Fabric Normalization Reference

FortiAnalyzer 8.0.0

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

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 21, 2026
FortiAnalyzer 8.0.0 Fabric Normalization Reference
00-800-1278937-20260421

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-04-21	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 > Logs > 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.
Logon	Logon data. Defines metadata about the logon events.
Network	Network data. Defines metadata about network information seen in a typical OSI layer.
Process	Process data. Defines metadata about processes in an system. Isolated memory address space that is used to run a program.

Category	Description
Protocol	Protocol data. Defines metadata about protocol related information for transmitting/exchanging data between the devices.
Registry	Registry data. Defines metadata about Windows registry entries in a system.
Source	Source data. Represents movement through geographic space, from a source to a destination.
TLS	Transport Layer Security (TLS) data.
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 8.0.0.

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_action	string	The operation the user performed in the context of the application.
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_asset_id	string	Destination asset ID.
dst_domain	string	Destination domain name.
dst_geo	string	Destination geo.
dst_geo_city	string	Destination geo city information.
dst_geo_country	string	Destination geo country.
dst_geo_country_code	string	Destination geo country code.
dst_geo_latitude	string	Destination geo latitude.
dst_geo_longitude	string	Destination geo longitude.
dst_geo_region	string	Destination geo region.
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_count	uint32	The number of aggregated events.
event_creation_time	uint32	Original time when event/log was created as reported from the log source itself.
event_duration	uint32	The length/duration of the event in seconds (for example, 1 min is 60.0).
event_end_time	uint32	The time in which the event ended.
event_error	string	Information about an error.
event_error_code	uint32	Integer that defines a particular error.
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_report_url	string	URL of the full analysis report.
event_resource_group	string	The resource group to which the device generating the record belongs. This might be an AWS account, or an Azure subscription or Resource Group.
event_resource_id	string	The resource ID of the device generating the message.
event_severity	string	Event severity.
event_source	string	Data\Event source on Application layer.
event_start_time	uint32	The time in which the event stated.
event_status	string	Defines the status of a particular event.
event_status_code	uint32	Integer that defines a particular status.
event_subtype	string	Event subtype.
event_type	string	Event type.
event_uuid	string	Original unique ID specific to the log/event assigned to the event (not original).
event_vendor	string	The vendor of the product generating the event.

File

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

Logon

Normalized fabric log field	Type	Description
logon_authentication	string	The name of the authentication package which was used for the logon authentication process.

Normalized fabric log field	Type	Description
logon_device_claims	string	Logon device claims.
logon_guid	string	Logon GUID.
logon_id	string	Logon ID.
logon_server	string	Logon server name (it is a free text). The server name of the URL.
logon_srcip	ip	Logon remote IP. It could be user's IP, and a remote IP.
logon_transmitted_services	string	The list of transmitted services.
logon_type	string	Logon type.
logon_user_claims	string	Logon user claims.
logon_virtual_account	string	Logon virtual account information.

Network

Normalized fabric log field	Type	Description
net_direction	string	Network direction.
net_name	string	Network name.
net_payloadid	uint32	Network payload ID.
net_pktlosspct	string	The package loss percentage info.
net_proto	string	Network protocol.
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.

Process

Normalized fabric log field	Type	Description
process_call_trace	string	Stack trace of where open process is called.
process_command_line	string	Command arguments that were were executed by the process in the endpoint.
process_company	string	Process company information.

Normalized fabric log field	Type	Description
process_guid	string	Process global unique identifer used to identify a process across other operating systems.
process_hash	string	Process hash value.
process_hash_type	string	Process hash type.
process_id	uint32	Process ID.
process_injected_address	string	The memory address where the subprocess is injected.
process_integrity_level	string	Process integrity level.
process_name	string	Process name.
process_parent_name	string	Process parent name.
process_status	string	Process hidden or other status information.

Protocol

Normalized fabric log field	Type	Description
dns_additional_name	string	DNS additional name.
dns_query	string	DNS query data.
dns_query_class	string	DNS query class.
dns_querytype	string	DNS query type.
dns_rejected	string	The server responded to the query but no answers were given.
dns_response	string	DNS response data.
dns_rtt	uint32	Round trip time (RTT) of the DNS query to answer.
dns_server	string	DNS server name.
dns_transaction_id	string	Hexadecimal identifier assigned by the program that generated the DNS query.
http_cookie	string	HTTP cookie.
http_method	string	HTTP method.
http_referer	string	HTTP referer.
http_response_body	string	The raw HTTP (response) body.
http_response_time	uint32	The amount of time in milliseconds it took to receive a response in the server.
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.

