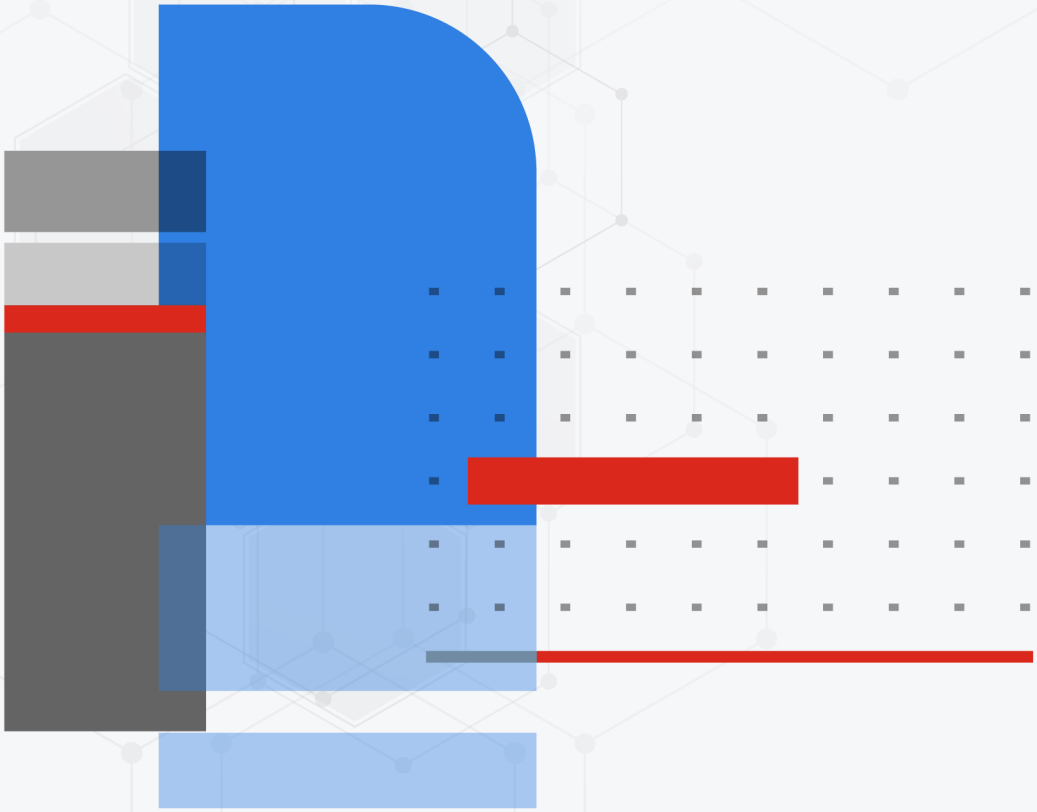
Fabric Normalization Reference

FortiAnalyzer 7.4.5



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 17, 2024
FortiAnalyzer 7.4.5 Fabric Normalization Reference
00-745-815638-20241017

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-17	Initial release.

FortiAnalyzer normalized Fabric logs

Logs from different Fabric devices can be normalized on FortiAnalyzer. When one or more devices are added to a Fabric ADOM and logs are sent to FortiAnalyzer, a SIEM database (siemdb) is automatically created for the ADOM. All logs are inserted into the siemdb and displayed in *Log View* > *Fabric* > *All* as normalized logs. This allows FortiAnalyzer administrators to view logs from Fabric devices in one place with log fields that are consistent across the devices.

SIEM features are available with all VM models and most hardware models starting in 6.4.0 and later.

This reference guide includes supported Fabric devices and the log field correlations between Fabric devices and FortiAnalyzer that are used to support normalized Fabric logs.

Fabric log field descriptions

The normalized fabric log fields are organized in the following categories.

Category	Description
base	Metadata as the proprietary fields of FortiAnalyzer.
data_source	Metadata as the data source fields of SIEM parser.
Application	Application data. Specifies the shared communication service and application's information used by hosts in a communications network.
Destination	Destination data. Represents movement through geographic space, from a source to a destination.
Event	Event data. Collected and stored by various tracking tools or methods in order to provide insights about user behavior, traffic patterns, and other metrics related to online events.
File	File data. Stores information to be used by a computer application or system.
Host	Host data. Stores information of a computer or other device that communicates with other hosts on a network.
Network	Network data. Defines metadata about network information seen in a typical OSI layer.
Protocol	Protocol data. Defines metadata about protocol related information for transmitting/exchanging data between the devices.
Source	Source data. Represents movement through geographic space, from a source to a destination.
Threat	Threat data. Refers to a known list of malicious threat information.
User	User data. Defines metadata about users in a network environment.

