

# Fabric Normalization Reference

**FortiAnalyzer 7.2.10**



**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](mailto:techdoc@fortinet.com)



February 12, 2025

FortiAnalyzer 7.2.10 Fabric Normalization Reference

00-7210-815638-20250212

# TABLE OF CONTENTS

|                                             |          |
|---------------------------------------------|----------|
| <b>Change Log</b>                           | <b>4</b> |
| <b>FortiAnalyzer normalized Fabric logs</b> | <b>5</b> |
| Fabric log field descriptions               | 5        |
| FortiGate logs                              | 10       |
| FortiManager/FortiAnalyzer logs             | 13       |
| FortiClient logs                            | 15       |
| FortiSandbox logs                           | 17       |
| FortiAuthenticator logs                     | 19       |
| FortiADC logs                               | 20       |
| FortiAI logs                                | 22       |
| FortiCache logs                             | 23       |
| FortiDeceptor logs                          | 26       |
| FortiDDoS logs                              | 27       |
| FortiEDR logs                               | 28       |
| FortiFirewall logs                          | 30       |
| FortiIsolator logs                          | 32       |
| FortiMail logs                              | 33       |
| FortiNAC logs                               | 35       |
| FortiProxy logs                             | 36       |
| FortiSOAR logs                              | 39       |
| FortiSwitch logs                            | 40       |
| FortiWeb logs                               | 41       |
| System logs                                 | 43       |
| Ubuntu logs                                 | 44       |
| Windows Event logs                          | 45       |

## Change Log

| Date       | Change Description |
|------------|--------------------|
| 2025-02-12 | Initial release.   |
|            |                    |
|            |                    |

# FortiAnalyzer normalized Fabric logs

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

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

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

## Fabric log field descriptions

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

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

The following tables list the available normalized fabric log fields in FortiAnalyzer 7.2.10.

**base**

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

**data\_source**

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

**Application**

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

**Destination**

| Normalized fabric log field | Type   | Description              |
|-----------------------------|--------|--------------------------|
| dst_domain                  | string | Destination domain name. |
| dst_geo                     | string | Destination geo.         |

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

## Event

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

## File

| Normalized fabric log field | Type   | Description         |
|-----------------------------|--------|---------------------|
| file_accesstime             | 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.     |

| Normalized fabric log field | Type   | Description |
|-----------------------------|--------|-------------|
| file_name                   | string | File name.  |
| file_path                   | string | File path.  |
| file_size                   | string | File size.  |

## Host

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

## Network

| Normalized fabric log field | Type   | Description                 |
|-----------------------------|--------|-----------------------------|
| net_direction               | string | Network direction.          |
| net_name                    | string | Network name.               |
| net_payloadid               | uint32 | Network payload ID.         |
| net_proto                   | string | Network protocol.           |
| net_rcvdpkts                | uint64 | Number of received packets. |
| net_rcvbytes                | uint64 | Received bytes.             |
| net_sentbytes               | uint64 | Sent bytes.                 |
| net_sentpkts                | uint64 | Number of sent packets.     |



| Normalized fabric log field | Type   | Description       |
|-----------------------------|--------|-------------------|
| net_sessionduration         | uint32 | Session duration. |
| net_sessionid               | string | Session ID.       |
| net_ssid                    | string | Network SSID.     |

## Protocol

| Normalized fabric log field | Type   | Description                |
|-----------------------------|--------|----------------------------|
| dns_query                   | string | DNS query data.            |
| dns_querytype               | string | DNS query type.            |
| dns_response                | string | DNS response data.         |
| http_cookie                 | string | HTTP cookie.               |
| http_method                 | string | HTTP method.               |
| http_referer                | string | HTTP referer.              |
| http_status_message         | string | HTTP server reply message. |
| http_url                    | string | HTTP URL.                  |
| http_useragent              | string | HTTP user agent.           |
| mail_from                   | string | Mail from.                 |
| mail_size                   | uint32 | Mail size.                 |
| mail_subject                | string | Mail subject.              |
| mail_to                     | string | Mail to.                   |

## Source

| Normalized fabric log field | Type   | Description       |
|-----------------------------|--------|-------------------|
| src_domain                  | string | Source domain.    |
| src_geo                     | string | Source geo.       |
| src_intf                    | string | Source interface. |
| src_ip                      | ip     | Source IP.        |
| src_mac                     | string | Source MAC        |
| src_natip                   | ip     | Source NAT IP.    |
| src_natport                 | uint16 | Source NAT port.  |
| src_port                    | uint16 | Source port.      |

## Threat

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

## User

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

## FortiGate logs

FortiAnalyzer supports normalizing FortiGate logs as Fabric logs.

