HDD is not mounted.

Priority: Warning

0003000252 (log index table broken)

This log ID relates to a system event involving a broken log index table.

Message: `The log index table [name] is broken and rebuild it.`

Meaning: The log index table (name) was broken and was rebuilt.

Priority: Warning

0003000253 (log index non-existent)

This log ID relates to a system event involving a log index that did not exist.

Message: `The unexist log table elog.000000001 is deleted it.`

Meaning: The non-existent log index table is deleted

Priority: Warning

0003000254 (log db disk full)

This log ID relates to a system event involving available space on log database disk.

Message: `The log db disk is FULL! Delete some tables.`

Meaning: The log database disk was full. Some tables were deleted.

Priority: Warning

0003000255 (statistics disk full)

This log ID relates to a system event involving the available space in the statistics disk.

Message: `The statistics disk is FULL! Delete some tables`

Meaning: The statistics disk was full. Some tables were deleted.

Priority: warning

0003000257 (mount hdd failed)

This log ID relates to a system event involving a failed attempt to mount the HDD.

Message: `Failed to mount log partition`

Meaning: An attempt to mount the HDD failed.

Priority: Error

0003000258 (update fortiguard successful)

This log ID relates to a system event involving the result of update of FortiGuard.

Message: `Update result: OK`

Meaning: FortiGuard was successfully updated.

Priority: Information

0003000259 (report disk full)

This log ID relates to a system event involving the available space of the disk used to store reports.

Message: `The report disk is full!`

Meaning: The disk used to store reports was full.

Priority: Warning

0003000260 (report expired)

This log ID relates to a system event involving an expired report.

Message: `The report On-Schedule-SLB-2018-01-05-090000 timeout`

Meaning: The report `On-Schedule-SLB-2018-01-05-090000` took too long to execute. No report was generated because it timed out.

Priority: Warning

0003000261 (ha switch console received)

This log ID relates to a system event involving the HA switch console.

Message: `Received switch console from SN.`

Meaning: An HA switch console was received from an appliance (serial number).

Priority: Information

0003000262 (ha switch console)

This log ID relates to a system event involving the HA console.

Message: `Switch console to SN.`

Meaning: Some log oAn HA switch console was received

Priority: Information

0003000263 (ha slave sync)

This log ID relates to a system event involving the synchronization of the slave with the master in an HA configuration.

Messages:

`(1) The Configuration is different from CfgMaster, System will be reloaded.`

`(2) The Slave device synchronized failed.`

`(3) File (filename md5) received successfully.`

`(4) File (filename) received failed.`

`(5) File (filename md5) sending finished.`

`(6) File (filename) sending failed.`

`(7) Operated File filename Exception.`

`(8) System Exception:cmd commandline failed!`

`(9) The Slave device has fully synchronized and will be reloaded.`

Meaning:

- configuration sync
- file sync
- Exception of sync

Priority: Informaiton

0003000264 (ha forced sync)

This log ID relates to a system event involving forced sync of HA configuration.

Message: The Slave device has fully synchronized and will be reloaded.

Meaning: HA forced sync

Priority: Information

0003000265 (ha system upgrade)

This log ID relates to a system event involving the system upgrade of an HA configuration.

Message: `System is upgrading`

Meaning: The system is being upgraded.

Priority: Information

0003000266 (ha received image)

This log ID relates to a system event involving the system image delivered to an HA configuration.

Message: `Received image from [dev sn]`

Meaning: The system image was received from (server name).

Priority: Information

0003000267 (ha remote IP status changed)

This log ID relates to a system event involving the HA remote IP status change.

Message: `Remote ip %s is [up|down]`

Meaning: Remote IP (address) is up/down.

Priority: Information

0003000268 (ha remote ip inactive too long)

This log ID relates to a system event involving the HA remote IP that has been inactive beyond the configured threshold.

Message: `Gateway inactive count exceed threshold`

Meaning: The HA gateway has been idle beyond the configured threshold.

Priority: Information

0003000269 (ha disk check)

This log ID relates to a system event involving an HA disk check.

Message: `Disk check failure`

Meaning: An attempt to check the HA disk failed.

