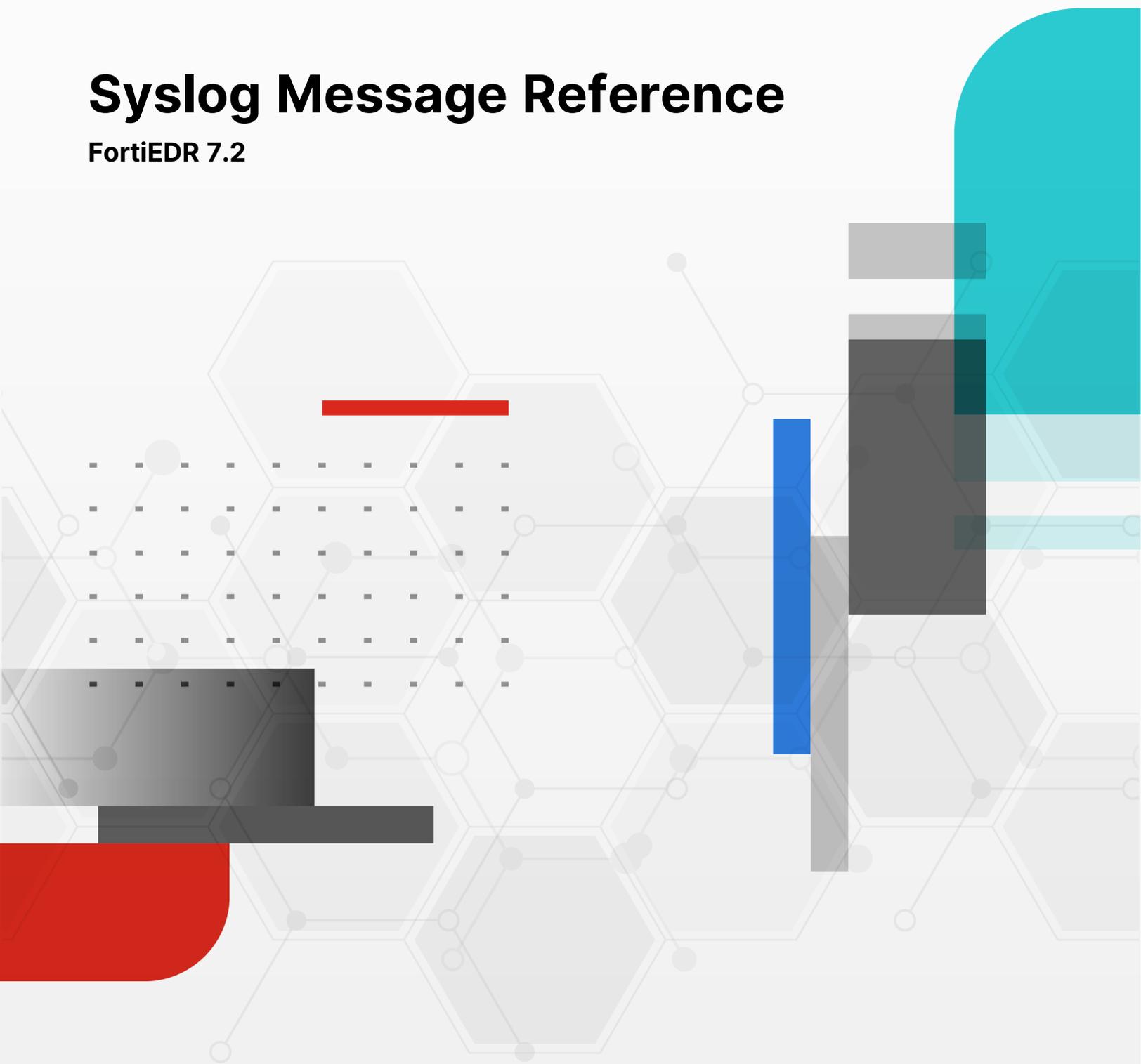


Syslog Message Reference

FortiEDR 7.2



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



October 10, 2025

FortiEDR 7.2 Syslog Message Reference

63-720-1214181-20251010

TABLE OF CONTENTS

Change log	4
Introduction	5
Syslog information	6
Syslog types	6
Syslog message format	6
FortiEDR syslog messages	7
Security event	7
System event	16
Audit trail	18

Change log

Date	Change Description
2025-10-10	Initial document release.

Introduction

This document provides information about all the syslog messages applicable to the FortiEDR 7.2. It provides administrators more information about specific syslog entries and messages.

For more information on configuring syslogs, see the [FortiEDR Administration Guide](#).

Syslog information

Syslog types

Each syslog message contains a Type (type) field that indicates its source.

Type	Description
Security event	FortiEDR security events.
System event	System events regarding FortiEDR deployment health.
Audit trail	Audit records of the FortiEDR console audit log.

Syslog message format

The FortiEDR syslog messages contain the following sections:

- **Facility Code:** All messages have the value 16 (Custom App).
- **Severity:** All messages have the value 5 (Notice).
- **MessageType:** Enables you to differentiate between syslog message categories – Security event, System event, or Audit trail.
- **Message Text:** Contains the name and value of all the selected fields.
For example, Device name: Laptop123. Each field is separated by a semi-colon (;).
- **Time:** Syslog events time in UTC format.

