Syslogs and Traps

SL1 version 11.2.0

Table of Contents

Chapter

1

Introduction to Syslogs and Traps

Overview

This manual describes how Syslog and SNMP Trap messages are processed by SL1 appliances that perform Message Collection.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all the menu options, click the Advanced menu icon (⋯).

This chapter includes the following topics:

Appliances that Process Syslog and SNMP Trap Messages

In SL1, three types of Appliances can process Syslog and SNMP Trap messages from monitored devices. The following appliances can perform the Message Collection function:

- All-In-One Appliances
- Message Collectors
- Data Collectors

NOTE: A Data Collector can perform Message Collection only if that Data Collector is in a Collector Group that contains no other Data Collectors

For more information about SL1 appliances functions and architecture, see the ***Architecture*** manual.

For information on how to create a collector group, see the ***System Administration*** manual.

Multi-byte Character Support

SL1 supports inbound syslog and SNMP trap messages that include multi-byte characters. Multi-byte characters can be displayed in the following pages:

- The **Event Console** page (**[Events]** tab) can display multi-byte characters in syslog and SNMP trap event messages.
- The **Device Logs** page (**[Logs]** tab under the Device Administration panel and the Device Reports panel) can display multi-byte characters in syslog and SNMP trap log messages.
- The ***Ticket Description*** and ***Ticket Notes*** fields in the **Ticket Editor** page can display BMP characters populated from an event message by an automation action. SMP characters are not supported in these fields.

Multi-byte characters can be included in the following fields and functions:

- Outbound SNMP Trap messages generated by the automation engine can now include an event message that contains multi-byte characters.
- Multi-byte characters can be included in the ***Event Message***, ***First Match***, ***Second Match***, and ***Identifier Pattern*** fields in the **Event Policy Editor** page.
- Multi-byte characters can be included in the ***Varbind OID Pattern*** field in an SNMP Trap Filter (Registry > Events > SNMP Trap Filters).
- Multi-byte characters can be included in the ***Expression Match*** field in a Redirect Policy (**[Redirects]** tab under the Device Administration panel).

Chapter 2

SNMP Traps

Overview

This chapter describes how SL1 handles SNMP traps.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all the menu options, click the Advanced menu icon (•••).

This chapter includes the following topics:

What Happens When a Message Collector Receives an SNMP Trap

When an appliance that performs Message Collection receives an SNMP Trap, it performs the following:

1. If the trap matches a defined filter, the trap is discarded. See ***Filtering Traps***.
2. Matches the IP address of the sender to an IP address of a device monitored by a collector group that includes the Appliance.
    - If the IP address of the sender does not match an IP address of a device monitored by a collector group that includes the Appliance, the message is discarded and a log message is generated. See ***Traps From Unknown Devices***.
3. Using the MIBs compiled on the SL1 system, translates varbind OIDs to symbolic values.

> NOTE: By default, Message Collectors and Data Collectors are not populated with information about all varbind OIDs. The first time a Message Collector or Data Collector attempts to translate a specific varbind OID, that varbind OID will not be translated, but information about that varbind OID will be added to theMessage Collector or Data Collector. All instances of a varbind OID after the first will then be translated correctly. To make SL1 translate the first occurrence of a varbind OID correctly, you can manually run a process that pre-populates Message Collectors and Data Collectors with information about all varbind OIDs. For steps on how to run this process, see the ***Manually Updating Varbind OIDs***.

4. Compares the trap to the defined trap event policies:
    - If the trap does not match an event policy, the trap is logged in the Device Logs for the device that sent the trap. See ***Traps That Do Not Match Event Policies***.
    - If the trap does match an event policy, the Source Host Varbind value for the event policy is evaluated. If the Source Host Varbind value matches a varbind OID in the trap, and the value of the varbind matches an IP address or hostname of a device monitored by a collector group that includes the Message Collector, the event is generated and aligned with the device with that IP address or hostname.
    - If the trap does match an event policy and is not realigned using the Source Host Varbind value, the event is generated and aligned with the device the trap was matched with in step two.

> NOTE: By default, the event policy "Trap: Unknown trap received" is enabled. This event policy matches all traps that do not match other event policies.