Normalized fabric log field	Type	Description
http_status_message	string	HTTP server reply message.
http_url	string	HTTP URL.
http_useragent	string	HTTP user agent.
http_version	string	HTTP request version.
mail_attachment	string	Mail attachment.
mail_from	string	Mail from.
mail_size	uint32	Mail size.
mail_subject	string	Mail subject.
mail_to	string	Mail to.

Registry

Normalized fabric log field	Type	Description
registry_hive_path	string	A hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when the operating system is started or a user logs in.
registry_key_access_rights	string	The Windows security model enables you to control access to registry keys. The valid access rights for registry keys.
registry_key_name	string	This field contains the key name without the full path. Take in consideration the name of the key value in the registry key path.
registry_key_path	string	Next-level down from registry root-keys. This field contains the full path of a registry key.
registry_root_key	string	Root-Keys are the root, or primary divisions, of the registry. They do not contain configuration data; they contain the keys, subkeys, and values in which the data is stored.
registry_value_data	string	Each registry key value consists of a value name and its associated data. Registry key value data store the actual configuration data for the operating system and the programs that run on the system.
registry_value_name	string	Registry values are the lowest-level element in the registry. They appear in the right pane of the registry editor window.

Source

Normalized fabric log field	Type	Description
src_asset_id	string	Source asset id.

Normalized fabric log field	Type	Description
src_domain	string	Source domain.
src_geo	string	Source geo.
src_geo_city	string	Source geo city information.
src_geo_country	string	Source geo country.
src_geo_country_code	string	Source geo country code.
src_geo_latitude	string	Source geo latitude.
src_geo_longitude	string	Source geo longitude.
src_geo_region	string	Source geo region.
src_intf	string	Source interface.
src_intf_guid	string	GUID of the network interface which was used for authentication request.
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.

TLS

Normalized fabric log field	Type	Description
tls_cipher	string	The cipher (encryption) parameters used to make the TLS connection.
tls_curve	string	Elliptic curve the server chose when using ECDH/ECDHE.
tls_established	string	Indicates if the session has been established successfully, or if it was aborted during the handshake.
tls_next_protocol	string	Next protocol the server chose using the application layer next protocol extension, if present.
tls_resumed	string	If the session was resumed from previous established connection.
tls_server_name	string	The name of the requested server/destination; this should be copied to dst_host_name.
tls_version	string	Version of TLS/SSL used (SSLv3.0, TLSv1.1, TLSv1.2, or TLSv1.3).

Threat

Normalized fabric log field	Type	Description
threat_action	string	Threat action.
threat_category	string	Threat category provided by the alert.
threat_direction	string	Threat direction.
threat_id	string	Threat ID.
threat_message	string	Threat message provided by the alert.
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.
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
slot	data_sourcenode
data_sourcetype	data_sourcetype
vd	data_sourcevdom
data_timestamp	data_timestamp
accessctrl,accessproxy	app_access
appact	app_action
appcat	app_cat
keyword,sensitivity	app_data
appid	app_id
app,appname,apps,saasapp	app_name
moscodec	app_proc
hash,id,name,type	app_risk
service,saasinfo	app_service
apstatus	app_state
fctver	app_ver
cloudaction	cloud_appaction
saasname	cloud_appname
used	dhcp_used
qname	dns_query

FortiGate Log Field	Normalized Fabric Log Field
dns_querytype	dns_querytype
ipaddr	dns_response
dstssid,dstuuid	dst_asset_id
domain	dst_domain
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dst_info,dstintf	dst_intf
dstintfrole	dst_intf_role
dstip,dst_ip,locip	dst_ip
dstmac	dst_mac
dst_natip,tranip	dst_natip
dst_natport,tranport	dst_natport
dstport,dst_port	dst_port
action,utmaction	event_action
catdesc,videocategoryname,activitycategory,cat,catdesc,category,utmevent	event_cat
total	event_count
eventtime,time	event_creation_time
event_id,logid,vwlid	event_id
event_message,dhcp_msg,msg	event_message
name,logdesc	event_name
error,result	event_

FortiGate Log Field	Normalized Fabric Log Field
	outcome
event_policy,policyname,usingpolicy	event_policy
policyid	event_policyid
policytype	event_policytype
applist,profile	event_profile
event_ref,reason	event_ref
ap,sn	event_resource_id
fsaverdict,level,severity	event_severity
vap,channel	event_source
scantime	event_start_time
quarskip,status	event_status
state	event_status_code
subtype	event_subtype
type,eventtype,kind	event_type
cfgtid,logid,poluuid,uid	event_uuid
manuf	event_vendor
filetype	file_ext
analyticscksum,filehash	file_hash
filename,file	file_name
filesize	file_size
host_classification	host_