FortiEDR syslog messages

The following table shows the standard format that is used for each syslog type described in this document.

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Organization	Organization	cs1	cs1Label=Organization	Name of the organization the system event belongs to.	String	100
Event ID	EventId	eventid	—	Security event ID automatically generated by the FortiEDR Manager.	Integer	10

Custom fields in CEF format (such as *cs1*) should be sent with the matching CEF custom label value in order to define the display label for this custom field to the consumer system. The message then includes the following two fields:

1. CEF custom label value
2. CEF field name (such as *cs1*) that holds the actual value of the field

For example, for *Organization "Marketing"*, FortiEDR sends the following two CEF fields in the message: "*cs1Label=Organization*" and "*cs1=Marketing*".

The following sections list the FortiEDR 7.2 syslog messages.

- [Security event on page 7](#)
- [System event on page 16](#)
- [Audit trail on page 18](#)

Security event

The following table describes the fields in security events. The order that the fields are listed reflects the order of the fields in security event syslog messages.

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Organization	Organization	cs1	cs1Label=Organization	Name of the	String	100

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				organization the security event belongs to.		
Organization ID	OrganizationId	cs2	cs2Label=OrganizationId	ID of the organization.	Integer	10
Event ID	EventId	eventid	—	Security event ID automatically generated by the FortiEDR Manager.	Integer	10
Raw Data ID	RawDataId	cs6	cs6Label=RawDataId	Raw data ID of the security event, which is automatically generated by the FortiEDR Manager.	Integer	10
Device Name	Hostname	Shost	—	Protected device name.	String	1000
Device State	DeviceState	cs5	cs5Label=DeviceState	State of the device triggering the event. The state can be one of the following: <ul style="list-style-type: none"> Degraded Disabl 	String	25

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				<ul style="list-style-type: none"> • Disconnected • Running 		
Operating System	OS	cs3	cs3Label=OS	Protected device operating system.	String	100
Process Name	fname	fname	—	Name of the process triggering the event.	String	32000
Process Path	filePath	filePath	—	Path of the process triggering the event.	String	32000
Process Type	AppBitness	AppBitness	—	Bitness of the process: 32 or 64 bit.	String	5
Severity	sev	Severity	—	Severity of the event. Legacy field.	String	25
Classification	Classification	Classification	—	Security grade of the event. The grade can be one of the following: <ul style="list-style-type: none"> • Malicious • Suspicious • PUP 	String	25

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				<ul style="list-style-type: none"> Inclusive Likely Safe Safe 		
Destination	dst	dst	—	Destination of the event. The target can be IP, URL, port, file creation, etc.	String	255
First Seen	FirstSeen	deviceCustomDate1	deviceCustomDate1Label=FirstSeen	Time of the first occurrence of the event in UTC format: <i>DD-MM-YYYY, hh:mm:ss</i> . FortiEDR uses the Collector device's time when tracking security events.	Timestamp	18
Last Seen	LastSeen	deviceCustomDate2	deviceCustomDate2Label=LastSeen	Time of the last occurrence of the event in UTC format: <i>DD-MM-YYYY, hh:mm:ss</i> . FortiEDR	Timestamp	18

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				uses the Collector device's time when tracking security events.		
Action	Cat	act	—	The action taken upon the event. The action can be either "logged" or "blocked".	String	50
Count	Count	cnt	—	Number of occurrences of the Raw Data Item (RDI).	Integer	16
Certificate	AppSigned	AppSigned	—	Signed status of the process triggering the event. The status can be "yes" or "no".	String	3
Rules List	Alerts	reason	—	Security policy rules triggering the event. Refer to Out-of-the-box policies for a full list of predefined	String	5000

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				d policies.		
Users	usrName	user	—	Names of device logged users at the time of the event.	String	750
MAC Addresses	srcMAC	dmac	—	Protected device MAC Address.	String	170
Script	ProcessScriptModule	ProcessScriptModule	—	Name of the script the process has run. This field applies to only security events that include scripts.	String	32000
Script Path	ProcessScriptModulePath	ProcessScriptModulePath	—	Path of the script the process has run. This field applies to only security events that include scripts.	String	32000
Autonomous System	ASN	ASN	—	ASN of the destination IP.	String	255
Country	Country	callLanguage	—	Name of country	String	255

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				the destination IP belongs to.		
Process Hash	ProcessHash	fileHash	—	Hash of the process triggering the event.	String	40
Source IP	src	deviceTranslatedAddress	—	The protected device IP.	String	255
Threat Name	ThreatName	threatAttackID	—	Name of the threat if the process is an identified threat.	String	250
Threat Family	ThreatFamily	threatActor	—	Family of the threat if the process is an identified threat.	String	200
Threat Type	ThreatType	frameworkName	—	Type of the threat if the process is an identified threat.	String	200

