Fabric Normalization Reference Guide

FortiAnalyzer 7.2.4

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

September 28, 2023
FortiAnalyzer 7.2.4 Fabric Normalization Reference Guide
00-724-815638-20230928

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-09-28	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

Normalized Fabric Log Field	Description
app_cat	Application Category
app_id	Application ID
app_proc	Application Process
app_ref	Application Reference
app_service	Application Service
app_state	Application State
app_ver	Application Version
app_name	Application Name
data_parsername	Data Parser Name
data_sourceid	Data Source ID
data_sourcename	Data Source Name
data_sourcetype	Data Source Type
data_sourceversion	Data Source Version
data_timestamp	Data Timestamp
dns_query	DNS Query
dns_querytype	DNS Query Type
dns_req	DNS Request
dns_resp	DNS Response

Normalized Fabric Log Field	Description
dns_response	DNS Response
dst_domain	Destination Domain
dst_geo	Destination Geo
dst_intf	Destination Interface
dst_mac	Destination MAC
dst_natip	Destination Nat IP
dst_natport	Destination Nat Port
event_action	Event Action
event_outcome	Event Outcome
event_policy	Event Policy
event_profile	Event Profile
event_ref	Event Ref
event_severity	Event Severity
event_subtype	Event Sub Type
event_type	Event Type
event_message	Event Message
file_accessetime	File Accessed Time
file_createtime	File Created Time
file_ext	File Extension
file_hash	File Hash
file_hashtype	File Hash Type
file_name	File Name
file_path	File Path
file_size	File Size
host_classification	Host Classification
host_hwvendor	Host Hardware Vendor
host_hwver	Host Hardware Version
host_ip	Host IP
host_location	Host Location
host_mac	Host MAC

Normalized Fabric Log Field	Description
host_name	Host Name
host_osfamily	Host OS Family
host_osname	Host OS Name
host_osver	Host OS Version
host_owner	Host Owner
host_type	Host Type
host_uid	Host UID
http_cookie	HTTP Cookie
http_referer	HTTP Referrer
http_useragent	HTTP User Agent
loguid	Data UID
mail_from	Mail From
mail_size	Mail Size
mail_subject	Mail Subject
mail_to	Mail To
net_direction	Net Direction
net_name	Net Name
net_payloadid	Net Payload ID
net_proto	Net Protocol
net_rcvdpkts	Net Received Packets
net_recvbytes	Net Received Bytes
net_sentbytes	Net Sent Bytes
net_sentpkts	Net Sent Packets
net_sessionduration	Net Session Duration
net_sessionid	Net Session ID
net_ssid	Net SSID
objectid	Object ID
objectname	Object Name
obj_name	Object Name
obj_value	Object Value

Normalized Fabric Log Field	Description
procid	Process ID
procname	Process Name
procowner	Process Owner
servicename	Service Name
src_domain	Source Domain
src_geo	Source Geo
src_intf	Source Interface
src_mac	Source MAC
src_natip	Source Nat IP
src_natport	Source Nat Port
src_ip	Source IP
threat_action	Threat Action
threat_direction	Threat Direction
threat_hash	Threat Hash
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
user_authtype	User Authentication Type
user_classification	User Classification
user_domain	User Domain
user_email	User Email
user_group	User Group
user_id	User ID
user_location	User Location
user_org	User Organization
user_phone	User Phone

Normalized Fabric Log Field	Description
user_role	User Role
user_social	User Social

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_timestamp	data_timestamp
appcat	app_cat
appid	app_id
app	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
error	event_outcome

FortiGate Log Field	Normalized Fabric Log Field
event_policy	event_policy
applist	event_profile
level	event_severity
subtype	event_subtype
type	event_type
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
referralurl	http_referer
url	http_url
srcssid	net_name
proto	net_proto
rcvdpkt,rcvdp	net_rcvdpkts
rcvdbyte,rcvdb	net_recvbytes
sentbyte,sentb	net_sentbytes
sentpkt,sentp	net_sentpkts
duration,dur	net_sessionduration
sessionid	net_sessionid

FortiGate Log Field	Normalized Fabric Log Field
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/FortiAnalyzer logs

FortiAnalyzer supports normalizing FortiManager/FortiAnalyzer logs as Fabric logs.