Priority: Information

0003000270 (ha push image)

This log ID relates to a system event involving installing the system image onto an HA node.

Message: `Pushing image to node [name]`

Meaning: The HA image was pushed to node (name).

Priority: Information

0003000271 (ha full config sync)

This log ID relates to a system event involving full HA configuration sync.

Message: `Full configuration sync failed`

Meaning: Attempt to run a full HA sync failed.

Priority: Information

0003000272 (ha init)

This log ID relates to a system event involving the initiation of an HA node.

Message: `HA device init`

Meaning: The HA device was initiated.

Priority: Information

0003000273 (ha change mode)

This log ID relates to a system event involving an HA device's mode change.

Message: `HA device moved into [Master|slave] mode`

Meaning: The HA device changed to (master/slave) mode

Priority: Information

0003000274 (ha device joined group)

This log ID relates to a system event involving a device that joined an HA group.

Message: `Member (name) join to the HA group`

Meaning: HA member device (name) joined the HA group.

Priority: Information

0003000275 (ha device left group)

This log ID relates to a system event involving a HA device that was removed from the HA configuration.

Message: `Member ([name]) leave from the HA group`

Meaning: The HA member (device name) left the HA group.

Priority: Information

0003000276 (ha interface state changed)

This log ID relates to a system event involving an HA interface's change of operating state.

Message: `[name] change state to [up|down]`

Meaning: The HA interface (name) has changed to up/down.

Priority: Information

0003000277 (ha traffic group work node changes)

This log ID relates to a system event involving the change in an HA traffic group's work node.

Message: `groupname work node change to nodeid`

Meaning: The ha traffic group work node has changed to (node ID).

Priority: Information

0003000278 (ha executed forced sync)

This log ID relates to a system event involving the execution of a forced HA sync.

Message:

`(1) sync-config`

`(2) standby`

Meaning: An HA forced sync was executed.

Priority: Information

0003000279 (arp conflict)

This log ID relates to a system event involving network traffic ARP conflict.

Message: `Detect MAC address xx:xx:xx:xx:xx:xx claims to have our IP x.x.x.x`

Meaning: An ARP conflict was detected.

Priority: Error

0003000280 (link status changed)

This log ID relates to a system event involving a network interface link status change.

Message: `Link status changed`

Meaning: A network interface link status has changed.

Priority: Notify

0003000281 (port exhausted)

This log ID relates to a system event involving unavailability of source ports.

Message: `Cannot find available source port from port range [port] to [port]`

Meaning: No source port was available from Port (number) to Port (number).

Priority: Notify

0003000282 (log disk full)

This log ID relates to a system event involving unavailability of log disk space.

Message: `The log disk is FULL`

Meaning: The system ran out of log disk space.

Priority: Notify

0003000283 (log rotate)

This log ID relates to a system event involving a log file rotation.

Message: `The log 2.admin.elog is rotated.`

Meaning: The log file `"2.admin.elog"` is too big. Close it and open the file `"3.admin.elog"` instead to record log.

Priority: Warning

0003000284 (share memory disk full)

This log ID relates to a system event involving lack of shared memory.

Message: `Share memory disk is full.`

Meaning: The system has run out shared memory.

Priority: Warning

0003000285 (ha vrrp group changed)

This log ID relates to a system event involving an HA VRRP group change.

Message: `node id [up|down] [join | leave | update] trafficgroupname`

Meaning: The node (whose status is up/down) has joined/ left the HA VRRP group.

Priority: Information

0003000286 (geoip database updated)

This log ID relates to a system event regarding update of the geography ip database.

Message: `update geography ip database`

Meaning: The geography ip database is updated

Priority: Information

0003000287 (ip reputation database updated)

This log ID relates to a system event regarding update of the ip reputation database.

Message: `update ip reputation database`

Meaning: The IP reputation database is updated.

Priority: Information

0003000288 (system voltage recovered)

This log ID relates to a system event involving voltage recover from error.

Message: `[device name] Input Voltage [device id] back to normal [number]`

Meaning: The (device name) input voltage has recovered from an error.

Priority: Information

0003000289 (system fan recovered)

This log ID relates to a system event involving system fan recover from error.