The following tables list the available normalized fabric log fields in FortiAnalyzer 7.4.5.

base

Normalized fabric log field	Type	Description
adom_oid	uint32	ADOM ID from DVM for internal use.
dstepid	uint32	Endpoint ID used as key for FortiAnalyzer-DST-UEBA correlation.
dsteuid	uint32	End-user ID used as key for FortiAnalyzer-DST-UEBA correlation.
epid	uint32	Endpoint ID used as key for FortiAnalyzer-UEBA correlation.
euid	uint32	End-user ID used as key for FortiAnalyzer-UEBA correlation.
itime	uint32	Timestamp set by FortiAnalyzer when it receives the data.
loguid	uint64	Unique ID set by FortiAnalyzer on each log for internal use.

data_source

Normalized fabric log field	Type	Description
data_parsername	string	Parser name used for parsing data.
data_sourceid	string	Machine\Host\Device\VM ID for the data source.
data_sourcename	string	Machine\Host\Device\VM Name for the data source.
data_sourcetype	string	Data source type.
data_sourceversion	string	Data source version.
data_timestamp	uint32	Timestamp set by data source.

Application

Normalized fabric log field	Type	Description
app_cat	string	Application category.
app_id	uint32	Application ID.
app_name	string	Application name.
app_proc	string	Process name.
app_ref	string	Reference for additional information about application.
app_service	string	Service name.
app_state	string	Application state.
app_ver	string	Application version.

Destination

Normalized fabric log field	Type	Description
dst_domain	string	Destination domain name.
dst_geo	string	Destination geo.
dst_intf	string	Destination interface.
dst_intf_guid	string	GUID of the network interface which was used for authentication request.
dst_ip	ip	Destination IP.
dst_mac	string	Destination MAC.
dst_natip	ip	Destination NAT IP.
dst_natport	uint16	Destination NAT port.
dst_port	uint16	Destination port.

Event

Normalized fabric log field	Type	Description
event_action	string	Main action taken.
event_cat	string	Event category.
event_id	uint32	Event\Log ID from data source.
event_message	string	Main message from data source or set by parser.
event_outcome	string	Event outcome.
event_policy	string	Event policy.
event_profile	string	Event profile.
event_ref	string	Reference for additional info about event.
event_severity	string	Event severity.
event_source	string	Data\Event source on Application layer.
event_subtype	string	Event subtype.
event_type	string	Event type.

File

Normalized fabric log field	Type	Description
file_accessetime	uint32	File accessed time.

Normalized fabric log field	Type	Description
file_createtime	uint32	File create time.
file_ext	string	File extention.
file_hash	string	File hash.
file_hashtype	string	File hash type.
file_name	string	File name.
file_path	string	File path.
file_size	string	File size.

Host

Normalized fabric log field	Type	Description
host_classification	string	Host classification.
host_hwvendor	string	Host hardware vendor.
host_hwver	string	Host hardware version.
host_ip	ip	Host IP.
host_location	string	Host location.
host_mac	string	Hostname MAC.
host_model_name	string	Host model name.
host_name	string	Host name.
host_osfamily	string	Host OS family.
host_osname	string	Host OS name.
host_osver	string	Host OS version.
host_owner	string	Host owner.
host_type	string	Host type.
host_uid	string	EDR Agent ID such as FortiClient UID.

Network

Normalized fabric log field	Type	Description
net_direction	string	Network direction.
net_name	string	Network name.
net_payloadid	uint32	Network payload ID.
net_proto	string	Network protocol.

Normalized fabric log field	Type	Description
net_rcvdpkts	uint64	Number of received packets.
net_recvbytes	uint64	Received bytes.
net_sentbytes	uint64	Sent bytes.
net_sentpkts	uint64	Number of sent packets.
net_sessionduration	uint32	Session duration.
net_sessionid	string	Session ID.
net_ssid	string	Network SSID.

Protocol

Normalized fabric log field	Type	Description
dns_query	string	DNS query data.
dns_querytype	string	DNS query type.
dns_response	string	DNS response data.
http_cookie	string	HTTP cookie.
http_method	string	HTTP method.
http_referer	string	HTTP referer.
http_status_code	uint16	HTTP response status code. 1XX Informational codes; 2XX Success codes; 3XX Redirection codes; 4XX Client error codes; 5XX Server error codes.
http_status_message	string	HTTP server reply message.
http_url	string	HTTP URL.
http_useragent	string	HTTP user agent.
mail_from	string	Mail from.
mail_size	uint32	Mail size.
mail_subject	string	Mail subject.
mail_to	string	Mail to.

Source

Normalized fabric log field	Type	Description
src_domain	string	Source domain.
src_geo	string	Source geo.

Normalized fabric log field	Type	Description
src_intf	string	Source interface.
src_ip	ip	Source IP.
src_mac	string	Source MAC
src_natip	ip	Source NAT IP.
src_natport	uint16	Source NAT port.
src_port	uint16	Source port.

Threat

Normalized fabric log field	Type	Description
threat_action	string	Threat action.
threat_direction	string	Threat direction.
threat_id	string	Threat ID.
threat_name	string	Threat name.
threat_pattern	string	Threat pattern.
threat_ref	string	Threat reference.
threat_score	uint32	Threat score.
threat_severity	string	Threat severity.
threat_type	string	Threat type.

User

Normalized fabric log field	Type	Description
user_authtype	string	User authtype.
user_classification	string	User importance as per data source.
user_domain	string	User domain.
user_email	string	User email.
user_group	string	User group.
user_id	string	User's ID/username (login).
user_location	string	User location info.
user_name	string	User's full name.
user_org	string	User organization.
user_phone	string	User phone number.

Normalized fabric log field	Type	Description
user_role	string	User role.
user_social	string	User's social account information.