FortiGate Log Field	Normalized Fabric Log Field
	classification
sn,tags,vendorurl	host_data
host_hwvendor,srchwvendor	host_hwvendor
host_hwver,srchwversion	host_hwver
host_ip,deviceip	host_ip
srccountry	host_location
host_mac,mac,devicemac,bssid	host_mac
module,srcproduct	host_model_name
srcname	host_name
srcfamily,os	host_osfamily
host_osname,osname	host_osname
host_osver,srcswversion	host_osver
user,dstowner	host_owner
cpu,disk,mem	host_perf_stats
host_type	host_type
srcuuid,fctuid	host_uid
http_host	http_host
httpmethod,method	http_method
referralurl	http_referer
url	http_url
agent	http_useragent
ui	logon_ui

FortiGate Log Field	Normalized Fabric Log Field
messageid	mail_messageid
to	mail_to
apn,name,onwire,radioband,sn	net_accesspoint
direction	net_direction
srcssid	net_name
bandwidth,erate,orate,setuprate,totalsession,trate	net_perf_stats
packetloss	net_pktlosspct
proto	net_proto
rcvdpkt,rcvdp	net_rcvdpkts
rcvdbyte,rcvdb,inbandwidthused	net_recvbytes
rcvddelta	net_recvdelta
ip,name	net_remote_server
bibandwidthused,downbandwidthmeasured,healthcheck,jitter,latency,moscodec,mosvalue,speedtestserver,upbandwidthmeasured,vwlid	net_sdwan
sentbyte,sentb,outbandwidthused,rate	net_sentbytes
sentdelta	net_sentdelta
sentpkt,sentp	net_sentpkts
duration,dur	net_sessionduration
sessionid	net_sessionid

FortiGate Log Field	Normalized Fabric Log Field
shaperdroprcvdbyte,shaperdropsentbyte,shaperperipdropbyte,shaperperipname,shaperrcvdname,shapingpolicyid,shapingpolicyname	net_shaper
srcssid,ssid	net_ssid
id,ip,type,vpn,vpntype	net_tunnel
u-bytes,u-pkts	net_userdata
rsrq,rssi,security,securitymode,signal,sinr,sn	net_wlan
pid	process_id
srcssid	src_asset_id
srcname	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
source_info,srcintf,interface	src_intf
srcintfrole	src_intf_role
srcip,src_ip	src_ip
srcmac,stamac	src_mac
src_natip,transip	src_natip
src_natport,transport	src_natport
srcport,src_port	src_port
threat_action	threat_action
vulncat	threat_category
threatcnts	threat_count
cveid	threat_cveid
threat_direction	threat_

FortiGate Log Field	Normalized Fabric Log Field
	direction
threat_id	threat_id
category,infoid,name,scantime,score,wfcatid	threat_ioc
threat_name	threat_name
threat_pattern	threat_pattern
threat_ref	threat_ref
crscore	threat_score
threat_severity	threat_severity
threat_type	threat_type
id,name,severity,type,weight	threat_rawlog
community	user_classification
collectedemail	user_email
group,unauthusersource	user_group
user,unauthuser	user_id
user,initiator	user_name
role	user_role
unauthuser	user_unauthuser
xauthgroup	user_xauthgroup
xauthuser	user_xauthuser

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
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
script	app_ref
service	app_service
state	app_state
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
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
start_time	event_start_time
end_time	event_end_time
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

FortiManager Log Field	Normalized Fabric Log Field
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
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

FortiClient Log Field	Normalized Fabric Log Field
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	app_ver
remotename	dst_domain
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
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
usingpolicy,policyname	event_policy
ruleid	event_policyid
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
device_ip,regip	host_ip
site	host_location
devicemac,mac	host_mac

FortiClient Log Field	Normalized Fabric Log Field
hostname,device_name	host_name
os	host_osname
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
sessionid	net_sessionid
processname	process_name
domain	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcip	src_ip
devicemac,mac	src_mac
srcport	src_port
detectedpath	target_file_path
vulncat	threat_category
threat_action	threat_action
vulnid	threat_id
threat_name,vulnname	threat_name
threat_pattern	threat_pattern
vulnref	threat_ref
vulnseverity	threat_severity
threat_type	threat_type
social_srvc	user_authtype
domain	user_domain

FortiClient Log Field	Normalized Fabric Log Field
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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstip	dst_ip
dstport	dst_port
concat_eventaction,snmpaction	event_action
etime	event_creation_time