Message: `[device name] Velocity of FAN back to normal`

Meaning: The (device name) system fan has recovered from an error.

Priority: Information

User Authentication

This section describes log messages involving user authentication events on the system. They are a subcategory of the event log.

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
user	string(64)
usergrp	string(64)
policy	string(64)
action	string(64)
status	string(64)
reason	string(64)
logdesc	string(255)
msg	string(1024)

0004001500 (user authentication)

This log ID relates to a system event involving user authentication queries.

Message: `valid authentication query`

Meaning: A valid user authentication query was received.

Priority: Information

Or

Message: `invalid authentication query`

Meaning: An invalid user authentication query was received.

Priority: Information

0004001501 (user authentication relay)

This log ID relates to authentication result when the virtual server binds to an authentication policy which uses authentication relay.

Message: `[Valid | Invalid] [authentication-relay | kerberos authentication-relay] query`

Meaning: An HTTP basic or Kerberos constrained delegation authentication succeeded or failed.

Priority: Information/Notification

Server Load Balance (SLB)

This section provides descriptions of the SLB log messages which fall into a sub-category of the event log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)

Field	Type
pri	string(16)
vd	string(64)
msg_id	uint64(20)
policy	string(64)
group	string(64)
member	string(64)
attrtype	string(64)
attrname	string(64)
action	string(64)
status	string(64)
logdesc	string(255)
msg	string(1024)

0005002000 (script load file error)

This log ID relates to a system event involving error happened when loading a script file.

Message: `script file load error log`

Meaning: An error occurred when the system was loading a script file.

Priority: Error

0005002001 (script run time error)

This log ID relates to a system event involving an error that happened when running a script file.

Message: `script run-time error log`

Meaning: The system encountered an error happen when running a script file.

Priority: Error

0005002002 (slb transaction rate limit)

This log ID relates to a system event involving SLB transaction rate limit.

Message: `VS [name] has [reached|dropped below] its transaction rate limit [number]`

Meaning: Virtual server (name) has reached/dropped below its transaction rate limit (value).

Priority: Alert

Or

Message: `rs [name] has [reached|dropped below] its transaction rate limit [number]`

Meaning: Real server (name) has reached/dropped below its transaction rate limit (value).

Priority: Alert

0005002003 (slb connection rate limit)

This log ID relates to a system event involving SLB real server or virtual server connection rate limit.

Message: `VS [name] has [reached|dropped below] its connection rate limit [number]`

Meaning: Virtual server (name) has reached/dropped below its connection rate limit (value).

Priority: Alert

Or

Message: `rS [name] has [reached|dropped below] its connection rate limit [number]`

Meaning: Real server (name) has reached/dropped below its connection rate limit (value).

Priority: Alert

0005002004 (client certificate verify)

This log ID relates to a system event involving SLB client certificate verify.

Message: `client [ipaddr] with certificate CN[name] [was validated successfully|failed to be validated] by CA with CN[name] [and OCSP server [name]] [ and CRL [name]]`

Meaning: Client (IP address) with certificate CN (name) was validated successfully/failed to be validated by the CA with CN (name) and OCSP server (name) and CRL (name).

Priority: Alert

0005002005 (slb ssl handshake)

This log ID relates to a system event involving SLB SSL handshake to the real server or virtual server.

Message: `VS [name] failed to establish SSL connection with real server [name]`

Meaning: Virtual Server (name) failed to establish an SSL connection with Real Server (name).

Priority: Alert

Or

Message: `VS [name] failed to establish SSL connection with real server [name]`

Meaning: Virtual Server (name) failed to establish an SSL connection with Real Server (name).

Priority: Alert

0005002007 (vdom rps limit)

This log ID relates to a system event involving VDOM RPS limit.

Message: `In VDOM vdom1, Drop 4 packets due to L7RPS`

Meaning: Four packets were dropped from VDOM `"vdom1"` due to its L7RPS resource limit.

Priority: Warning

0005002008 (vdom cps limit)

This log ID relates to a system event involving VDOM CPC limit.

Message: `In VDOM vdom1, Drop 4 packets due to L4CPS/L7CPS/SSLCPS`

Meaning: Four packets were dropped from "vdom1" due to its L4CPS/L7CPS/SSLCPS resource limit.

