

Sending Syslog Notifications to SIEMs

Lumeta [superusers](#) can use the CEF logging feature to send syslog output to an external viewer in a common-event format. By enabling it, all event notifications to which the superuser has subscribed can be displayed in one preferred Security Information and Event Management (SIEM) viewer such as HP ArcSight, Splunk, or QRadar.

CEF Notifications are either system-related or device-related. The system-related notifications are global and pertain to all of Lumeta. Device notifications pertain to a particular zone. Subscribe to receive notifications at Settings > Lumeta Systems > CEF Notifications > System and Device tabs.

| System License CEF Notifications eth0 | | | |
|---------------------------------------|-----------------|----------|-----------------|
| Configuration Device System | | | |
| Edit ▾ | | | |
| Subscribed | Name | Priority | Event Type |
| No | Agent Connected | | AGENT_CONNECTED |
| Yes | Agent Started | | AGENT_START |
| No | Agent Status | | AGENT_STATUS |
| Yes | Agent Stopped | | AGENT_STOP |

- **System notices** report when an Agent, Collector, Scout, or Zone has been created, started or stopped. They also alert on license status (e.g., reminder, warning, and violation).
- **Device notices** report findings about your network architecture such as when a device, edge, or node has been discovered, updated, or removed.

This section provides an example of integrating to the representative event manager HP ArcSight.

Configure CEF Server

Enable the CEF logging feature to make Lumeta compile all subscribed event notifications to a logging server. Here's an example of how to enable logging to a HP ArcSight console via the Lumeta graphical user interface (GUI) or the Lumeta command-line interface (CLI).

Configure CEF Server via GUI

1. [Log in](#) Lumeta.
2. Select **Settings > Lumeta Systems**.
3. Click the **CEF Notifications** tab.
4. Identify the logging server to which you want to send event notifications.
 - a. **Protocol:** Type TCP-IPv4, UDP-IPv4, TCP-IPv6, UDP-IPv6
Note: Use TCP-IPv4 or UDP-IPv4 for HP ArcSight.)
 - b. **Host Name or IP Address:** Must be an IPv4-type IP address
 - c. **Port number:** Must be a valid integer
5. When you are ready to send CEF-formatted event notifications, click the **CEF Enabled** checkbox.
6. Click **Submit**.
A message displays, indicating that your configuration settings were saved.
Lumeta is now configured to display CEF-formatted syslog output in your ArcSight console.

Configure CEF Server via CLI

1. Log in the Command-Line Interface (CLI).
 - a. Open a host or server that supports SSH.
 - b. At the prompt, type **ssh admin@<yourservername>** and press **Enter**.
 - c. Enter your password (i.e., **admin**) and press **Enter**.
2. At the command prompt, type
log cefserver <enable/disable> <protocol> <IP address> <port number> and press **Enter**.
 - a. **Protocol:** Type TCP-IPv4, UDP-IPv4, TCP-IPv6, UDP-IPv6 (Note: Use TCP-IPv4 or UDP-IPv4 for HP ArcSight.)
 - b. **IP Address:** Must be an IPv4-type IP address
 - c. **Port number:** Must be a valid integer
 - d. **Enable:** Enables the CEFserver
 - e. **Disable:** Disables the CEFserver

Lumeta is now configured to display CEF-formatted syslog output in your HP ArcSight console.

Configuring CEF-Formatted Syslog Output

1. On the CEF Notifications tab, click the tab for the type of CEF Notifications to which you want to subscribe: either **System** or **Device**.
2. To edit the prioritization of the event and whether you subscribe to it, click Edit and update the form.
 - a. **Subscribed:** Indicates whether or not you've opted to send notifications of the particular event type.
 - b. **Name:** Name of the event
 - c. **Priority:** Indicates level of severity: informational, alert, or warning.
 - d. **Event Type:** The Event Type is the predefined category of event.
3. To Add a device notification, click Add and update the form.
4. To apply additional filters to your device notifications, update this form:

| Optional filtering criteria for Device Notifications | | | | |
|--|--|-------------|----------------------------------|--|
| Device Type: | <input type="text" value="All"/> | | | |
| Vendor: | <input type="text" value="All"/> | Model: | <input type="text" value="All"/> | |
| OS: | <input type="text" value="All"/> | OS Version: | <input type="text" value="All"/> | |
| Ports: | <input type="text" value="Enter one or more ports separated by commas"/> | | | |

CEF Output

Header Syntax

<syslogheader> CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity

Header Sample

22 Jul 2014 13:28:59 grog CEF:0|Lumeta|Lumeta|3.2.4.9086|DEVICE_DISCOVERED|Device Discovered|5

Message Sample

msg=Device stealth:c:3038:1 created.

