Ransomware Detection powered by CyberSense®

v8.13.0

System Log Messages Guide

Lists the various alerts and application-level messages that can appear in the Ransomware Detection system log file.

MK-25RDCS005-00
September 2025

Contents

Chapter 1. Introduction

This document lists the various alerts and application-level messages that can appear in the Index Engines system log file. When configured, informational and alert messages are collected in a log file usually named `iesyslog.log`. On SLES and RHEL systems, the file is typically located in `/var/log` on the Index Engines server. The location and file name can be changed to suit your requirements or preferences. See Audit Trail logging *(on page 6)* for more information on configuring syslog to capture audit trail messages.

Audit Trail logging

The Audit Trail feature logs all user actions and application-level messages, which are also referred to as message center alerts. Audit trail information includes the user who performed an action, the action taken, the engine on which the action happened, and the date and time of the action. The message center alerts covers the services that run during different processes, such as indexing jobs, starting and stopping services.

These Index Engines messages are sent to the syslog facility called `local1`. In order to see the messages in the `/var/log/iesyslog.log` file, syslog must be configured to direct the messages from the `local1` facility to the log file. See Suggested syslog configuration *(on page 6)* for more information.

Suggested syslog configuration

To capture the user actions and application-level messages on a SLES or RHEL system, update the system logging configuration as follows:

1. Save a copy of the `/etc/rsyslog.conf` file.
2. Update the `/etc/rsyslog.conf` file as follows:

   a. Add the following lines to the end of the script if they don't exist. If they do exist and are commented out, uncomment them by removing the # in front of the line.

   ```
   $ModLoad imudp
   $UDPServerRun 514
   $ModLoad imtcp
   $InputTCPServerRun 514
   LOCAL1.* /var/log/iesyslog.log
   ```

   Note: The last line above determines where the logs will be stored. If you use the Index Engines backup feature to return your log(s), store the logs in the `/opt/ie/var/` directory. For example: `/opt/ie/var/log/iesyslog.log`

   b. In `/etc/rsyslog.conf`, add `local1.none` to the line for `/var/log/messages` as shown below:

   ```
   *.info;mail.none;authpriv.none;cron.none;local1.none /var/log/messages
   ```

   Note: The line in the `/etc/rsyslog.conf` file may look different than the example above depending on your OS and should be located at the end of the file.

3. Restart the `rsyslog` service by executing this command:

```
systemctl restart rsyslog.service
```

The `/var/log/iesyslog.log` file will now record all user actions. Your system administrator should manage this file using `logrotate` — or a similar command — to rotate and purge logs as desired.

Once the setup completes, messages start appearing in `/var/log/iesyslog.log`. These messages will be similar to those in the following example:


```
Mar 4 09:16:03 farset local1: {"engine":["farset.test.indexengines.com"],"description":
["Index trunk_r98672 (ID 110) has been deselected."],"date":["Mar-04-2016 09:16:03"],"user":
["admin"],"function":["DeselectIndex"]}

Mar 4 09:16:39 farset local1: {"engine":["farset.test.indexengines.com"],"description":
["Index trunk_R98712 (ID 111) has been selected."],"date":["Mar-04-2016 09:16:39"],"user":
["admin"],"function":["SelectIndex"]}

Mar 4 09:40:06 farset local1: {"engine":["farset.test.indexengines.com"],"description":["admin
logging in..."],"date":["Mar-04-2016 09:40:06"],"user":["admin"],"function":["LogIn"]}

Mar 4 09:41:31 farset local1: {"engine":["farset.test.indexengines.com"],"description":
["Catalog Ingestion Save Server"],"date":["Mar-4-2016 09:41:31"],"user":["admin"],"function":
["CatalogIngestionSaveServer"]}
```

Chapter 2. Message format

The system log messages are written in Common Event Format (CEF) to `/var/log/iesyslog.log`, unless you have set up a different location, such as `/opt/ie/var/log`, and file name. The messages for various services alerts are written in one of the two CEF message formats, CEF:0 and CEF:1.