Priority: warning

0005002009 (vdom tp limit)

This log ID relates to a system event involving VDOM TP limit.

Message: `In VDOM vdom1, Drop 4 packets due to SSLTP`

Meaning: Four packets were dropped from VDOM "vdom1" due to SSLTP resource limit.

Priority: Warning

0005002010 (slb connection limit)

This log ID relates to a system event involving SLB connection limit.

Message: `Virtual server vsname is [recovered from | reached ]connection limit`

Meaning: Virtual server (name) recovered from or reached its SLB connection limit.

Priority: Warning

0005002011 (slb source port exhausted)

This log ID relates to a system event regarding the availability of SLB source port.

Message: `Virtual server vsname is [recovered from | out of] source ports`

Meaning: Virtual server (name) recovered or ran out of source ports.

Priority: Warning

0005002012 (slb ip pool exhausted)

This log ID relates to slb ip pool exhausted

Message:

```
(1) Virtual server rsname is no source pool configured on the
interface to real server rsname
```

```
(2) Virtual server vsname to real server vsname is recovered from bad
source pool list configuration
```

Meaning: Virtual server (name) had exhausted its SLB IP pool (no IP is available for SLB).

Priority: Warning

0005002013 (slb config error)

This log ID relates to a system event regarding use of invalid arguments for SLB configuration.

Message: `Invalid configuration arguments`

Meaning: Invalid configuration arguments were used for SLB configuration.

Priority: Alert

0005002014 (slb memory allocation error)

This log ID relates to a system event regarding memory allocation in SLB configuration.

Message: `Failed to allocate memory`

Meaning: No (enough) memory was allocated for SLB configuration.

Priority: Alert

0005002015 (slb mkdir error)

This log ID relates to a system event regarding mkdir in SLB configuration.

Message: `Failed to make directory`

Meaning: The system was unable to create the directory for SLB configuration.

Priority: Alert

0005002016 (slb open file error)

This log ID relates to a system event regarding set SLB configuration.

Message: `Failed to open file`

Meaning: The system failed to open the file.

Priority: Alert

0005002017 (slb write file error)

This log ID relates to a system event regarding set SLB configuration.

Message: `Failed to write file`

Meaning: The system failed to generate the configuration.

Priority: Alert

0005002018 (slb drop log)

This log ID relates to a L4 SLB kernel packet drop.

Message: `SLB packet is dropped in IPVS`

Meaning: There is a L4 SLB packet drop in IPVS.

Priority: Warning

0005002019 (vs restart)

This log ID relates to a system event involving the restart of a virtual machine.

Message: `Restart virtual server [VSNAME]`

Meaning: The virtual machine (name) was restarted because it did not work properly.

Priority: Information

Link load balance

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
policy	string(64)
group	string(64)
member	string(64)
attrtype	string(64)
attrname	string(64)
action	string(64)
status	string(64)
logdesc	string(255)
msg	string(1024)

0006003000 (llb bandwidth usage)

This log ID relates to a bandwidth usage in link load-balancing operations.

Message:

```
gateway [name][
"exceed inbound bandwidth",
"exceed outbound bandwidth",
"exceed inbound spillover bandwidth",
"exceed outbound spillover bandwidth",
"exceed total spillover bandwidth"]
```

Meaning: Gateway (name) exceeded its allocated inbound/outbound/inbound spillover/outbound spillover bandwidth.

Priority: Warning

Global load balance

This section describes log messages involving global load balancing operation, which is are a subcategory of the event log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
policy	string(64)
group	string(64)
member	string(64)
attrtype	string(64)
attrname	string(64)
action	string(64)
status	string(64)
logdesc	string(255)
msg	string(1024)

0007005000 (glb peer status change)

This log ID relates to peer status change in a GLB operation.

Message: `GLB Peer [name] is [Connected:Disconnected]`

Meaning: GLB peer (name) is connected/disconnected.

Priority: Alert

0007005001 (glb remote server status change)

This log ID relates to the remote server's status change in a GLB operation.

Message: `Server [name] is [Online|Off]`

Meaning: GLB server (name) is online/offline.

Priority: Alert.