Lumeta-specific Fields

The message is followed by Lumeta specific custom fields mapped to CEF attributes. All custom fields are appended after "msg."

CEF Event Mapping

Following is a CEF notification and how it maps to custom fields in Lumeta.

0|Lumeta|Lumeta|3.2.4.9086|DEVICE_DISCOVERED| Device Discovered |5|msg=Device stealth:c:3038:1 created. cat= DISCOVERY dvchost=CCM-AMC
rt=Nov 02 2017 13:19:55 cn1=1 cn1Label=Facility Zone1 dhost= c6a3= mac=

| | Lumeta Custom Fields | | | |
|------------------|----------------------|-------------------|---|---------------------------------------|
| CEF Key Name | Full Name | DataType | Lumeta name | Mapping to a notification from Lumeta |
| Device Vendor | | | Lumeta | Lumeta |
| Device Product | | | Lumeta | Lumeta |
| Device Version | | | 2.1 (version of Lumeta) | 3.2.4 |
| Signature ID | | String or integer | Notification Type | DEVICE_DISCOVERED |
| Name | | String | NotificationName/NotificationType | Device Discovered |
| Severity | | Integer | 1, 5, 10 | 5 |
| cat | deviceEventCategory | String | DISCOVERY("/discovery"), SYSTEM("/system"), CONFIG("/config") | DISCOVERY |
| deviceMacAddress | deviceMacAddress | MAC Address | mac | |
| dvc | deviceAddress | IPv4 Address | ip | |
| rt | receiptTime | TimeStamp | event.getTimeStamp() | Nov 02 2017 13:19:55 |
| dvchost | deviceHostName | String | systemName | CCM-AMC |

| | | | | |
|-----------------|--------------------------|--------|----------|----------------|
| dhost | destinationHostName | String | ip | c6a3 |
| c6a3 | destination format | IPv6 | ip | |
| suser | sourceUserName | String | userName | |
| cn1 | deviceCustomNumber1 | Long | zoneId | 1 |
| cn1Label | deviceCustomNumber1Label | String | zoneName | Facility Zone1 |