FortiGate logs

FortiAnalyzer supports normalizing FortiGate logs as Fabric logs.

The following field mapping applies:

FortiGate Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
appcat	app_cat
appid	app_id
app,saasapp	app_name
service	app_service
qname	dns_query
dns_querytype	dns_querytype
ipaddr	dns_response
hostname	dst_domain
dstcountry	dst_geo
dst_info	dst_intf
dstip,dst_ip	dst_ip
dstmac	dst_mac
dst_natip,tranip	dst_natip
dst_natport,tranport	dst_natport
dstport,dst_port	dst_port
action	event_action
event_id	event_id
event_message	event_message

FortiGate Log Field	Normalized Fabric Log Field
error	event_outcome
event_policy	event_policy
applist,profile	event_profile
level	event_severity
subtype	event_subtype
type	event_type
catdesc,videocategoryname,activitycategory	event_cat
analyticscksum	file_hash
filename	file_name
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
srccountry	host_location
host_mac	host_mac
host_name	host_name
srcfamily	host_osfamily
host_osname	host_osname
host_osver	host_osver
user	host_owner
host_type	host_type
srcuuid	host_uid
httpmethod	http_method
referralurl	http_referer
url	http_url
agent	http_useragent
srcssid	net_name
proto	net_proto
rcvdpkt,rcvdp	net_rcvdpkts
rcvdbyte,rcvdb	net_recvbytes

FortiGate Log Field	Normalized Fabric Log Field
sentbyte,sentb	net_sentbytes
sentpkt,sentp	net_sentpkts
duration,dur	net_sessionduration
sessionid	net_sessionid
srcssid	net_ssid
srcname	src_domain
srccountry	src_geo
source_info	src_intf
srcip,src_ip	src_ip
srcmac	src_mac
src_natip,transip	src_natip
src_natport,transport	src_natport
srcport,src_port	src_port
threat_action	threat_action
threat_direction	threat_direction
threat_id	threat_id
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref
threat_severity	threat_severity
threat_type	threat_type
group,unauthusersource	user_group
user,unauthuser	user_id

FortiManager logs

FortiAnalyzer supports normalizing FortiManager logs as Fabric logs.

The following field mapping applies:

FortiManager Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid

FortiManager Log Field	Normalized Fabric Log Field
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
script	app_ref
service	app_service
state	app_state
dstcountry	dst_geo
action,event_action	event_action
event_id	event_id
msg,constmsg	event_message
desc	event_outcome
desc	event_profile
event_message,authmsg	event_ref
level,pri	event_severity
subtype	event_subtype
type,eventtype	event_type
file,remote_filename	file_name
log_path	file_path
log_size	file_size
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
userfrom	host_location
host_mac	host_mac
device,remote_host,host_name	host_name
host_osname	host_osname
sw_version	host_osver
host_type	host_type
dev_oid	host_uid

FortiManager Log Field	Normalized Fabric Log Field
url	http_url
session_id,sid	net_sessionid
srccountry	src_geo
remote_ip	src_ip
remote_port	src_port
user_type	user_classification
use_mb	user_group
userid	user_id
address	user_location
user	user_name
adminprof	user_role

FortiClient logs

FortiAnalyzer supports normalizing FortiClient logs as Fabric logs.

The following field mapping applies:

FortiClient Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
fctver	data_sourceversion
data_timestamp	data_timestamp
cat	app_cat
appid	app_id
app	app_name
srcproduct	app_proc
fgtserial,appvendor	app_ref
service,ae_api,ems_service_info	app_service
endpoint_status	app_state
appversion,fctver	app_ver

FortiClient Log Field	Normalized Fabric Log Field
remotename	dst_domain
dstcountry	dst_geo
dstip,remoteip,destinationip	dst_ip
dstport,remoteport,destinationport	dst_port
action	event_action
logid	event_id
msg,affected_prod_list	event_message
status,epenfeatures	event_outcome
ruleid,policyname	event_policy
usingpolicy	event_profile
endpoint_features_info,clientfeature	event_ref
level	event_severity
event_subtype	event_subtype
type	event_type
filetype	file_ext
checksum	file_hash
file	file_name
path	file_path
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
device_ip,regip,host_ip	host_ip
devicemac,mac,host_mac	host_mac
hostname,device_name,host_name	host_name
os,host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
vpntype	http_method
social_srvc	http_referer

FortiClient Log Field	Normalized Fabric Log Field
url	http_url
direction	net_direction
proto	net_proto
rcvdbyte	net_recvbytes
sentbyte	net_sentbytes
sessionid	net_sessionid
domain	src_domain
srccountry	src_geo
srcip	src_ip
devicemac,mac	src_mac
srcport	src_port
threat_action	threat_action
threat_id	threat_id
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref
threat_severity	threat_severity
threat_type	threat_type
social_srvc	user_authtype
domain	user_domain
social_email	user_email
uid,vpnuser	user_id
user	user_name
pcdomain	user_org
social_phone	user_phone
social_user	user_social

FortiSandbox logs

FortiAnalyzer supports normalizing FortiSandbox logs as Fabric logs.