The following field mapping applies:

| FortiGate Log Field  | Normalized Fabric Log Field |
|----------------------|-----------------------------|
| devid,device_id      | data_sourceid               |
| data_source_name     | data_sourcename             |
| data_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               |
| 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         |

| FortiGate Log Field   | Normalized Fabric Log Field |
|-----------------------|-----------------------------|
| 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                   |
| srcuid                | host_uid                    |
| referralurl           | http_referer                |
| url                   | http_url                    |
| srcssid               | net_name                    |
| proto                 | net_proto                   |
| rcvdpkt,rcvdp         | net_rcvdpkts                |
| rcvdbyte,rcvdb        | net_rcvbytes                |
| sentbyte,sentb        | net_sentbytes               |
| sentpkt,sentp         | net_sentpkts                |
| duration,dur          | net_sessionduration         |
| sessionid             | net_sessionid               |
| srcssid               | net_ssid                    |
| srcname               | src_domain                  |
| srccountry            | src_geo                     |
| source_info           | src_intf                    |
| srcip,src_ip          | src_ip                      |
| srcmac                | src_mac                     |
| src_natip,transip     | src_natip                   |
| src_natport,transport | src_natport                 |

| FortiGate Log Field    | Normalized Fabric Log Field |
|------------------------|-----------------------------|
| 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             |
| 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               |

| FortiManager/FortiAnalyzer Log Field | Normalized Fabric Log Field |
|--------------------------------------|-----------------------------|
| 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_hwwendor               |
| 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               |
| 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                |
| logid                                | event_id                    |
| msg,affected_prod_list               | event_message               |
| status,openfeatures                  | 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                   |

| FortiClient Log Field          | Normalized Fabric Log Field |
|--------------------------------|-----------------------------|
| 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               |
| 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             |



| FortiClient Log Field | Normalized Fabric Log Field |
|-----------------------|-----------------------------|
| 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               |
| 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                      |

| FortiSandbox Log Field        | Normalized Fabric Log Field |
|-------------------------------|-----------------------------|
| 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_hwwendor               |
| 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                   |
| 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                    |

| 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                     |

## 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              |
| 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               |

| FortiAuthenticator Log Field | Normalized Fabric Log Field |
|------------------------------|-----------------------------|
| 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               |
| 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                |

| FortiADC Log Field             | Normalized Fabric Log Field |
|--------------------------------|-----------------------------|
| msg_id                         | event_id                    |
| msg                            | event_message               |
| status                         | event_outcome               |
| policy                         | event_policy                |
| logdesc                        | event_profile               |
| cfgattr                        | event_ref                   |
| level,pri                      | event_severity              |
| subtype                        | event_subtype               |
| type                           | event_type                  |
| quar_file_name,smtp_attachname | file_name                   |
| http_host,dm_orihost           | host_name                   |
| http_cookie                    | http_cookie                 |
| http_method                    | http_method                 |
| http_referer                   | http_referer                |
| http_url                       | http_url                    |
| http_agent                     | http_useragent              |
| smtp_from                      | mail_from                   |
| smtp_bodylen                   | mail_size                   |
| smtp_subject                   | mail_subject                |
| smtp_to                        | mail_to                     |
| proto                          | net_proto                   |
| ibytes                         | net_rcvbytes                |
| 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                   |

| FortiADC Log Field | Normalized Fabric Log Field |
|--------------------|-----------------------------|
| 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              |
| status              | app_state                   |
| action              | event_action                |
| logid               | event_id                    |
| level               | event_severity              |
| subtype             | event_subtype               |
| type                | event_type                  |
| host_classification | host_classification         |
| host_hwvender       | host_hwvender               |
| host_hwver          | host_hwver                  |
| host_ip             | host_ip                     |
| host_mac            | host_mac                    |

| FortiAI Log Field | Normalized Fabric Log Field |
|-------------------|-----------------------------|
| 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                      |
| 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                   |