FortiSandbox Log Field	Normalized Fabric Log Field
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
host_osname	host_osname
host_osver	host_osver
host_type	host_type
url	http_url
emlsndr	mail_from
subject	mail_subject
emlrcvr	mail_to
proto	net_proto
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcip	src_ip
srcport	src_port

FortiSandbox Log Field	Normalized Fabric Log Field
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
event_time	event_creation_time
msg	event_message
event_subtype	event_subtype
event_type	event_type
scan_time	event_start_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

EMS-Connector Log Field	Normalized Fabric Log Field
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
data_timestamp	data_timestamp
dm_appid	app_id
service	app_service
dns_req	dns_query
dns_resp	dns_response
dst	dst_domain
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dst_port	dst_port
action	event_action
duration	event_duration
msg_id	event_id
msg	event_message

FortiADC Log Field	Normalized Fabric Log Field
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
dm_orihost	host_name
http_cookie	http_cookie
http_host	http_host
http_method	http_method
http_referer	http_referer
http_retcode	http_status_code
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
ibytes	net_recvbytes
obytes	net_sentbytes
dm_sessionid	net_sessionid
src	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
src_port	src_port
threat_action	threat_action

FortiADC Log Field	Normalized Fabric Log Field
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
service	app_service
state	app_state
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
action,event_action	event_action
event_id	event_id

FortiAnalyzer Log Field	Normalized Fabric Log Field
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
start_time	event_start_time
end_time	event_end_time
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
remote_ip	src_ip
remote_port	src_port

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

FortiAP logs

FortiAnalyzer supports normalizing FortiAP logs as Fabric logs.

The following field mapping applies:

FortiAP Log Field	Normalized Fabric Log Field
devid	data_sourceid
devname	data_sourcename
data_sourcetype	data_sourcetype
vd	data_sourcevdom
data_timestamp,eventtime	data_timestamp
appcat	app_cat
appid	app_id
app	app_name
name	app_risk
hostname	dst_domain
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstip	dst_ip
dstport	dst_port
action	event_action
catdesc	event_cat
eventtime	event_creation_time

FortiAP Log Field	Normalized Fabric Log Field
logid	event_id
msg	event_message
level	event_severity
subtype	event_subtype
eventtype	event_tags
type	event_type
sn,tags	host_data
hostname	host_name
url	http_url
direction	net_direction
proto	net_proto
sessionid	net_sessionid
ssid	net_ssid
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcip	src_ip
srcport	src_port

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
app_service	app_service
status	app_state

FortiAuthenticator Log Field	Normalized Fabric Log Field
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
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
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
userip	src_ip
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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
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
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
sentpkt	net_sentpkts

FortiCache Log Field	Normalized Fabric Log Field
duration	net_sessionduration
sessionid	net_sessionid
srcssid	net_ssid
src_int	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
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

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

FortiCASB Log Field	Normalized Fabric Log Field
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
eventtype	event_cat
policytype,policymode	event_policy
poluuid	event_profile
severity	event_severity
subtype	event_subtype
type	event_type
eventtime	event_creation_time
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
to	mail_to
sentbyte	net_sentbytes
rcvdbyte	net_sentpkts
sessionid	net_sessionid
srcdomain	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcip	src_ip
user	user_id

FortiClient Forwarded Linux logs

FortiAnalyzer supports normalizing FortiClient Forwarded Linux logs as Fabric logs.

The following field mapping applies:

FortiClient Forwarded Linux Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
vd	data_sourcevdom
data_timestamp	data_timestamp
app_name	app_name
app_proc	app_proc
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dst_ip	dst_ip
event_action	event_action
event_cat	event_cat
event_error	event_error
message	event_message
event_outcome	event_outcome
event_profile	event_profile
msg	event_rawmsg
event_severity	event_severity
tag	event_source
event_tags	event_tags
event_type	event_type
file_path	file_path
host_mac	host_mac
host_name,hostname	host_name
host_osfamily	host_osfamily
host_osname	host_osname

FortiClient Forwarded Linux Log Field	Normalized Fabric Log Field
net_recvbytes	net_recvbytes
net_sentbytes	net_sentbytes
process_call_trace	process_call_trace
pid	process_id
process_name	process_name
src_domain	src_domain
src_intf	src_intf
src_ip	src_ip
src_port	src_port
user_authtype	user_authtype
user_domain	user_domain
user_group	user_group
user_id	user_id
user	user_name

FortiCNAPP FEC logs

FortiAnalyzer supports normalizing FortiCNAPP FEC logs as Fabric logs.