The following field mapping applies:

FortiSandbox Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
vmos	app_cat
jobid,sid	app_id
vmname	app_name
pid	app_proc
rsrc	app_ref
service	app_service
vmkey	app_ver
dstcountry	dst_geo
dstip	dst_ip
dstport	dst_port
concat_eventaction,snmpaction	event_action
logid,log_id	event_id
msg	event_message
letype	event_ref
level	event_severity
subtype	event_subtype
type	event_type
ftype	file_ext
file_hash	file_hash
file_hash_type	file_hashtype
fname	file_name
filepath	file_path
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip

FortiSandbox Log Field	Normalized Fabric Log Field
host_mac	host_mac
hostname,host,host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
url	http_url
emlsndr	mail_from
subject	mail_subject
emlrcvr	mail_to
proto	net_proto
srccountry	src_geo
srcip	src_ip
srcport	src_port
attackname,mname	threat_name
risk	threat_severity
stype	user_classification
ui	user_domain
email	user_email
user,unauthuser,suser	user_id

EMS-Connector logs

FortiAnalyzer supports normalizing EMS-Connector logs as Fabric logs.

The following field mapping applies:

EMS-Connector Log Field	Normalized Fabric Log Field
devid	data_sourceid
devid	data_sourcename
data_sourcetype	data_sourcetype
event_time,dtime,itime	data_timestamp

EMS-Connector Log Field	Normalized Fabric Log Field
msg	event_message
event_subtype	event_subtype
event_type	event_type
scan_time	event_start_time
event_time	event_time
connector_uuid	event_uuid
hostname	host_name
os_type	host_osfamily
os_ver	host_osname
fctuid	host_uid
connector_name	src_asset_id
site	src_domain
src_ip	src_ip
mac	src_mac
category	threat_category
vuln_id	threat_id
vuln_name	threat_name
severity	threat_severity
threat_type	threat_type
site	user_domain
user_name	user_name

FortiADC logs

FortiAnalyzer supports normalizing FortiADC logs as Fabric logs.

The following field mapping applies:

FortiADC Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype

FortiADC Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp
dm_appid	app_id
service	app_service
dns_req	dns_query
dns_resp	dns_response
dst	dst_domain
dstcountry	dst_geo
dst_port	dst_port
action	event_action
msg_id	event_id
msg	event_message
status	event_outcome
policy	event_policy
logdesc	event_profile
cfgattr	event_ref
level,pri	event_severity
subtype	event_subtype
type	event_type
quar_file_name,smtp_attachname	file_name
http_host,dm_orihost	host_name
http_cookie	http_cookie
http_method	http_method
http_referer	http_referer
http_url	http_url
http_agent	http_useragent
smtp_from	mail_from
smtp_bodylen	mail_size
smtp_subject	mail_subject
smtp_to	mail_to
proto	net_proto

FortiADC Log Field	Normalized Fabric Log Field
ibytes	net_recvbytes
obytes	net_sentbytes
dm_sessionid	net_sessionid
src	src_domain
srccountry	src_geo
src_port	src_port
threat_action	threat_action
threat_direction	threat_direction
threat_id	threat_id
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref
threat_score	threat_score
threat_severity	threat_severity
threat_type	threat_type
auth_status	user_authtype
usergrp	user_group
user	user_id
ftp_username	user_name

FortiAnalyzer logs

FortiAnalyzer supports normalizing FortiAnalyzer logs as Fabric logs.

The following field mapping applies:

FortiAnalyzer Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
script	app_ref

FortiAnalyzer Log Field	Normalized Fabric Log Field
service	app_service
state	app_state
dstcountry	dst_geo
action,event_action	event_action
event_id	event_id
msg,constmsg	event_message
desc	event_outcome
desc	event_profile
event_message,authmsg	event_ref
level,pri	event_severity
subtype	event_subtype
type,eventtype	event_type
file,remote_filename	file_name
log_path	file_path
log_size	file_size
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
userfrom	host_location
host_mac	host_mac
device,remote_host,host_name	host_name
host_osname	host_osname
sw_version	host_osver
host_type	host_type
dev_oid	host_uid
url	http_url
session_id,sid	net_sessionid
srccountry	src_geo
remote_ip	src_ip

FortiAnalyzer Log Field	Normalized Fabric Log Field
remote_port	src_port
user_type	user_classification
use_mb	user_group
userid	user_id
address	user_location
user	user_name
adminprof	user_role

FortiAuthenticator logs

FortiAnalyzer supports normalizing FortiAuthenticator logs as Fabric logs.

The following field mapping applies:

FortiAuthenticator Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
status	app_state
dstcountry	dst_geo
action	event_action
logid	event_id
msg	event_message
logdesc	event_profile
faclogindex	event_ref
level	event_severity
subtype	event_subtype
type	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver

FortiAuthenticator Log Field	Normalized Fabric Log Field
host_ip	host_ip
host_mac	host_mac
nas,host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
srccountry	src_geo
user	user_id

FortiCache logs

FortiAnalyzer supports normalizing FortiCache logs as Fabric logs.