Firewall

This section describes log messages about FortiADC firewall, which is a subcategory of the event log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
policy	string(64)
group	string(64)
member	string(64)
attrtype	string(64)
attrname	string(64)

Field	Type
action	string(64)
status	string(64)
logdesc	string(255)
msg	string(1024)

0008004000 (firewall snat source port exhausted)

This log ID relates to a firewall event.

Message: `SNAT rule [name] run out of source port and can't open new connection with others`

Meaning: SNAT Rule (name) ran out of source ports and could not open new connections with others.

Priority: Warning

Security logs

This section describes the various security log messages FortiADC generates.

IP Reputation

This section describes security log messages involving IP reputation—a subcategory of the security log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
count	unit32(10)
severity	string(64)
proto	string(16)
service	string(16)
src	string(128)
src_port	unit32(10)
dst	string(128)
dst_port	unit32(10)
policy	string(64)

Field	Type
action	string(64)
srccountry	string(255)
dstcountry	string(255)
msg	string(1024)

0200006001 (security: ip reputation)

This log ID relates to a security incident involving IP reputation rules.

Message: `IP Reputation Violation: [Botnet | Anonymous Proxy | Phishingnm | Spam | Others]`

Meaning: IP reputation rule violation: (The name of the specific violation)

Priority: Warning

Synflood

This section describes security log messages involving synflood attacks—a subcategory of the security log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
count	unit32(10)

Field	Type
severity	string(64)
proto	string(16)
service	string(16)
src	string(128)
src_port	unit32(10)
dst	string(128)
dst_port	unit32(10)
policy	string(64)
action	string(64)
srccountry	string(255)
dstcountry	string(255)

0201006003 (security: synflood)

This log ID relates to a security incident involving synflood attack.

Message: `Security rule name, category, subcategory, and description of the attack.`

Meaning:

Priority: Alert

GEO

This section describes security log messages involving GEO IP whitelists.

Log format:

Field	Type
date	string(10)
time	string(8)

Field	Type
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
count	unit32(10)
severity	string(64)
proto	string(16)
service	string(16)
src	string(128)
src_port	unit32(10)
dst	string(128)
dst_port	unit32(10)
policy	string(64)
action	string(64)
srccountry	string(255)
dstcountry	string(255)
msg	string(1024)

0203006002 (security: geo)

This log ID relates to security incident involving GEO rules.

Message: `Security rule name, category, subcategory, and description of the attack.`

Meaning: The GEO rule was violated.

Priority: Warning

Web Application Firewall (WAF)

This section describes security log messages related to Web Application Firewall—a subcategory of the security log.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
count	unit32(10)
severity	string(64)
proto	string(16)
service	string(16)
src	string(128)
src_port	unit32(10)
dst	string(128)
dst_port	unit32(10)
policy	string(64)
action	string(64)
sigid	uint32(10)
subcat	string(255)

Field	Type
http_method	string(32)
http_host	string(1024)
http_url	string(1024)
user_agent	string(1024)
pkt_hdr	string(1024)
srccountry	string(255)
dstcountry	string(255)
msg	string(1024)

0202006004 (security: waf signature)

This log ID relates to a security incident involving WAF signature attack.

Message: `Find Attack ID: 100*** NAME: "Web Application Joomla! SQL Injection Attempt -- category.php catid SELECT" CATEGORY: "SQL Injection" SUB_CATEGORY: "Coldfusion Injection"`

Meaning: A web generic attack was detected.

Priority: Alert

0202006005 (security: http protocol constraint)

This log ID relates to a security incident involving HTTP protocol constraint rule.

Message: `"Attack ID: 101*** NAME: "HTTP Method Violation" CATEGORY: "HTTP Protocol Constraint" SUB_CATEGORY: "Request Method Rule""`

Meaning: A violation is triggered due to a match of one or more of the HTTP protocol constraint options.

Priority: Alert

0202006006 (security: waf sql injection)

This log ID relates to a security incident involving the violation of the WAF SQL injection rule.

Message: `"Attack ID: 102*** NAME: "Cross Site Scripting Attack" CATEGORY: "Heuristic SQL/XSS Injection Detection" SUB_CATEGORY: "XSS Injection Detection""`

Meaning: A MySQL injection or cross-site injection was detected.