The following field mapping applies:

FortiCNAPP FEC Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourceuuid	data_sourceuuid
data_sourcetags	data_sourcetags
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
dst_ip	dst_ip
event_id	event_id
event_message	event_message
event_name	event_name

FortiCNAPP FEC Log Field	Normalized Fabric Log Field
event_policy	event_policy
event_policyid	event_policyid
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_subtype	event_subtype
msg_tag	event_tags
event_type	event_type
file_hash	file_hash
file_path	file_path
host_ip	host_ip
host_name	host_name
http_method	http_method
http_url	http_url
src_ip	src_ip
user_name	user_name

FortiData logs

FortiAnalyzer supports normalizing FortiData logs as Fabric logs.

The following field mapping applies:

FortiData Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourceuuid	data_sourceuuid
data_sourcetags	data_sourcetags
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
event_action	event_action

FortiData Log Field	Normalized Fabric Log Field
event_cat	event_cat
event_creation_time	event_creation_time
event_message	event_message
event_name	event_name
event_policy	event_policy
event_profile	event_profile
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_status	event_status
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
file_name	file_name
file_path	file_path
file_size	file_size
name,email	file_owner
storage_type,storage_name,storage_notes	file_scan
file_labels	file_labels
file_uuid	file_uuid
incident_id	incident_id
user_email	user_email
user_name	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
data_sourcetype	data_sourcetype
dtime	data_timestamp
status	app_state
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
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
subnet_name	net_name
srcgeoid	src_geo

FortiDDoS Log Field	Normalized Fabric Log Field
srccity	src_geo_city
srccountry	src_geo_country
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
fdc_id	data_sourceuuid
devid	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,dtime	data_timestamp
data_version	data_version
service	app_service
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
victimip	dst_ip
victimmac	dst_mac
victimport	dst_port
action	event_action
event_cat	event_cat

FortiDeceptor Log Field	Normalized Fabric Log Field
eventid	event_id
event_message,msg	event_message
status	event_outcome
msg_body	event_rawmsg
status	event_status
event_severity,level	event_severity
event_source	event_source
subtype	event_subtype
type	event_type
event_uuid	event_uuid
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
fctuid	host_uid
incident_id	incident_id
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
attackerip	src_ip
attackermac	src_mac
attackerport	src_port
botnetname,attackname	threat_name
user	user_id
username	user_name

FortiDLP FEC logs

FortiAnalyzer supports normalizing FortiDLP FEC logs as Fabric logs.

The following field mapping applies:

FortiDLP FEC Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourceuuid	data_sourceuuid
data_sourcetags	data_sourcetags
data_sourcename	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp,itime	data_timestamp
app_name	app_name
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dst_ip	dst_ip
dst_port	dst_port
event_message	event_message
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
file_name	file_name
file_path	file_path
file_printer_type	file_printer_type
file_printer_uuid	file_printer_uuid
file_size	file_size
host_name	host_name
host_uid	host_uid

FortiDLP FEC Log Field	Normalized Fabric Log Field
http_url	http_url
mail_from	mail_from
mail_to	mail_to
process_command_line	process_command_line
process_guid	process_guid
process_name	process_name
process_owner	process_owner
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
src_ip	src_ip
src_port	src_port
target_file_name	target_file_name
target_file_path	target_file_path
threat_score	threat_score
user_id	user_id
user_name	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
data_sourcename,devid	data_sourcename
data_sourcetags	data_sourcetags
data_sourcetype	data_sourcetype
vd	data_sourcevdom
data_timestamp,dtime	data_timestamp
component_type	app_cat

FortiEDR Log Field	Normalized Fabric Log Field
data_id	app_id
component_name	app_name
autonomous_system	app_ref
device_state	app_state
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dst_ip	dst_ip
action,event_action	event_action
classification	event_cat
event_count	event_count
event_id	event_id
event_message	event_message
event_outcome	event_outcome
event_policy,rules_list	event_policy
msg	event_rawmsg
event_ref	event_ref
severity	event_severity
classification	event_subtype
event_tags	event_tags
event_type	event_type
event_first_seen_time	event_first_seen_time
event_last_seen_time	event_last_seen_time
last_seen	file_accessetime
first_seen	file_createtime
process_hash,file_hash	file_hash
script,remediation_files	file_name
script_path,file_path	file_path
file_size	file_size
source_ip,host_ip	host_ip