| CEF Event Type | Description | Sample Message |
|-----------------------------|---|--|
| AGENT_CONNECTED | A connection was created between discovery-agent and lumeta-webapp | Discovery Agent Connected |
| AGENT_START | Displays one of the following Agent and that it has started: TCP Port Scanner Host Discovery Snmp Hunter Snmp Scanner Path Scanner Broadcast Discovery CIFSScanner DNSScanner Http Scanner Leak Discovery | Host Discovery (or any other agent name) Started Agents: TCP Port Scanner Host Discovery Snmp Hunter Snmp Scanner Path Scanner Broadcast Discovery CIFSScanner DNSScanner Http Scanner Leak Discovery |
| AGENT_STATUS | Displays the Agent Name (to show that the Agent is currently running): TCP Port Scanner Host Discovery Snmp Hunter Snmp Scanner Path Scanner Broadcast Discovery CIFSScanner DNSScanner Http Scanner Leak Discovery | Host Discovery (or any other agent name) |
| AGENT_STOP | Displays one of the following Agent and that it has stopped: TCP Port Scanner Host Discovery Snmp Hunter Snmp Scanner Path Scanner Broadcast Discovery CIFSScanner DNSScanner Http Scanner Leak Discovery | Host Discovery (or any other agent name) Stopped |
| COLLECTOR_CREATED | New Lumeta Collector created containing device discovery configuration | Collector <> created |
| COLLECTOR_REMOVED | Indicated existing Lumeta Collector has been removed | Collector <> removed |
| COLLECTOR_UPDATED | Updated discovery configuration was applied to a Lumeta Collector | Collector <> Config Inserted |
| DEVICE_ACTIVITY | Discovered device's status has changed from active to inactive (or vice versa) | Device <> became active. Earlier state : inactive OR Device <> became inactive. Earlier state : active |
| DEVICE_DISCOVERED | New entry for a Device discovered. Multiple entries for each scan technique | Device<>created |
| DEVICE_PROFILED | Discovered device's profile information has changed. Profile information includes device type, operating system, operating system version and vendor. | Device<>profileattributeschanged: DeviceType=<>,OS=<>,Vendor=<>, Version=<> 2017-11-0709:24:13.384338 |
| DEVICE_REMOVED | Discovered device has become inactive and removed | Device<>removed |
| DEVICE_UPDATED | Discovered Device has been updated with new information. Multiple entries for each scan technique. | Device<>updated. IPassignedto<> IPchangedto<> |
| FORWARDER_DISCOVERED | Discovered device has been identified as a forwarding device based on TTL | Device<>forwardstraffic |
| JOB_COMPLETED | Displays status of a background job that was deployed on the Lumeta box (example: importing pattern file, importing zone attributes) | Job Success (jobId : 1, jobName : importPatterns-job) |
| JOB_STARTED | Displays initialization of a background job that was deployed on the Lumeta box (example: importing pattern file, importing zone attributes) | Job Started (jobId : 1, jobName : importPatterns-job) |
| LEAK_DISCOVERED | Lumeta has identified a potential Leak Path to / from a protected network | |
| LICENSE_REMINDER | User notification that the Lumeta license is about to expire | License expiration imminent – contact support@lumeta.com |

| | | |
|--------------------------------------|--|--|
| LICENSE_VIOLATION | User notification that the Lumeta license has exceeded the IP Count | License expired – new license required – contact support@lumeta.com IP count exceeded – contact support@lumeta.com |
| LICENSE_WARNING | User notification that the Lumeta license is approaching the IP Count limit | License expired – contact support@lumeta.com IP count exceeded – contact support@lumeta.com |
| LINK_DISCOVERED | Path has been discovered between two IPs | Linkdiscoveredbetween<>and<> |
| LOGLEVEL_UPDATED | Log level has been changed to INFO/WARN/DEBUG | Service <> log level set to <> |
| NOTIFICATION_ACKNOWLEDGED | Displays the Notification ID that was acknowledged by the user on Lumeta System's map. | Notification<notificationnumber>acknowledged |
| NOTIFICATION_ACKNOWLEDGED_ALL | All Notifications on Lumeta System's map have been acknowledged for a specific priority. | AllNotificationsacknowledgedforpriority<INFO WARN ALERT> |
| OPENPORT_DISCOVERED | Discovered Device has been found with an open port | |
| ROUTER_DISCOVERED | Discovered Device is now profiled as a router | |
| ROUTER_REMOVED | Discovered Device that was profiled as a router has now been removed | |
| SYSTEM_CONNECT | User notification that a connection has been created between CC <-> Portal, CC <-> Scout | Peer connection established (<> <-> <->) |
| SYSTEM_DISCONNECT | User notification that a disconnection occurred between CC <-> Portal, CC <-> Scout | Peer connection closed (<> <-> <->) |
| UPDATE_ERROR | | |
| UPDATE_REMOTE | | |
| UPDATE_STEP | | |
| UPDATE_WARNING | | |
| USER_CREATED | New Lumeta user was created | User <> created |
| USER_REMOVED | Lumeta user was deleted | User <> removed |
| USER_UPDATED | Changes were made to an existing Lumeta user | User <> updated |
| ZONE_CREATED | New Lumeta Zone created containing device discovery configuration | Created zone. (name = <>, description = <>, updatenotes = "time"=>"2017-11-07 13:35:07.257405-05") |
| ZONE_REMOVED | Indicated existing Lumeta Zone has been removed | Deleted zone. (name = <>, description = <>, updatenotes = "time"=>"<>", "user"=>"<>") |
| ZONE_UPDATED | Updated discovery configuration was applied to a Lumeta Zone | Zone <> CIDRs Updated |