The following field mapping applies:

FortiCache Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
appcat,app_cat,monitor-type,webfilter_catdesc	app_cat
appid,webfilter_cat_id	app_id
app,applist,app_list,monitor-name,webfilter_mode	app_name
appact,app_action,cloudaction	app_state
request_info	dns_query
scheme	dns_querytype
response_info	dns_response
dst_int	dst_domain
dstcountry	dst_geo
dstintf	dst_intf
dstip	dst_ip

FortiCache Log Field	Normalized Fabric Log Field
tranip	dst_natip
dstport	dst_port
action	event_action
logid	event_id
msg,logdesc	event_message
log_rate_info	event_outcome
ips_attack_id	event_policy
ips_profile,spam_profile	event_profile
level,ips_severity	event_severity
subtype,messagetype,message_type	event_subtype
type,eventtype	event_type
filetype,spam_file_type	file_ext
checksum	file_hash
virus_file_hashtype	file_hashtype
filename,spam_subject,filesize	file_name
spam_file_size,filesize	file_size
host_info,host_classification	host_classification
osgen,os_gen,osvendor,host_hwvendor	host_hwvendor
host_hwver	host_hwver
ip,host_ip	host_ip
srccountry	host_location
mastersrcmac,host_mac	host_mac
hostname,host_name	host_name
osfamily	host_osfamily
osname,os,host_osname	host_osname
osversion,host_osver	host_osver
hostname	host_owner
devtype,host_type	host_type
host_uid	host_uid
method	http_method

FortiCache Log Field	Normalized Fabric Log Field
url,webfilter_url_list	http_url
agent	http_useragent
collectedemail,from	mail_from
spam_file_size	mail_size
spam_subject	mail_subject
to	mail_to
vpntype,direction	net_direction
vpn	net_name
policyid	net_payloadid
proto	net_proto
rcvdpkt	net_rcvdpkts
rcvdbyte	net_recvbytes
sentbyte,bandwidth	net_sentbytes
sentpkt	net_sentpkts
duration	net_sessionduration
sessionid	net_sessionid
srcssid	net_ssid
src_int	src_domain
srccountry	src_geo
srcintf	src_intf
srcip	src_ip
srcmac	src_mac
transip	src_natip
transport	src_natport
srcport	src_port
threat_action	threat_action
threat_id	threat_id
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref

FortiCache Log Field	Normalized Fabric Log Field
threat_severity	threat_severity
threat_type	threat_type
group	user_group
custom,clouduser	user_id
user	user_name

FortiCASB logs

FortiAnalyzer supports normalizing FortiCASB logs as Fabric logs.

The following field mapping applies:

FortiCASB Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
dstcountry	dst_geo
eventtype	event_cat
policytype,policymode	event_policy
poluuid	event_profile
severity	event_severity
subtype	event_subtype
type	event_type
filetype,infectedfiletype	file_ext
filename,infectedfilename	file_name
filesize,infectedfilesize	file_size
hostname	host_name
httpmethod	http_method
url	http_url
from	mail_from
subject	mail_subject

FortiCASB Log Field	Normalized Fabric Log Field
to	mail_to
sentbyte	net_sentbytes
rcvdbyte	net_sentpkts
sessionid	net_sessionid
srcdomain	src_domain
srccountry	src_geo
srcip	src_ip
user	user_id

FortiDDoS logs

FortiAnalyzer supports normalizing FortiDDoS logs as Fabric logs.

The following field mapping applies:

FortiDDoS Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
status	app_state
dstcountry	dst_geo
dip	dst_ip
dport	dst_port
action	event_action
msg_id,log_id	event_id
msg	event_message
detail	event_outcome
attack_observed_profile	event_profile
event_state_disp	event_ref
level	event_severity
subtype	event_subtype

FortiDDoS Log Field	Normalized Fabric Log Field
type	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
subnet_name	net_name
srccountry	src_geo
sip	src_ip
sport	src_port
attack_desc	threat_action
attack_direction	threat_direction
evecode	threat_id
uniqueid	threat_name
detail	threat_ref

FortiDeceptor logs

FortiAnalyzer supports normalizing FortiDeceptor logs as Fabric logs.

The following field mapping applies:

FortiDeceptor Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp

FortiDeceptor Log Field	Normalized Fabric Log Field
service	app_service
dstcountry	dst_geo
victimip	dst_ip
action	event_action
eventid	event_id
msg	event_message
status	event_outcome
level	event_severity
subtype	event_subtype
type	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
srccountry	src_geo
attackerip	src_ip
user	user_id
username	user_name

FortiEDR logs

FortiAnalyzer supports normalizing FortiEDR logs as Fabric logs.

The following field mapping applies:

FortiEDR Log Field	Normalized Fabric Log Field
devid	data_sourceid
device_name,devid	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
component_type	app_cat
data_id	app_id
component_name	app_name
autonomous_system	app_ref
device_state	app_state
dstcountry	dst_geo
action	event_action
event_id	event_id
event_message	event_message
destination	event_outcome
rule_list	event_policy
severity	event_severity
classification	event_subtype
event_type	event_type
last_seen	file_accessetime
first_seen	file_createtime
process_hash	file_hash
process_name,script,remediation_files	file_name
process_path,script_path	file_path
source_ip	host_ip
mac_address	host_mac
device_name	host_name
operating_system	host_osname
remote_connection	http_method
organization	src_domain
country,srccountry	src_geo

FortiEDR Log Field	Normalized Fabric Log Field
source_ip	src_ip
action	threat_action
siem_threat_name	threat_name
siem_threat_pattern	threat_pattern
siem_threat_type	threat_type
users	user_id
user_name	user_name

FortiFirewall logs

FortiAnalyzer supports normalizing FortiFirewall logs as Fabric logs.