FortiEDR Log Field	Normalized Fabric Log Field
mac_address	host_mac
device_name	host_name
operating_system	host_osname
host_uid	host_uid
remote_connection	http_method
process_path	process_call_trace
process_command_line,command_line	process_command_line
process_hash	process_hash
process_name	process_name
process_parent_name	process_parent_name
process_type	process_type
process_owner	process_owner
organization	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry,country	src_geo_country
source_ip	src_ip
action	threat_action
threat_category	threat_category
siem_threat_name,threat_name	threat_name
siem_threat_pattern	threat_pattern
siem_threat_type,threat_type	threat_type
user_group	user_group
users	user_id
user_name,process_owner	user_name
user_org	user_org

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
appact	app_action
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
dns_ip	dns_server
dstname	dst_domain
dstssid	dst_asset_id
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry,dst_country	dst_geo_country
dstregion	dst_geo_region
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

FortiFirewall Log Field	Normalized Fabric Log Field
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
sessionid,SN	net_sessionid
ssid	net_ssid
srcssid	src_asset_id
srcname,srcdomain	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry,src_country	src_geo_country

FortiFirewall Log Field	Normalized Fabric Log Field
srcregion	src_geo_region
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

FortiGate Security Rating logs

FortiAnalyzer supports normalizing FortiGate Security Rating logs as Fabric logs.

The following field mapping applies:

FortiGate Security Rating Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
devname,data_sourceid	data_sourcename
data_sourcetype	data_sourcetype
data_sourcevdom	data_sourcevdom
data_sourceversion	data_sourceversion
data_timestamp,itime	data_timestamp
msg_cat	event_cat
event_id	event_id
event_message	event_message
event_name	event_name
event_outcome	event_outcome
event_policy	event_policy

FortiGate Security Rating Log Field	Normalized Fabric Log Field
msg	event_rawmsg
event_ref	event_ref
event_severity	event_severity
event_source	event_source
event_subtype	event_subtype
msg_tag	event_tags
event_type	event_type
session_id	net_sessionid

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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
avaction,wfaction	event_action
eventtime	event_creation_time
msg	event_message
avresult	event_outcome
avblockreason	event_policy
avengine,wfprofile,icapprofile,iprofile,clicmd	event_profile

FortiIsolator Log Field	Normalized Fabric Log Field
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
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
vd	data_sourcevdom
data_timestamp,dtime	data_timestamp
dst_domain	dst_domain
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dst_ip	dst_ip

FortiMail Log Field	Normalized Fabric Log Field
concat_eventaction,action	event_action
classifier	event_cat
eventtime	event_creation_time
scan_time	event_duration
event_error	event_error
event_error_code	event_error_code
logid,log_id	event_id
msg	event_message
event_name	event_name
disposition	event_outcome
polid	event_policyid
reason	event_ref
pri	event_severity
status	event_status
event_status_code	event_status_code
subtype	event_subtype
type	event_type
file_hash,checksum	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
url	http_url
ui	logon_ui
endpoint,header_from,mailer,resolved,source_	mail_data

FortiMail Log Field	Normalized Fabric Log Field
type,source_folder,cat_id	
message_id	mail_messageid
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry,location	src_geo_country
client_cc	src_geo_country_code
client_ip	src_ip
threat_name	threat_name
threat_pattern	threat_pattern
score	threat_score
id,name,signature	threat_rawlog
domain,domain_name	user_domain
user	user_id
user_name	user_name

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

FortiNAC Log Field	Normalized Fabric Log Field
dtime	data_timestamp
sn	app_name
agentplat	app_service
mailstate	app_state
agentver,fwver	app_ver
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
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
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
srcgeoid	src_geo
srccity	src_geo_city

FortiNAC Log Field	Normalized Fabric Log Field
srccountry	src_geo_country
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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
action	event_action
eventtime	event_creation_time
logid	event_id
level	event_severity

FortiNDR Log Field	Normalized Fabric Log Field
devicetype	event_source
subtype	event_subtype
type	event_type
filetype	file_ext
file_hash	file_hash
file_hashtype	file_hashtype
fileid	file_name
filesize	file_size
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
fossn	src_asset_id
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
victimip	src_ip
victimport	src_port
malwarefamily	threat_category
virusname,vname	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
appact	app_action
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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstregion	dst_geo_region
dst_info	dst_intf
dstip	dst_ip
dstmac	dst_mac
tranip	dst_natip
tranport	dst_natport
dstport,dst_port	dst_port
action	event_action
eventtime	event_creation_time
logid,log_id	event_id

FortiPAM Log Field	Normalized Fabric Log Field
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
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

FortiPAM Log Field	Normalized Fabric Log Field
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcregion	src_geo_region
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
appact	app_action
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
dstssid	dst_asset_id
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstregion	dst_geo_region
dst_info	dst_intf
dstip	dst_ip
dstmac	dst_mac
tranip	dst_natip
tranport	dst_natport
dstport,dst_port	dst_port
action	event_action
eventtime	event_creation_time

FortiProxy Log Field	Normalized Fabric Log Field
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
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

FortiProxy Log Field	Normalized Fabric Log Field
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcregion	src_geo_region
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

FortiSIEM Forwarded Linux logs

FortiAnalyzer supports normalizing FortiSIEM Forwarded Linux logs as Fabric logs.