| FortiCache Log Field                | Normalized Fabric Log Field |
|-------------------------------------|-----------------------------|
| 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,message_type,message_type   | event_subtype               |
| type,eventtype                      | event_type                  |
| filetype,spam_file_type             | file_ext                    |
| checksum                            | file_hash                   |
| virus_file_hashtype                 | file_hashtype               |
| filename,spam_subject,filesize      | file_name                   |
| spam_file_size,filesize             | file_size                   |
| host_info,host_classification       | host_classification         |
| osgen,os_gen,osvendor,host_hwvendor | host_hwvendor               |
| host_hwver                          | host_hwver                  |
| ip,host_ip                          | host_ip                     |
| srccountry                          | host_location               |
| mastersrcmac,host_mac               | host_mac                    |
| hostname,host_name                  | host_name                   |
| osfamily                            | host_osfamily               |



| FortiCache Log Field   | Normalized Fabric Log Field |
|------------------------|-----------------------------|
| 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               |
| 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                    |

| FortiCache Log Field | Normalized Fabric Log Field |
|----------------------|-----------------------------|
| 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              |
| 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_hwvender           | host_hwvender               |

| FortiDeceptor Log Field | Normalized Fabric Log Field |
|-------------------------|-----------------------------|
| 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             |
| 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              |

| FortiDDoS Log Field | Normalized Fabric Log Field |
|---------------------|-----------------------------|
| 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               |

| FortiEDR Log Field                      | Normalized Fabric Log Field |
|-----------------------------------------|-----------------------------|
| device_name, devid                      | data_sourcename             |
| data_sourcetype                         | data_sourcetype             |
| data_timestamp                          | data_timestamp              |
| component_type                          | app_cat                     |
| data_id                                 | app_id                      |
| component_name                          | app_name                    |
| autonomous_system                       | app_ref                     |
| device_state                            | app_state                   |
| 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_name, script, remediation_files | file_name                   |
| process_path, script_path               | file_path                   |
| source_ip                               | host_ip                     |
| mac_address                             | host_mac                    |
| device_name                             | host_name                   |
| operating_system                        | host_osname                 |
| remote_connection                       | http_method                 |
| organization                            | src_domain                  |
| country                                 | src_geo                     |
| source_ip                               | src_ip                      |
| action                                  | threat_action               |

| FortiEDR Log Field  | Normalized Fabric Log Field |
|---------------------|-----------------------------|
| 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                   |
| dns_name                | dns_querytype               |
| dstname                 | dst_domain                  |
| dstcountry,dst_country  | dst_geo                     |
| dstintf,dst_intf        | dst_intf                    |
| dstip,dst               | dst_ip                      |
| dstmac                  | dst_mac                     |
| dstport,dst_port        | dst_port                    |

| FortiFirewall Log Field | Normalized Fabric Log Field |
|-------------------------|-----------------------------|
| 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                   |
| srchwvvendor            | host_hwvvendor              |
| 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_rcvbytes                |
| sentbyte,sent           | net_sentbytes               |
| sentpkt,sent_pkt        | net_sentpkts                |

| FortiFirewall Log Field                      | Normalized Fabric Log Field |
|----------------------------------------------|-----------------------------|
| 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                   |

## Fortisolator logs

FortiAnalyzer supports normalizing Fortisolator logs as Fabric logs.

The following field mapping applies:

| Fortisolator Log Field | Normalized Fabric Log Field |
|------------------------|-----------------------------|
| id, loguid             | loguid                      |
| epid                   | epid                        |
| euid                   | euid                        |
| devid                  | data_sourceid               |
| data_sourcename        | data_sourcename             |
| data_sourcetype        | data_sourcetype             |
| eventtime              | data_timestamp              |
| browsertype            | app_name                    |



| Fortisolator Log Field                            | Normalized Fabric Log Field |
|---------------------------------------------------|-----------------------------|
| pid                                               | app_proc                    |
| browserver                                        | app_ver                     |
| avaction, wfaction                                | event_action                |
| msg                                               | event_message               |
| avresult                                          | event_outcome               |
| avblockreason                                     | event_policy                |
| avengine, wfprofile, icaprofile, 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             |

| FortiMail Log Field            | Normalized Fabric Log Field |
|--------------------------------|-----------------------------|
| 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_hwvender                  | host_hwvender               |
| host_hwver                     | host_hwver                  |
| host_ip                        | host_ip                     |
| host_mac                       | host_mac                    |
| host_name                      | host_name                   |
| host_osname                    | host_osname                 |
| host_osver                     | host_osver                  |
| host_type                      | host_type                   |
| mail_from                      | mail_from                   |
| message_length                 | mail_size                   |
| subject                        | mail_subject                |
| to                             | mail_to                     |
| direction                      | net_direction               |
| session_id                     | net_sessionid               |
| client_name                    | src_domain                  |