The following field mapping applies:

FortiFirewall Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
appcat,app_cat,app-type	app_cat
appid	app_id
app	app_name
service	app_service
appact,app_action	app_state
dns_name	dns_querytype
dstname	dst_domain
dstcountry,dst_country	dst_geo
dstintf,dst_int	dst_intf
dstip,dst	dst_ip
dstmac	dst_mac
dstport,dst_port	dst_port
action,status	event_action

FortiFirewall Log Field	Normalized Fabric Log Field
msg	event_message
policyid	event_policy
alert,error	event_profile
level	event_severity
subtype	event_subtype
type	event_type
processtime	file_accessetime
hash	file_hash
file	file_name
filesize	file_size
srchwvendor	host_hwvendor
srchwversion	host_hwver
mac	host_mac
hostname	host_name
srcfamily	host_osfamily
osname	host_osname
osversion	host_osver
devtype	host_type
vpntype	http_method
vpn	http_referer
url	http_url
agent	http_useragent
from	mail_from
to	mail_to
direction	net_direction
rcvdpkt,rcvd_pkt	net_rcvdpkts
rcvdbyte,rcvd	net_recvbytes
sentbyte,sent	net_sentbytes
sentpkt,sent_pkt	net_sentpkts
duration	net_sessionduration

FortiFirewall Log Field	Normalized Fabric Log Field
sessionid,SN	net_sessionid
srcssid,ssid	net_ssid
srcname,srcdomain	src_domain
srccountry,src_country	src_geo
srcintf,src_int	src_intf
srcip,src	src_ip
srcmac	src_mac
srcport,src_port	src_port
utmaction	threat_action
virus,attack,attackname,attack_name,vulnname	threat_name
securitymode	threat_pattern
security	threat_severity
group	user_group
user,carrier_ep	user_id
unauthuser,dstunauthuser	user_name

FortiIsolator logs

FortiAnalyzer supports normalizing FortiIsolator logs as Fabric logs.

The following field mapping applies:

FortiIsolator Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
browsertype	app_name
pid	app_proc
browserver	app_ver
dstcountry	dst_geo
avaction,wfaction	event_action

FortiIsolator Log Field	Normalized Fabric Log Field
msg	event_message
avresult	event_outcome
avblockreason	event_policy
avengine,wfprofile,icapprofile,iprofile,clicmd	event_profile
event_severity	event_severity
subtype	event_subtype
type	event_type
filepath	file_path
filesize	file_size
protocol	http_method
dsturl	http_url
sessionid	net_sessionid
srccountry	src_geo
clientip	src_ip
usertype	user_classification
user	user_id

FortiMail logs

FortiAnalyzer supports normalizing FortiMail logs as Fabric logs.

The following field mapping applies:

FortiMail Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
dstcountry	dst_geo
dst_ip	dst_ip
concat_eventaction,disposition	event_action
logid,log_id	event_id

FortiMail Log Field	Normalized Fabric Log Field
msg	event_message
polid	event_policy
classifier	event_profile
event_message	event_ref
pri	event_severity
subtype	event_subtype
type	event_type
file_hash	file_hash
file_hash_type	file_hashtype
file_name	file_name
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
mail_from	mail_from
message_length	mail_size
subject	mail_subject
to	mail_to
direction	net_direction
session_id	net_sessionid
client_name	src_domain
location,srccountry	src_geo
client_ip	src_ip
threat_name	threat_name
threat_pattern	threat_pattern

FortiMail Log Field	Normalized Fabric Log Field
ui,domain_name	user_domain
user,user_name	user_id

FortiNAC logs

FortiAnalyzer supports normalizing FortiNAC logs as Fabric logs.

The following field mapping applies:

FortiNAC Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
sn	app_name
agentplat	app_service
mailstate	app_state
agentver,fwver	app_ver
dstcountry	dst_geo
action	event_action
msg	event_message
severity	event_severity
subtype	event_subtype
type	event_type
lastactivitytime	file_accessetime
createtime	file_createtime
imagetype	file_ext
element,label,host_classification	host_classification
vendorname,vendoroid,host_hwvendor	host_hwvendor
hwtype,host_hwver	host_hwver
ip,host_ip	host_ip
location	host_location

FortiNAC Log Field	Normalized Fabric Log Field
mac,host_mac	host_mac
hostname,name,host_name	host_name
os,host_osname	host_osname
fwver,host_osver	host_osver
owner	host_owner
endpointtype,devtype,cat,host_type	host_type
endpointid,vendoroid	host_uid
srccountry	src_geo
portid	src_port
usertype	user_classification
adminprofile	user_domain
email	user_email
userid,user	user_id
user_geo	user_location
user_username	user_name
org	user_org
user_phone	user_phone
position	user_role
user_social	user_social

FortiNDR logs

FortiAnalyzer supports normalizing FortiNDR logs as Fabric logs.