For a complete list of alerts for the various services, see the enclosed Alert tables *(on page 13)* tables.

CEF:0 Message format

The format is:

```
CEF:0|Index Engines|Catalyst |ie_version |service_name |servtype_alertstat |alert_severity
 |message_text
```

The message format is broken down into the various parts in the table below.

Name	Description
CEF:0	Specifies the message format and version which is CEF, version 0.
Index Engines	The name of the device or software vender that is producing the alert
Catalyst	The vendor product.
ie_version	The version of the Index Engines software.
service_name	The name of the service which caused the alert.
servtype_alertstat	The service type and the alert status. See the Status of a CEF:0 message *(on page 11)* section below.
alert_severity	The severity of the service alert. See the Severity of a CEF:0 message *(on page 10)* section below.
message_text	The message text is an optional JSON-encoded string that has extra parameters as listed in the descriptions of the alerts. These extra parameters add information to the message text, such as a job ID or the name of a production.

Severity of a CEF:0 message

The table below lists the possible message severities that can occur in CEF:0 messages.

Severity	Description
notice	The alert is for informational purposes only.
normal	The alert indicates an event that occurred.
warning	Indicates that the issue which raised the alert may be a concern and to observe if the alert changes.
error	The alert was caused by an error.
critical	The issue is critical and must be dealt with.
attn	Indicates that action is required to clear the alert.

Severity	Description
`detail`	Indicates an event occurred during post-processing job phases, such as at the start and the successful ending of the post-processing job. If a job does not end successfully, the severity would change to “warning” or “error”.

Status of a CEF:0 message

The following table lists the available status values which appear in the messages.

Status	Description
`event`	This was a singular event and not updated.
`pend`	The pending condition must be resolved.
`resolve_ok`	The issue was resolved successfully.
`resolve_skip`	The issue was resolved by skipping, ignoring, or discarding it.
`resolve_cancel`	The issue was resolved by being withdrawn, canceled, or abandoned.
`resolve_restart`	The issue was resolved or abandoned as part of the service restart or crash.
`resolve_failed`	The issue was resolved by failure.
`resolve_replace`	The issue was replaced with a new one.
`inprogress`	The process, job, or step has not completed yet.
`done_ok`	A successful end to the process, job, or step that was previously “inprogress”.
`done_failed`	The process, job, or step completed as failed.
`done_cancel`	The process, job, or step was cancelled and did not complete.
`done_abrupt`	The process, job, or step was abruptly ended due to a service restart or crash.

CEF:1 Message format

The format is:

```
CEF:1 |Index Engines |service_name |ie_version |log_entry_ID |entry_name |alert_severity
 |message_text
```

The message is broken down into the parts listed in the table below.

Name	Description
`CEF:1`	Specifies the message format and version which is CEF, version 1.
`Index Engines`	The name of the device or software vendor that is producing the alert
`service_name`	The name of the service which caused the alert.
`ie_version`	The version of the Index Engines software.
`log_entry_ID`	ID of the log entry for reference.
`entry_name`	Alert name and status of the service that caused the alert.
`alert_severity`	The severity of the notification message.
`message_text`	The message text is a string which has extra parameters as listed in the descriptions of the alerts. These extra parameters add information to the message text, such as: • `suser` mentions the user accessing the software. • `src` specifies the ip address of the user machine. • `msg` specifies the associated key-value pairs as applicable.

Severity of a CEF:1 message

The table below lists the possible message severities that can occur in CEF:1 messages.

Severity	Description
`Low`	The issue is of Low severity. It needs to be monitored and dealt with as required.
`Medium`	The issue is of Medium severity. It needs monitoring and dealt with as required.
`High`	The issue is significant and must be dealt with.
`Critical`	The issue is critical and must be dealt with.

Chapter 3. Alert tables

The following tables list possible alerts for the various services that run in the Index Engines software. As you become more familiar with the alert messages, you will see that most alert messages are self-explanatory and can easily be deciphered to troubleshoot issues.