The following field mapping applies:

FortiSIEM Forwarded Linux Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename,devname	data_sourcename
data_sourcetype	data_sourcetype
data_timestamp	data_timestamp
event_action	event_action
msg_body	event_message
event_name	event_name
event_tags	event_tags
event_type	event_type
file_name	file_name
host_ip	host_ip
host_name	host_name
host_osfamily	host_osfamily
user_group	user_group
user	user_name

FortiSIEM Forwarded Windows logs

FortiAnalyzer supports normalizing FortiSIEM Forwarded Windows logs as Fabric logs.

The following field mapping applies:

FortiSIEM Forwarded Windows Log Field	Normalized Fabric Log Field
devid	data_sourceid
data_sourcename,devname	data_sourcename
data_sourcetype	data_sourcetype
data_sourceuuid	data_sourceuuid

FortiSIEM Forwarded Windows Log Field	Normalized Fabric Log Field
data_timestamp	data_timestamp
dst_ip	dst_ip
dst_port	dst_port
event_action,sys_keywords	event_action
event_creation_time	event_creation_time
event_id	event_id
event_uuid	event_uuid
event_message	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	event_subtype
event_type,channel	event_type
event_source	event_source
event_name	event_name
msg_body	event_rawmsg
event_tags	event_tags
event_cat	event_cat
file_name	file_name
host_ip	host_ip
computer,host_name	host_name
host_osfamily	host_osfamily
http_method	http_method
http_referer	http_referer
http_status_code	http_status_code
http_useragent	http_useragent
logon_authentication	logon_authentication
logon_id	logon_id
event_data_subj_user_name	logon_user_claims

FortiSIEM Forwarded Windows Log Field	Normalized Fabric Log Field
process_name	process_name
parent_process_name	process_parent_name
src_ip	src_ip
src_port	src_port
user_domain,user_account_domain	user_domain
user_group	user_group
user_id	user_id
user_name,user,user_account	user_name

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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
event_id	event_id
event_message	event_message
event_profile	event_profile
event_severity	event_severity
event_subtype	event_subtype
event_type	event_type

FortiSOAR Log Field	Normalized Fabric Log Field
host_classification	host_classification
host_name	host_name
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
src_ip	src_ip
user_id	user_id
user_name	user_name

FortiSRA logs

FortiAnalyzer supports normalizing FortiSRA logs as Fabric logs.

The following field mapping applies:

FortiSRA Log Field	Normalized Fabric Log Field
devid,device_id	data_sourceid
data_source_name	data_sourcename
data_sourcetype	data_sourcetype
dtime	data_timestamp
appact	app_action
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
dstgeoid	dst_geo
dstcity	dst_geo_city

FortiSRA Log Field	Normalized Fabric Log Field
dstcountry	dst_geo_country
dstregion	dst_geo_region
dst_info	dst_intf
dstip	dst_ip
dstmac	dst_mac
tranip	dst_natip
tranport	dst_natport
dstport,dst_port	dst_port
action	event_action
eventtime	event_creation_time
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
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

FortiSRA Log Field	Normalized Fabric Log Field
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
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcregion	src_geo_region
src_info	src_intf
srcip	src_ip
srcmac,source_mac	src_mac
transip	src_natip
transport	src_natport
srcport,src_port	src_port

FortiSRA Log Field	Normalized Fabric Log Field
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

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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstip	dst_ip
action	event_action
logid,log_id	event_id
msg	event_message
status	event_outcome
profile,reason	event_profile

FortiSwitch Log Field	Normalized Fabric Log Field
level,pri	event_severity
subtype	event_subtype
type	event_type
ui	http_url
mirror-session	net_sessionid
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
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
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
action	event_action
event_time	event_creation_time
response	event_message
result	event_outcome

FortiToken Log Field	Normalized Fabric Log Field
resource	event_profile
event_ref	event_ref
subtype	event_subtype
type	event_type
customer_id	src_asset_id
source_device	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry,location	src_geo_country
user_ip	src_ip
realm_id	user_domain
account_id	user_id
username	user_name
mobile_number	user_social