The following field mapping applies:

FortiNDR Log Field	Normalized Fabric Log Field
devid	data_sourceid
device_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
status	app_state

FortiNDR Log Field	Normalized Fabric Log Field
dstcountry	dst_geo
action	event_action
logid	event_id
level	event_severity
subtype	event_subtype
type	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
devhost,host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
srccountry	src_geo
victimip	src_ip
victimport	src_port
virusname	threat_name
url,filetype	threat_pattern
risklevel	threat_severity
scenariotype	threat_type
user	user_id

FortiPAM logs

FortiAnalyzer supports normalizing FortiPAM logs as Fabric logs.

The following field mapping applies:

FortiPAM Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
appcat	app_cat
appid	app_id
app	app_name
daemon,pid	app_proc
service	app_service
state	app_state
qname	dns_query
qtype	dns_querytype
hostname	dst_domain
dstcountry	dst_geo
dst_info	dst_intf
dstip	dst_ip
dstmac	dst_mac
tranip	dst_natip
tranport	dst_natport
dstport,dst_port	dst_port
action	event_action
logid,log_id	event_id
msg	event_message
error	event_outcome
policyid	event_policy
applist	event_profile
level	event_severity
subtype	event_subtype
type	event_type
filetype	file_ext

FortiPAM Log Field	Normalized Fabric Log Field
hash,checksum	file_hash
file,filename	file_name
path	file_path
filesize	file_size
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
mastersrcmac,host_mac	host_mac
srcname,host_name	host_name
osname,host_osname	host_osname
osversion,host_osver	host_osver
devtype,host_type	host_type
srcuuid	host_uid
url	http_url
agent	http_useragent
from	mail_from
size	mail_size
subject	mail_subject
to	mail_to
direction	net_direction
srcssid	net_name
proto	net_proto
rcvdpkt	net_rcvdpkts
rcvdbyte	net_recvbytes
sentbyte	net_sentbytes
sentpkt	net_sentpkts
duration	net_sessionduration
sessionid,session_id	net_sessionid
ssid	net_ssid

FortiPAM Log Field	Normalized Fabric Log Field
srcname	src_domain
srccountry	src_geo
src_info	src_intf
srcip	src_ip
srcmac,source_mac	src_mac
transip	src_natip
transport	src_natport
srcport,src_port	src_port
sslaction	threat_action
direction	threat_direction
vulnid,virusid,attackid	threat_id
vulnname,virus,attack	threat_name
attackcontext	threat_pattern
ref,cveid	threat_ref
auditscore	threat_score
severity	threat_severity
threattype	threat_type
group,unauthusersource	user_group
user,unauthuser,clouduser	user_id

FortiProxy logs

FortiAnalyzer supports normalizing FortiProxy logs as Fabric logs.

The following field mapping applies:

FortiProxy Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
appcat	app_cat

FortiProxy Log Field	Normalized Fabric Log Field
appid	app_id
app	app_name
daemon,pid	app_proc
service	app_service
state	app_state
qname	dns_query
qtype	dns_querytype
hostname	dst_domain
dstcountry	dst_geo
dst_info	dst_intf
dstip	dst_ip
dstmac	dst_mac
tranip	dst_natip
tranport	dst_natport
dstport,dst_port	dst_port
action	event_action
logid,log_id	event_id
msg	event_message
error	event_outcome
policyid	event_policy
applist	event_profile
level	event_severity
subtype	event_subtype
type	event_type
filetype	file_ext
hash,checksum	file_hash
file,filename	file_name
path	file_path
filesize	file_size
host_classification	host_classification

FortiProxy Log Field	Normalized Fabric Log Field
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
mastersrcmac,host_mac	host_mac
srcname,host_name	host_name
osname,host_osname	host_osname
osversion,host_osver	host_osver
devtype,host_type	host_type
srcuuid	host_uid
url	http_url
agent	http_useragent
from	mail_from
size	mail_size
subject	mail_subject
to	mail_to
direction	net_direction
srcssid	net_name
proto	net_proto
rcvdpkt	net_rcvdpkts
rcvdbyte	net_recvbytes
sentbyte	net_sentbytes
sentpkt	net_sentpkts
duration	net_sessionduration
sessionid,session_id	net_sessionid
ssid	net_ssid
srcname	src_domain
srccountry	src_geo
src_info	src_intf
srcip	src_ip
srcmac,source_mac	src_mac

FortiProxy Log Field	Normalized Fabric Log Field
transip	src_natip
transport	src_natport
srcport,src_port	src_port
sslaction	threat_action
direction	threat_direction
vulnid,virusid,attackid	threat_id
vulnname,virus,attack	threat_name
attackcontext	threat_pattern
ref,cveid	threat_ref
auditscore	threat_score
severity	threat_severity
threattype	threat_type
group,unauthusersource	user_group
user,unauthuser,clouduser	user_id

FortiSOAR logs

FortiAnalyzer supports normalizing FortiSOAR logs as Fabric logs.

The following field mapping applies:

FortiSOAR Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,dtime	data_timestamp
FSR_NAME	app_name
service_name	app_service
FSR_VER	app_ver
dstcountry	dst_geo
event_id	event_id
event_message	event_message

FortiSOAR Log Field	Normalized Fabric Log Field
event_profile	event_profile
event_severity	event_severity
event_subtype	event_subtype
event_type	event_type
host_classification	host_classification
host_name	host_name
srccountry	src_geo
src_ip	src_ip
user_id	user_id
user_name	user_name

FortiSwitch logs

FortiAnalyzer supports normalizing FortiSwitch logs as Fabric logs.