The following field mapping applies:

FortiManager/FortiAnalyzer Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
devid,device_id	data_sourceid
data_source_name	data_sourcename

FortiManager/FortiAnalyzer Log Field	Normalized Fabric Log Field
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
script	app_ref
service	app_service
state	app_state
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

FortiManager/FortiAnalyzer Log Field	Normalized Fabric Log Field
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
device_id	data_sourceid
data_source_name	data_sourcename
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
remotename	dst_domain
dstip,remoteip,destinationip	dst_ip
dstport,remoteport,destinationport	dst_port
action	event_action

FortiClient Log Field	Normalized Fabric Log Field
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
url	http_url
direction	net_direction
proto	net_proto
rcvdbyte	net_recvbytes
sentbyte	net_sentbytes

FortiClient Log Field	Normalized Fabric Log Field
sessionid	net_sessionid
domain	src_domain
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
loguid,id	loguid
epid	epid
euid	euid
devid,device_id	data_sourceid

FortiSandbox Log Field	Normalized Fabric Log Field
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
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
host_mac	host_mac
hostname,host,host_name	host_name

FortiSandbox Log Field	Normalized Fabric Log Field
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
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

FortiAuthenticator logs

FortiAnalyzer supports normalizing FortiAuthenticator logs as Fabric logs.

The following field mapping applies:

FortiAuthenticator Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp

FortiAuthenticator Log Field	Normalized Fabric Log Field
status	app_state
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
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
user	user_id

FortiADC logs

FortiAnalyzer supports normalizing FortiADC logs as Fabric logs.

The following field mapping applies:

FortiADC Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
device_id, devid	data_sourceid

FortiADC Log Field	Normalized Fabric Log Field
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
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

FortiADC Log Field	Normalized Fabric Log Field
smtp_to	mail_to
proto	net_proto
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

FortiAI logs

FortiAnalyzer supports normalizing FortiAI logs as Fabric logs.

The following field mapping applies:

FortiAI Log Field	Normalized Fabric Log Field
devid	data_sourceid
device_name	data_sourcename
data_timestamp	data_timestamp

FortiAI Log Field	Normalized Fabric Log Field
status	app_state
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
victimip	src_ip
victimport	src_port
virusname	threat_name
url,filetype	threat_pattern
risklevel	threat_severity
scenariotype	threat_type
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
loguid,id	loguid

FortiCache Log Field	Normalized Fabric Log Field
epid	epid
euid	euid
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	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
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

FortiCache Log Field	Normalized Fabric Log Field
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
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

FortiCache Log Field	Normalized Fabric Log Field
sentpkt	net_sentpkts
duration	net_sessionduration
sessionid	net_sessionid
srcssid	net_ssid
src_int	src_domain
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
threat_severity	threat_severity
threat_type	threat_type
group	user_group
custom,clouduser	user_id
user	user_name

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_timestamp	data_timestamp

FortiDeceptor Log Field	Normalized Fabric Log Field
service	app_service
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
attackerip	src_ip
user	user_id
username	user_name

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

FortiDDoS Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp
status	app_state
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
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
sip	src_ip
sport	src_port
attack_desc	threat_action
attack_direction	threat_direction
evecode	threat_id
uniqueid	threat_name
detail	threat_ref

FortiEDR logs

FortiAnalyzer supports normalizing FortiEDR logs as Fabric logs.