Note: If an alert has parameters which will produce the additional JSON-encoded message text, these parameters are listed in the **Description** field.

Extract process alerts

The following table lists the alerts produced by the extract process service. This service performs extracting, archiving, file copying, deleting, click-through, relinking, and job re-indexing.

Example

```
CEF:0|Index Engines|Catalyst|8.3.0-1.25|extract|extract_up - event|normal
```

In this example, the extract process service is running – `extract_up` – with the status being an “event” and the severity is “normal”. This alert does not have any extra parameters for additional information.

Alert Type	Description
`extract_up`	The service is up and running.
`extract_down`	The service is down/disabled.
`extract_mntprob`	Indicates a mount problem, and the parameters can be included in the message text: • jobid • run • indexed_file • hint_path • mntid • clickthrough
`extract_job`	The job status is created at the start of running a job. The status is updated when it is in progress or done. Additional information is: • jobid • run • user • type • status • msg • parent job information
`extract_prod_create`	The production was created. Additional information is:

Alert Type	Description
	• id • name
`extract_prod_del`	The production was deleted. Additional information is: • id • name

Indexing (dispatch) alerts

The following table lists the alerts for the indexing (dispatch) service. The index (dispatch) service manages the indexing process for all indexing jobs.

Example

```
CEF:0|Index Engines|Catalyst|8.3.0-1.25|dispatch|dispatch_down - event|normal
```

In this example, the indexing service is down or disabled – `dispatch_down` – with the status being an "event" and the severity is "normal". This alert does not have any extra parameters for additional information. This alert is generated when the service is stopped or restarted.

Alert Type	Description
`dispatch_up`	The service is up and running.
`dispatch_down`	The service is down/disabled.
`dispatch_seg`	The status of an Index Segment, which is updated when finished. Additional information in the message string is: • dbname • dbuuid • updated on close
`dispatch_crawljob`	The dispatch job status, which is updated when the status changes on the LAN crawl job, NFS, CIFS, NDMP, or local job. Additional information in the message string can include: • message or jobdefid • jobdefname • jobinstid
`dispatch_ieapijob`	The dispatch job status on an IEAPI job, which excludes crawl, cat-ing, reindex. The status is updated when it changes and a new message is created.
`dispatch_ndmpjob`	The dispatch job status on a NDMP job, which excludes crawl-initiated. The status is updated when it changes and a new message is created..

Generic service alerts

The following table lists the possible generic service alerts. This service generates alerts about events that are not tied to a specific service.

Alert Type	Description
`generic_resource`	Resource limitation with additional information included in the message string.
`exit_abnormal`	Service abnormal termination with the following additional information: • processname • pid
`low_disk`	Low disk space with the disk information displayed as an array of mount points and the percentage of used space.
`full_disk`	No available disk space remaining. The information displayed as an array of mount points and the percentage of used space.
`stall_disk`	Some processing is stalled because of low disk space. The status is updated when changed and is used by exchange indexer.
`thrashing`	Thrashing process status, which is updated when changed.
`failstart`	A service failed to start. The process name is listed in the message string.
`insuf_lic`	Insufficient licenses with additional information listed in the message string.
`cloud_persistent_limit`	The limit of the number of persistent cloud instances has been reached.
`login_blocked`	The specified user name has been blocked from logging in.
`login_unblocked`	The specified user name has been unblocked and can log into the Index Engines system again.

Post-processing alerts

The following table lists the possible post-processing service alerts. This service runs after indexing and completes the segments so that they can be rapidly searched as well as controls segment migration and segment merge.

Alert Type	Description
`postproc_up`	The service is up and running.
`postproc_down`	The service is down/disabled.
`postproc_job`	The post-processing job status, which updates when the status changes. Additional information is included in the message string: • name • dbname • dbuuid • status • message
`postproc_malware`	A malware file was found.
`postproc_yara`	A YARA ruleset matched.

Query service (qserv) alerts

The following table lists the possible query service (qserv) alerts. This service manages and executes queries.