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Remediation Processes	TerminateProcess ProcessName, TerminateProcessId	TerminateProcess ProcessName, TerminateProcessId	—	List of processes that FortiEDR attempted to kill if the Process Termination action has been triggered by the event.	String	1000
Remediation Files	ExecutablesToRemove	ExecutablesToRemove	—	List of files that FortiEDR attempted to delete if the File Remediation action has been triggered by the event.	String	1000
MITRE Techniques	MitreTags	MitreTags	—	MITRE technique associated with the event, if any.	String	3000

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Target	EventTarget	EventTarget	—	Target of the operation that triggered the event. The target can be a file/process, registry key, or CVE Identifier.	String	2000
Command line	EventCommandLine	EventCommandLine	—	Command line involved in the event, if any.	String	2000
Remote Connection	RemoteConnection	RemoteConnection	—	IP address of the remote host, if a remote host initiated the exploitation of the triggering device.	String	2000
Deployment	Deployment	Deployment	—	Server name.	String	64
Stack Hashes	StackHashes	StackHashes	—	Hashes of files on the process stack.	String	512

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Stack Certificates	StackCertificates	StackCertificates	—	Signed status of files on the process stack.	String	64
<p>Custom fields in CEF format (such as <i>cs1</i> and <i>deviceCustomDate1</i>) should be sent with the matching CEF custom label value in order to define the display label for this custom field to the consumer system. The message then includes the following two fields:</p> <ol style="list-style-type: none"> 1. CEF custom label value 2. CEF field name (such as <i>cs1</i>) that holds the actual value of the field <p>For example, for <i>Organization "Marketing"</i>, FortiEDR sends the following two CEF fields in the message: "<i>cs1Label=Organization</i>" and "<i>cs1=Marketing</i>".</p>						

System event

The following table describes the fields in system events. The order that the fields are listed reflects the order of the fields in system event syslog messages.

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Organization	Organization	cs1	cs1Label=Organization	Name of the organization the system event belongs to.	String	100
Message Type	MessageType	cs2	cs2Label=MessageType	Type of the message, such as audit record, security event, or system event.	String	One of the following fixed values: <ul style="list-style-type: none"> • Audit • Security Event

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
						<ul style="list-style-type: none"> System Event
Server Name	Servername	cs4	cs4Label=Servername	Name or address of the FortiEDR Manager that initiated the message.	String	128
Date and Time	Date	deviceCustomDate1	deviceCustomDate1Label=Date	Time of the occurrence of the event in UTC format: <i>DD-MM-YYYY, hh:mm:ss</i> . FortiEDR uses the Central Manager's time when tracking system events.	Timestamp	18
Component	Component	cs6	cs6Label=Component	FortiEDR component type. It can be one of the following: <ul style="list-style-type: none"> • Collector • Core • Manager • Aggregator 	String	100

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
				<ul style="list-style-type: none"> Repository License 		
Component Name	Component Name	cs5	cs5Label=Component Name	Name of the component.	String	150
Description	Description	reason	—	Details of the event.	String	300

Custom fields in CEF format (such as *cs1* and *deviceCustomDate1*) should be sent with the matching CEF custom label value in order to define the display label for this custom field to the consumer system. The message then includes the following two fields:

1. CEF custom label value
2. CEF field name (such as *cs1*) that holds the actual value of the field

For example, for *Organization "Marketing"*, FortiEDR sends the following two CEF fields in the message: "*cs1Label=Organization*" and "*cs1=Marketing*".

Audit trail

The following table describes the fields in audit trails. The order that the fields are listed reflects the order of the fields in audit trails syslog messages.

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Organization	Organization	cs1	cs1Label=Organization	Name of the organization the system event belongs to.	String	100

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Message Type	MessageType	cs2	cs2Label=MessageType	Type of the message, such as audit record, security event, or system event.	String	One of the following fixed values: <ul style="list-style-type: none"> Audit Security Event System Event
Server Name	Servername	cs4	cs4Label=Servername	Name or address of the FortiEDR Manager that initiated the message.	String	128
Date and Time	Date	deviceCustomDate1	deviceCustomDate1Label=Date and Time	Time of the occurrence of the audited action in UTC format: <i>DD-MM-YYYY, hh:mm:ss</i> . FortiEDR uses the Central Manager's time when tracking audit trails.	Timestamp	18

Syslog Field	LEEF Field	CEF Field ¹	CEF custom label value	Description	Data Type	Length
Sub-system	Subsystem	cs3	cs3Label=Sub-system	Name of the FortiEDR module where the audited action was performed. For example: Administration, System, System Events.	String	25
User Name	usrName	suser	—	Name of the user performing the audited action.	String	250
Description	Description	reason	—	Details of the audited action.	String	1500

Custom fields in CEF format (such as *cs1* and *deviceCustomDate1*) should be sent with the matching CEF custom label value in order to define the display label for this custom field to the consumer system. The message then includes the following two fields:

1. CEF custom label value
2. CEF field name (such as *cs1*) that holds the actual value of the field

For example, for *Organization "Marketing"*, FortiEDR sends the following two CEF fields in the message: "*cs1Label=Organization*" and "*cs1=Marketing*".



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 Chief Legal Officer, 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.