The following field mapping applies:

FortiEDR Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
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
autonomours_system	app_ref
device_state	app_state
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_accesstime
first_seen	file_createtime
process_hash	file_hash
process_nam, script, remediation_files	file_name
process_path, script_path	file_path
source_ip	host_ip
mac_address	host_mac

FortiEDR Log Field	Normalized Fabric Log Field
device_name	host_name
operating_system	host_osname
remote_connection	http_method
organization	src_domain
country	src_geo
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
loguid,id	loguid
epid	epid
euid	euid
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

FortiFirewall Log Field	Normalized Fabric Log Field
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
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

FortiFirewall Log Field	Normalized Fabric Log Field
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
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
id, loguid	loguid

FortiIsolator Log Field	Normalized Fabric Log Field
epid	epid
euid	euid
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	dat_sourcetype
eventtime	data_timestamp
browsertype	app_name
pid	app_proc
browserver	app_ver
avaction, wfaction	event_action
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
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
loguid,id	loguid
epid	epid
euid	euid
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
dst_ip	dst_ip
concat_eventaction,disposition	event_action
logid,log_id	event_id
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

FortiMail Log Field	Normalized Fabric Log Field
message_length	mail_size
subject	mail_subject
to	mail_to
direction	net_direction
session_id	net_sessionid
client_name	src_domain
location	src_geo
client_ip	src_ip
threat_name	threat_name
threat_pattern	threat_pattern
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
loguid,id	loguid
epid	epid
euid	euid
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
sn	app_name
agentplat	app_service
mailstate	app_state
agentver,fwver	app_ver
action	event_action

FortiNAC Log Field	Normalized Fabric Log Field
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
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
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

FortiProxy logs

FortiAnalyzer supports normalizing FortiProxy logs as Fabric logs.

The following field mapping applies:

FortiProxy Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
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	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

FortiProxy Log Field	Normalized Fabric Log Field
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
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

FortiProxy Log Field	Normalized Fabric Log Field
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
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
loguid,id	loguid
epid	epid
euid	euid
device_id,devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
FSR_NAME	app_name
service_name	app_service
FSR_VER	app_ver
event_id	event_id
event_message	event_message
event_profile	event_profile
event_severity	event_severity
event_subtype	event_subtype
event_type	event_type
host_classification	host_classification
host_name	host_name
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
loguid,id	loguid
epid	epid
euid	euid

FortiSwitch Log Field	Normalized Fabric Log Field
device_id,devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
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
ui	http_url
mirror-session	net_sessionid
switch.interface	src_intf
srcip,auto-ip	src_ip
switch.physical-port,port	src_port
userfrom	user_group
user	user_id

FortiWeb logs

FortiAnalyzer supports normalizing FortiWeb logs as Fabric logs.

The following field mapping applies:

FortiWeb Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
devid,device_id	data_sourceid

FortiWeb Log Field	Normalized Fabric Log Field
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
service,backend_service,server_pool_name	app_service
http_host	dst_domain
srccountry	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
host_uid	host_uid
http_method	http_method
http_refer	http_referer
http_url	http_url

FortiWeb Log Field	Normalized Fabric Log Field
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

System logs

FortiAnalyzer supports normalizing System logs as Fabric logs.

The following field mapping applies:

System Log Field	Normalized Fabric Log Field
device_id	data_sourceid
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

System Log Field	Normalized Fabric Log Field
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 following field mapping applies:

Ubuntu Log Field	Normalized Fabric Log Field
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

Ubuntu Log Field	Normalized Fabric Log Field
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 following field mapping applies:

Windows Event Log Field	Normalized Fabric Log Field
loguid,id	loguid
epid	epid
euid	euid
devid	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
channel	app_cat
provider_guid	app_id
provider_name	app_name
execution_pid	app_proc
cor_activity_id	app_ref
version	app_ver
sys_keywords	event_action
event_id	event_id
event_log	event_message
event_data_return_code	event_outcome
event_record_id	event_ref
level	event_severity
provider_name	event_subtype

Windows Event Log Field	Normalized Fabric Log Field
channel	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
os_family	host_osfamily
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
event_data_subj_domain_name	user_domain
event_data_subj_user_sid	user_id
event_data_subj_user_name	user_name

www.fortinet.com