| FortiMail Log Field | Normalized Fabric Log Field |
|---------------------|-----------------------------|
| 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                |
| msg                | event_message               |
| severity           | event_severity              |
| subtype            | event_subtype               |
| type               | event_type                  |
| lastactivitytime   | file_accessetime            |
| createtime         | file_createtime             |

| FortiNAC Log Field                 | Normalized Fabric Log Field |
|------------------------------------|-----------------------------|
| 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                   |
| transport            | dst_natport                 |
| dstport,dst_port     | dst_port                    |
| action               | event_action                |
| logid,log_id         | event_id                    |
| msg                  | event_message               |
| error                | event_outcome               |
| policyid             | event_policy                |
| applist              | event_profile               |
| level                | event_severity              |

| FortiProxy Log Field  | Normalized Fabric Log Field |
|-----------------------|-----------------------------|
| 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_hwwendor         | host_hwwendor               |
| host_hwver            | host_hwver                  |
| host_ip               | host_ip                     |
| mastersrcmac,host_mac | host_mac                    |
| srcname,host_name     | host_name                   |
| osname,host_osname    | host_osname                 |
| osversion,host_osver  | host_osver                  |
| devtype,host_type     | host_type                   |
| srcuuid               | host_uid                    |
| url                   | http_url                    |
| agent                 | http_useragent              |
| from                  | mail_from                   |
| size                  | mail_size                   |
| subject               | mail_subject                |
| to                    | mail_to                     |
| direction             | net_direction               |
| srcssid               | net_name                    |
| proto                 | net_proto                   |
| rcvdpkt               | net_rcvdpkts                |
| rcvdbyte              | net_rcvbytes                |
| sentbyte              | net_sentbytes               |
| sentpkt               | net_sentpkts                |

| FortiProxy Log Field      | Normalized Fabric Log Field |
|---------------------------|-----------------------------|
| 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             |
| threatype                 | 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                        |

| FortiSOAR Log Field | Normalized Fabric Log Field |
|---------------------|-----------------------------|
| 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                        |
| device_id,devid       | data_sourceid               |
| data_source_name      | data_sourcename             |



| FortiSwitch Log Field     | Normalized Fabric Log Field |
|---------------------------|-----------------------------|
| 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               |
| data_source_name   | data_sourcenname            |
| data_sourcetype    | data_sourcetype             |

| FortiWeb Log Field                       | Normalized Fabric Log Field |
|------------------------------------------|-----------------------------|
| 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_hwvender                            | host_hwvender               |
| 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                    |
| http_agent                               | http_useragent              |
| proto                                    | net_proto                   |

| FortiWeb Log Field             | Normalized Fabric Log Field |
|--------------------------------|-----------------------------|
| 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                    |
| host_name           | host_name                   |
| host_osname         | host_osname                 |

| System Log Field | Normalized Fabric Log Field |
|------------------|-----------------------------|
| host_osver       | host_osver                  |
| host_type        | host_type                   |
| host_uid         | host_uid                    |

## Ubuntu logs

FortiAnalyzer supports normalizing Ubuntu logs as Fabric logs.



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

The following field mapping applies:

| Ubuntu Log Field    | Normalized Fabric Log Field |
|---------------------|-----------------------------|
| 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_eventssubtype   | 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                 |

| Ubuntu Log Field | Normalized Fabric Log Field |
|------------------|-----------------------------|
| host_osver       | host_osver                  |
| host_type        | host_type                   |
| host_uid         | host_uid                    |
| ip               | src_ip                      |
| srcmac           | src_mac                     |

## Windows Event logs

FortiAnalyzer supports normalizing Windows Event logs as Fabric logs.



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

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

The following field mapping applies:

| Windows Event Log Field | Normalized Fabric Log Field |
|-------------------------|-----------------------------|
| 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                    |

| Windows Event Log Field     | Normalized Fabric Log Field |
|-----------------------------|-----------------------------|
| event_log                   | event_message               |
| event_data_return_code      | event_outcome               |
| event_record_id             | event_ref                   |
| level                       | event_severity              |
| provider_name               | event_subtype               |
| 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](http://www.fortinet.com)

---

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.