Alert Type	Description
`qserv_up`	The service is up and running.
`qserv_down`	The service is down/disabled.
`qserv_job`	The status of a single query job, which updates if the status changes. Additional information is included in the message string: • jobdefid • jobinstid • descript • name • qtime • nfound • url

Index manager alerts

The following table lists the possible index manager alerts. The index manager service manages the indexes, which includes letting you add, select, remove, and deactivate indexes as well as setting up and managing engines in a federation.

Example

```
CEF:0|Index Engines|Catalyst|8.3.0-1.25|indexman|indexman_up - event|normal
```

Alert Type	Description
`indexman_up`	The service is up and running.
`indexman_down`	The service is down/disabled.
`indexman_ixcreate`	The index was created with additional details included in the message string: • id • name • tapedb_uuid
`indexman_ixdestroy`	The index was destroyed with additional details included in the message string: • id • name
`indexman_ixselect`	The status of an index in the process of being selected, which updates when the status changes to in progress or done. Additional information is included in the message string: • id • name • error
`indexman_fedjoin`	The engine has joined a federation with additional information included in the message string.
`indexman_fedleave`	The engine has left a federation with additional information included in the message string.

Security domain (secd) manager alerts

The following table lists the possible security domain (secd) service alerts. The security domain manager typically works with Active Directory (AD) and NIS to deduce current information regarding users and their access rights.

Alert Type	Description
`secdman_up`	The service is up and running.
`secdman_down`	The service is down/disabled.
`secdman_ad_oosync`	Indicates the time is out of sync with the AD time and can update when changed. Additional information in the message string is: • domain • offset

Scheduler alerts

The following table lists the possible scheduler service alerts. The scheduler service starts, stops, and pauses scheduled indexing jobs and queries.

Alert Type	Description
`sched_up`	The service is up and running.
`sched_down`	The service is down/disabled.
`sched_pause`	The scheduler job paused with additional information in the message string: • job type • reason
`sched_unpause`	The scheduler job was unpaused and the job type information is included in the message string.

CyberSense service alerts

The following table lists the possible CyberSense (iecrd, SearchResults, and ClearInfectionFromIndexResults) service alerts.

Alert Type	Description
`iecrd_up`	The service is up and running.
`iecrd_down`	The service is down/disabled.
`iecrd_infection`	An infection was detected with the message string including the CyberSense policy name. **Note:** The message text of the `iecrd_infection` log messages contain a JSON-encoded string of additional alert details, detailing to the unique directory containing the suspect files.
`iecrd_job`	The status of a CyberSense job with additional information included in the message string: • CyberSense job ID • CyberSense policy name • LAN job definition name • LAN job instance ID
`SearchResults`	The **Stop Reporting** button was selected on a particular **Infection found** alert in the **Message Center**. The message also returns the Query ID (qid) that searches for the files tagged with `/suspect`.
`ClearInfectionFromIndexResults`	The `/suspect` tag was cleared from a set of files returned by a search of the index.

Licensing alerts

The following table lists the possible licensing service alerts.

Alert Type	Description
`licd_up`	The service is up and running.
`licd_down`	The service is down/disabled.
`licd_overd`	A license overdraft occurred. The additional information in the message string includes the grace time limit.

GCSDB alerts

The following table lists the possible GCSDB service alerts. This service is one of the post-processing services that run during the post-processing phase of a job.

Alert Type	Description
`gcsdb_up`	The service is up and running.
`gcsdb_down`	The service is down/disabled.
`gcsdb_job`	The status of a single post processing step with additional information included in the message string: • name • dbname • dbuuid • status • message

Filestore alerts

The following table lists the possible filestore service alerts. This service is one of the post-processing services that run during the post-processing phase of a job.

Alert Type	Description
`filestore_up`	The service is up and running.
`filestore_down`	The service is down/disabled.
`filestore_job`	The status of a single post processing step with additional information included in the message string: • name • dbname • dbuuid • status • message

REST API alerts

The REST API service alerts use CEF:1 message format.