The following field mapping applies:

FortiSwitch Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
dstcountry	dst_geo
dstip	dst_ip
action	event_action
logid,log_id	event_id
msg	event_message
status	event_outcome
profile,reason	event_profile
level,pri	event_severity
subtype	event_subtype
type	event_type

FortiSwitch Log Field	Normalized Fabric Log Field
ui	http_url
mirror-session	net_sessionid
srccountry	src_geo
switch.interface	src_intf
srcip,auto-ip	src_ip
switch.physical-port,port	src_port
userfrom	user_group
user	user_id

FortiToken logs

FortiAnalyzer supports normalizing FortiToken logs as Fabric logs.

The following field mapping applies:

FortiToken Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
action	event_action
response	event_message
result	event_outcome
resource	event_profile
event_ref	event_ref
subtype	event_subtype
type	event_type
source_device	src_domain
user_ip	src_ip
realm_id	user_domain
account_id	user_id
username	user_name

FortiWeb logs

FortiAnalyzer supports normalizing FortiWeb logs as Fabric logs.

The following field mapping applies:

FortiWeb Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
service,backend_service,server_pool_name	app_service
http_host	dst_domain
dstcountry	dst_geo
dst_info	dst_intf
dst	dst_ip
dstport,dst_port	dst_port
action	event_action
logid,log_id	event_id
msg	event_message
status	event_outcome
trigger_policy,policy	event_policy
pri,severity_level	event_severity
subtype	event_subtype
type	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
host_name	host_name
host_osname	host_osname
host_osver	host_osver
devtype,host_type	host_type

FortiWeb Log Field	Normalized Fabric Log Field
host_uid	host_uid
http_method	http_method
http_refer	http_referer
http_url	http_url
http_agent	http_useragent
proto	net_proto
srccountry,original_srccountry	src_geo
ui	src_intf
src	src_ip
srcport,src_port	src_port
threat_action	threat_action
direction	threat_direction
main_type	threat_name
signature_info,bot_info	threat_pattern
threat_weight	threat_score
threat_level	threat_severity
threat_type	threat_type
user	user_id
user_name	user_name

Apache logs

FortiAnalyzer supports normalizing Apache logs as Fabric logs.

The following field mapping applies:

Apache Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_name	app_name

Apache Log Field	Normalized Fabric Log Field
pid	app_proc
service	app_service
message	event_message
file_name	file_name
host_ip	host_ip
host_name	host_name
http_method	http_method
http_referer	http_referer
http_url	http_url
http_useragent	http_useragent
http_status_code	http_status_code

Nginx logs

FortiAnalyzer supports normalizing Nginx logs as Fabric logs.

The following field mapping applies:

Nginx Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_name	app_name
message	event_message
host_ip	host_ip
host_name	host_name
http_method	http_method
http_referer	http_referer
http_url	http_url
http_useragent	http_useragent

System logs

FortiAnalyzer supports normalizing System logs as Fabric logs.

The following field mapping applies:

System Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
host_name,devid	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
app_cat	app_cat
service	app_service
message,cleaned_msg,msg	event_message
level	event_severity
type	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid

Ubuntu logs

FortiAnalyzer supports normalizing Ubuntu logs as Fabric logs.

The Ubuntu Syslog Parser will only parse Ubuntu logs if they are sent from FortiClient.

The following field mapping applies:

Ubuntu Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_name	app_name
pid	app_proc
service	app_service
dst_info	dst_intf
event_action	event_action
message	event_message
log_level	event_severity
ext_eventsubtype	event_subtype
ext_eventtype	event_type
host_classification	host_classification
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
hostname,host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
ip	src_ip
srcmac	src_mac

Windows Event logs

FortiAnalyzer supports normalizing Windows Event logs as Fabric logs.

The Windows Event Log Parser will only parse Windows event logs if:

- the logs are sent from FortiClient to FortiAnalyzer, or
- the syslog logs are sent from the Windows endpoint directly to FortiAnalyzer in JSON format.

The following field mapping applies:

Windows Event Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
app_cat,channel	app_cat
app_name,provider_name	app_name
execution_pid	app_proc
app_ref	app_ref
version	app_ver
domain_name	dst_domain
dstcountry	dst_geo
dstip	dst_ip
sys_keywords	event_action
event_id	event_id
event_log,exch_log,event_json	event_message
event_data_return_code,event_outcome	event_outcome
event_profile	event_profile
event_record_id,event_ref	event_ref
event_severity,level	event_severity
event_subtype,provider_name	event_subtype
event_type,channel	event_type
host_ip	host_ip
host_name	host_name
os_family	host_osfamily
host_uid	host_uid
mail_from	mail_from

Windows Event Log Field	Normalized Fabric Log Field
mail_subject	mail_subject
net_direction	net_direction
net_proto	net_proto
net_sentbytes	net_sentbytes
src_domain	src_domain
srccountry	src_geo
srcip,src_ip	src_ip
user_domain,event_data_subj_domain_name	user_domain
user_group	user_group
user_id,event_data_subj_user_sid	user_id
user_name,event_data_subj_user_name	user_name

www.fortinet.com