Priority: Alert

0202006007 (security: waf url protection)

This log ID relates to a security incident involving the violation of URL protection rules.

Message: `"Attack ID: 103*** NAME: "Request URL Pattern Violation" CATEGORY: "URL Protection" SUB_CATEGORY: "URL Access Rule""`

Meaning: A violation is triggered due to a match of one or more of the url protection rules.

Priority: Alert

0202006008 (security: waf bot)

This log ID relates to a security incident involving Bot detection.

Message: `Attack ID: 104*** NAME: "Bad Robot Attack" CATEGORY: "Bot Detection" SUB_CATEGORY: "Bad Robot"`

Meaning: A bad robot or content scraper is detected.

Priority: Alert

0202006009 (security: waf xml validation)

This log ID relates to a security incident involving XML validation.

Message: `"Attack ID: 105*** NAME: "XML schema is invalid" CATEGORY: "XML validation detection" SUB_CATEGORY: "XML schema check""`

Meaning: A violation is triggered due to a match of one or more of the XML options.

Priority: Alert

0202006010 (security: waf json validation)

This log ID relates to a security incident involving WAF JSON validation rules.

Message: `"Attack ID: 106*** NAME: "possible cross-site scripting attacks" CATEGORY: "JSON validation detection" SUB_CATEGORY: "JSON cross-site scripting check"`

Meaning: A violation is triggered due to a match of one or more of the JSON options.

Priority: Alert

0202006011 (security: waf soap validation)

This log ID relates to a security incident involving SOAP validation.

Message: `"Attack ID: 1050*** NAME: "SOAP content is invalid for WSDL" CATEGORY: "XML validation detection" SUB_CATEGORY: "SOAP WSDL validate""`

Meaning: A violation is triggered due to a match of one or more of the SOAP options.

Priority: Alert

Anti-virus (AV)

This section describes log messages related to the anti-virus module.

Log format:

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
count	unit32(10)
severity	string(64)
proto	string(16)
service	string(16)
src	string(128)
src_port	unit32(10)
dst	string(128)
dst_port	unit32(10)
policy	string(64)

Field	Type
action	string(64)
sigid	uint32(10)
av_anatype	string(255)
vr_id	uint32(10)
vr_category	string(255)
vr_botnet	string(255)
http_url	string(1024)
av_profile	string(64)
sandbox_checksum	string(64)
quar_file_crc_32	string(64)
quar_file_name	string(255)
ana_submiti	string(16)
vr_replaced	string(16)
proto_method	string(32)
srccountry	string(255)
dstcountry	string(255)
msg	string(1024)

0204006500 (security: av detected virus)

This log ID relates to a virus is detected by AV.

Message: `AV detected virus`

Meaning: The AV module detected a virus attack.

Priority: Alert

0204006501 (security: av heuristic)

This log ID relates to AV heuristic detected virus.

Message: `AV heuristic detected virus`

Meaning: The AV heuristic module detected a virus attack.

Priority: Alert

0204006502 (security: av upload request to fortisandbox)

This log ID relates to AV upload request to FortiSandbox to do analytics.

Message: AV upload FortiSandbox to do analytics

Meaning: The AV module uploaded the request to FortiSandbox for data analysis.

Priority: Alert

0204006503 (security: av scan length oversize)

This log ID relates to AV scan length oversize.

Message: `AV scan length oversize`

Meaning: The AV scan length oversize is exceeded.

Priority: Alert

0204006504 (security: av error)

This log ID relates to an AV engine error.

Message: `AV engine meet error, code x.`

Meaning: The AV engine has encountered an error, Code X.

Priority: Alert

Script logs

This section describes log messages involving FortiADC script. These log messages are designed by users to record a specific log while the script is running.

Field	Type
date	string(10)
time	string(8)
log_id	string(10)
type	string(8)
subtype	string(16)
pri	string(16)
vd	string(64)
msg_id	uint64(20)
obj_name	string(255)
obj_value	string(255)
msg	string(8192)

0300010000 (script)

This log ID relates to a script event involving error system load a script file.

Message: `script log`

Meaning: The system loaded a script.

Priority: information