Example:

```
CEF:1|Index Engines|REST API|8.6.0|24|Audit trail settings updated successful|Low|suser=admin
 src=10.20.10.20 msg=cybersense : 1; heartbeat : 0
```

In this example, the REST API service for audit trail setting was run by user 'admin' from source '10.20.10.20' with severity as “Low".

The following table lists the possible REST API service alerts and associated severity level.

Entry Name	Severity
Login settings updated successfully.	Medium
Failed to update login settings.	Medium
User delete successfully.	Medium
User delete operation failed.	Medium
User creation operation succeeded.	Low
User creation operation failed.	Low
User update operation succeeded.	Low
User update operation failed.	Low
Software upgrade succeeded.	Medium
Software install failed.	Medium
RSS Threshold created.	Low
Failed to create RSS Threshold bad request values.	Medium
Failed to create RSS Threshold.	High
RSS Threshold modified.	Low
Failed to modify RSS Threshold bad request values.	Medium
Failed to modify RSS Threshold - internal system failure.	High
Activity alert level was modified.	Low
Activity alert level was retired.	Low
Threshold configuration changes successfully.	Low
Failed to change threshold configuration.	Low

Entry Name	Severity
Alert cleared successfully.	Medium
Host or hosts removed from the Disabled Hosts list.	Low
Hosts or hosts added to the Disabled Hosts list.	Low
Session configuration was modified.	Low
Register to the license server succeeded.	Low
Register to the license server failed.	Medium
Deregister from the license server succeeded.	Low
Deregister from the license server failed.	Medium
Active directory enable/disable operation succeeded.	Low
Active directory enable/disable operation failed.	Medium
Email notification settings updated successfully.	Low
Email notification settings failed to update.	Medium
Security certificates for SSL/TLS connection uploaded successfully.	Low
Failed to upload security certificates for SSL/TLS connection.	Medium
Audit trail settings updated successful.	Low
Failed to update audit trail settings.	Low
Enable/disable HTTP operation succeeded.	Medium
Enable/disable HTTP operation failed.	Medium
Query domain settings modified successfully.	Medium
Failed to modify query domain settings.	Medium

Chapter 4. Notifications

Some messages that appear in the `/var/log/iesyslog.log` file are not alerts but are informational messages or notifications. These informational messages have the same format as the alert messages with a few differences.

The format is:

```
CEF:0|Index Engines|CyberSense|ie_version|service_name_num|alert_severity_num|{JSON_message}
```

The message is broken down into the parts listed in the table below.

Name	Description
`CEF:0`	Specifies the message format and version and CEF, version 0.
`Index Engines`	The name of the device or software vender that is producing the alert
`CyberSense`	The vendor product, which is the CyberSense product.
`ie_version`	The version of the Index Engines software.
`service_name_num`	The number that corresponds to the name of the service which created the notification.
`alert_severity_num`	The number that corresponds to the severity of the notification message. Currently, this is `2`, which corresponds to the severity of `normal`, for all notification messages
`message_text`	The message text is a JSON-encoded string which has extra parameters as listed in the descriptions of the alerts. These extra parameters add information to the message text, such as a job ID or the name of a production.

For a list of notification messages, see the enclosed Informational messages *(on page 30)* table.

Informational messages

The following table lists the informational messages produced by the web service, `20`. The JSON string displays the notification information in the `log_description` text.

Example

```
CEF:0|Index Engines|CyberSense|8.3.0-1.25|20|2|{"user": "admin", "remote_ip":
"10.20.10.28", "hostnames": ["server1.domainname.com", "server2.domainname.com"],
"infection_types": ["Possible corruption of a database"],
"log_description": "Hosts added to disabled hosts list"}
```

Log Description Text	Description
`Hosts added to disabled hosts list`	Database corruption alerts will no longer be reported for this host(s) in the CyberSense UI.
`Hosts removed from the disabled hosts list`	Database corruption alerts will be reported for the host(s) in the CyberSense UI.

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information
Americas: +1 866 374 5822 or info@hitachivantara.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com
Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com