Configuring Syslog Notifications to QRadar

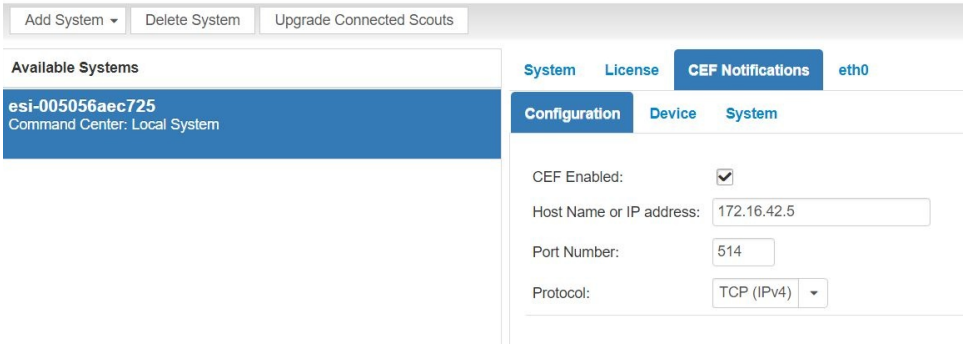
Lumeta superusers can use the CEF logging feature to send syslog output to QRadar in a common-event format. By enabling it, all event notifications to which the superuser has subscribed are sent to QRadar for analysis.

> QRadar 7.3 or later is required for this procedure.

Configure CEF Server via GUI

To enable logging to a QRadar console via the Lumeta graphical user interface (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
   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 QRadar console.

Configure CEF Server via CLI

To enable logging to a QRadar console via the Lumeta graphical user interface (GUI) or the Lumeta command-line interface (CLI).

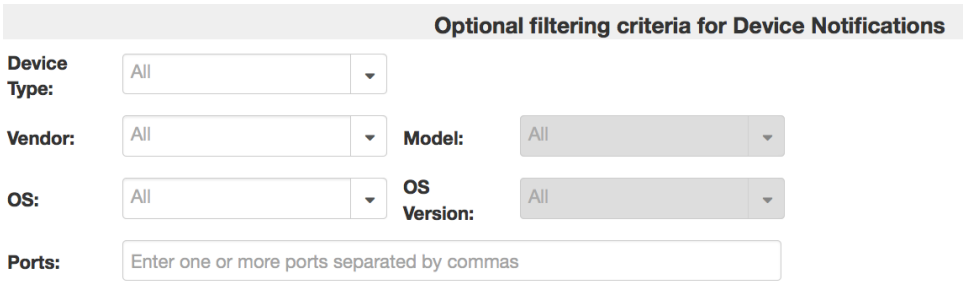
1. Log in the Command-Line Interface (CLI).
   a. Open a host or server that supports SSH.
   b. At the prompt, type **ssh admin@*<yourservername>*** and press **Enter**.
   c. Enter your password (i.e., **admin**) and press **Enter**.
2. At the command prompt, type
   log cefserver <***enable/disable***> <***protocol***> <***IP address***> <***port number***> and press **Enter**.

   a. **Protocol:** Type TCP-IPv4, UDP-IPv4, TCP-IPv6, UDP-IPv6
   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 QRadar console.

Configuring CEF-Formatted Syslog Output

1. On the CEF Notifications tab, click the tab for the type of CEF Notifications you want to display: 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 receive 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:



Note: Filtering does not affect the exporting of notifications. Unfiltered data exports.

CEF Output

Header Syntax
<sysloghеader> 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 to qRadar Property Mapping

A CEF Event generated from Lumeta will have its fields separated by a | and will look as follows:

```
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=
```

Mapping of CEF Event fields to qRadar Properties is defined in the table below:

QRadar Property	DataType	Lumeta Event Attribute	Value from Above Example
Device Vendor	static word: Lumeta	Name of Company	Lumeta
Device Product	static word: Lumeta	Name of Product	Lumeta
Device Version	Real Number	Version of Product	3.2.4
Event ID	String or integer	Notification Type	DEVICE_DISCOVERED
Event Name	String	NotificationName/NotificationType	Device Discovered
Severity	Integer	1, 5, 10	5
Event Category	String	DISCOVERY("/discovery"), SYSTEM("/system"), CONFIG("/config")	DISCOVERY
	MAC Address	mac address associated with the event	
	IPV4 Address	IP Address asscociated with the event	
Log Source Time	TimeStamp	Event generation time	Nov 02 2017 13:19:55
Hostname (custom)	String	Lumeta CC System Name	CCM-AMC
dhost	String	Host associated with the event	c6a3
c6a3	IPv6	IP associated with the event	
suser	String	User name associated with the event	
cn1	Long	Zone ID of the event	1
cn1Label	String	Zone Name of the event	Facility Zone1

Message (custom)	String	Event generated	

Events Generated by Lumeta

The following events are generated by Lumeta and have been added as Event Mapping in qRadar:

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 occured 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