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
app_id	app_id
app_name	app_name
service,backend_service,server_pool_name	app_service
app_domain	dst_domain
dst_city_country	dst_geo
dstcountry	dst_geo_country

FortiWeb Log Field	Normalized Fabric Log Field
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,policy_name	event_policy
reason	event_ref
pri,severity_level	event_severity
subtype,sub_type	event_subtype
type,main_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
http_host	http_host
http_method	http_method
http_refer	http_referer
http_response_time	http_response_time
http_retcode	http_status_code
http_url	http_url
http_agent	http_useragent
http_version	http_version
proto	net_proto

FortiWeb Log Field	Normalized Fabric Log Field
http_session_id	net_sessionid
srcgeoid	src_geo
srccity	src_geo_city
srccountry,original_srccountry	src_geo_country
ui	src_intf
src,src_ip	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_id,account_id	user_id
user_name,login_user,user	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
pid	app_proc
service	app_service
message	event_message

Apache Log Field	Normalized Fabric Log Field
eventSeverity	event_severity
event_tags	event_tags
event_type	event_type
file_name	file_name
host_ip	host_ip
host_name	host_name
http_method	http_method
http_referer	http_referer
http_request_bytes	http_request_bytes
http_url	http_url
http_useragent	http_useragent
http_version	http_version
procId	process_id
procName	process_name
srcIpAddr	src_ip
srcIpPort	src_port
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

Nginx Log Field	Normalized Fabric Log Field
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
version	app_ver
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstip	dst_ip
event_cat	event_cat
message,cleaned_msg,msg	event_message
level	event_severity
type	event_type
event_uuid	event_uuid
vendor	event_vendor
host_classification	host_classification
host_hwvendor	host_hwvendor

System Log Field	Normalized Fabric Log Field
host_hwver	host_hwver
host_ip	host_ip
host_mac	host_mac
product	host_model_name
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
srcip	src_ip

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

Ubuntu Log Field	Normalized Fabric Log Field
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

VMware logs

FortiAnalyzer supports normalizing VMware logs as Fabric logs.

The following field mapping applies:

VMware Log Field	Normalized Fabric Log Field
data_sourceid	data_sourceid
data_sourcetype	data_sourcetype
data_sourceversion	data_sourceversion
data_timestamp,itime	data_timestamp
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country

VMware Log Field	Normalized Fabric Log Field
dstip,destIpAddr	dst_ip
eventAction	event_action
event_cat	event_cat
event_message,vmwEventMsg	event_message
event_outcome	event_outcome
msg,msg_body	event_rawmsg
event_severity	event_severity
event_source	event_source
event_subtype	event_subtype
event_tags	event_tags
event_type	event_type
event_uuid	event_uuid
event_vendor	event_vendor
host_hwvendor	host_hwvendor
host_hwver	host_hwver
host_ip,hostIpAddr	host_ip
product	host_model_name
host_name	host_name
host_osname	host_osname
host_osver	host_osver
host_type	host_type
host_uid	host_uid
http_useragent	http_useragent
net_sessionid	net_sessionid
process_id	process_id
procName	process_name
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country
host_ip,srcIpAddr	src_ip

VMware Log Field	Normalized Fabric Log Field
srcIpPort	src_port
userGrp	user_group
user_name,user	user_name

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_sourcetags	data_sourcetags
data_timestamp	data_timestamp
app_cat,channel	app_cat
app_name,provider_name	app_name
execution_pid,pid	app_proc
app_ref	app_ref
version	app_ver
domain_name	dst_domain
dstgeoid	dst_geo
dstcity	dst_geo_city
dstcountry	dst_geo_country
dstip	dst_ip
sys_keywords	event_action
event_id	event_id

Windows Event Log Field	Normalized Fabric Log Field
event_log,exch_log,event_json,event_msg	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
event_source,provider_name	event_source
msg	event_rawmsg
event_tags	event_tags
host_ip	host_ip
host_name	host_name
os_family	host_osfamily
host_uid	host_uid
logon_authentication	logon_authentication
logon_id	logon_id
event_data_subj_user_name	logon_user_claims
mail_from	mail_from
mail_subject	mail_subject
net_direction	net_direction
net_proto	net_proto
net_sentbytes	net_sentbytes
process_id	process_id
process_name	process_name
parent_process_name	process_parent_name
process_status	process_status
src_domain	src_domain
srcgeoid	src_geo
srccity	src_geo_city
srccountry	src_geo_country

Windows Event Log Field	Normalized Fabric Log Field
srcip,src_ip	src_ip
user_domain	user_domain
user_group	user_group
user_id	user_id
user_name	user_name

www.fortinet.com