For more information on Trap events, see the ***Events*** manual.

Traps That Do Not Match Event Policies

If an Appliance that performs Message Collection receives a trap that:

- Is from a device that is monitored by a collector group that includes the Message Collector.
- Does not generate an event.

SL1 will log the receipt of the trap in the device logs for the device. If SL1 includes a compiled MIB that contains OIDs used in the received trap, SL1 will include the symbolic translation of those OIDs in the log message. The Device Log will have the following format:

```
Trap Received | Trap Detail: varbind OID or symbolic translation: varbind data type:
varbind data; (Trap OID: trap OID)
```

NOTE: Device Logs that are not associated with an Event are retrieved from Collection Units at five-minute intervals. It may take up to five minutes for traps that do not match event policies to appear in the Device Logs.

Traps From Unknown Devices

If an Appliance that performs Message Collection receives a trap from an unknown device, a "From unknown device: <*ip-address-of-unknown-device*>, received the following Trap message:" event will be generated. An unknown device is defined as either:

- A device monitored by the SL1 system, but by a collector group that does not include the Appliance.
- A device not monitored by the SL1 system.

The "From unknown device: <*ip-address-of-unknown-device*>, received the following Trap message:" event will appear in the Event Console page associated with the System organization.

For the first trap received from an unknown device, the event will have a Severity value of "Notice". If multiple traps are received from the same unknown device, additional events will be generated at the following thresholds:

- ***10, 25 Traps Received***. Severity value of "Minor".
- ***100 Traps Received, and every 100 traps up to and including 900 Traps Received***. Severity value of "Minor".
- ***1,000 Traps Received, and every 1,000 traps up to and including 9,000 Traps Received***. Severity value of "Minor".
- ***10,000 Traps Received, and every 10,000 traps received thereafter***. Severity value of "Major".

NOTE: The counters for the number of traps received from unknown devices will be reset to zero if the Event Engine on the Appliance that performs Message Collection is restarted, or the Appliance is restarted.

NOTE: The default threshold for incoming traps is set to 25 messages per second to prevent degraded performance.

Filtering Traps

In some situations, you might want to filter or limit the traps that are processed by SL1. SNMP Trap Filters allow you to define policies that filter incoming traps to an Appliance that performs Message Collection. When a trap is filtered, the Appliance that performs Message Collection receives the trap, but does not store the trap, does not act on the trap, and does not pass the trap on to be examined by the ScienceLogic event engine.

You can filter incoming SNMP traps using one, multiple, or all of the following parameters:

- IP or hostname of the host that sent the trap. You can also specify "all hosts"
- Trap OID
- Varbind OID
- Varbind content

So you can:

- Filter all incoming traps from a specific host.
- Filter incoming traps with a specific trap OID from all hosts.
- Filter incoming traps with a specific trap OID and from a specific host.
- Filter traps with a specific trap OID and specific varbind OID from all hosts.
- Filter traps with a specific trap OID and specific varbind OID from a specific host.

Global Settings that Affect SNMP Trap Processing

The following global setting affects how SL1 processes SNMP traps:

- ***use_v1trap_envelope_addr***. In environments where Network Address Translation is performed on SNMP v1 trap messages sent to SL1, you can configure SL1 to read the envelope address (the address of the host sending the trap) instead of the agent address (the IP address variable sent as part of the trap). To use the envelope address instead of the agent address for SNMP v1 trap messages, the *use_v1trap_envelope_addr=1* configuration option can be added to the [LOCAL] section of silo.conf on Message Collectors, Data Collectors that perform message collection, and All-In-One Appliances. If *use_v1trap_envelope_addr* is not defined in silo.conf or *use_v1trap_envelope_addr=0* is defined, SL1 will use the agent address for SNMP v1 trap messages.

To add a settings to the silo.conf file on an appliance:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Login as user ***em7admin*** with the password you configured during setup.
3. At the shell prompt, enter the following:

   ```
   sudo visilo
   ```

4. On a line of its own, add the new entry.
5. Save your changes and exit the file (:wq).

System Settings that Affect SNMP Trap Processing

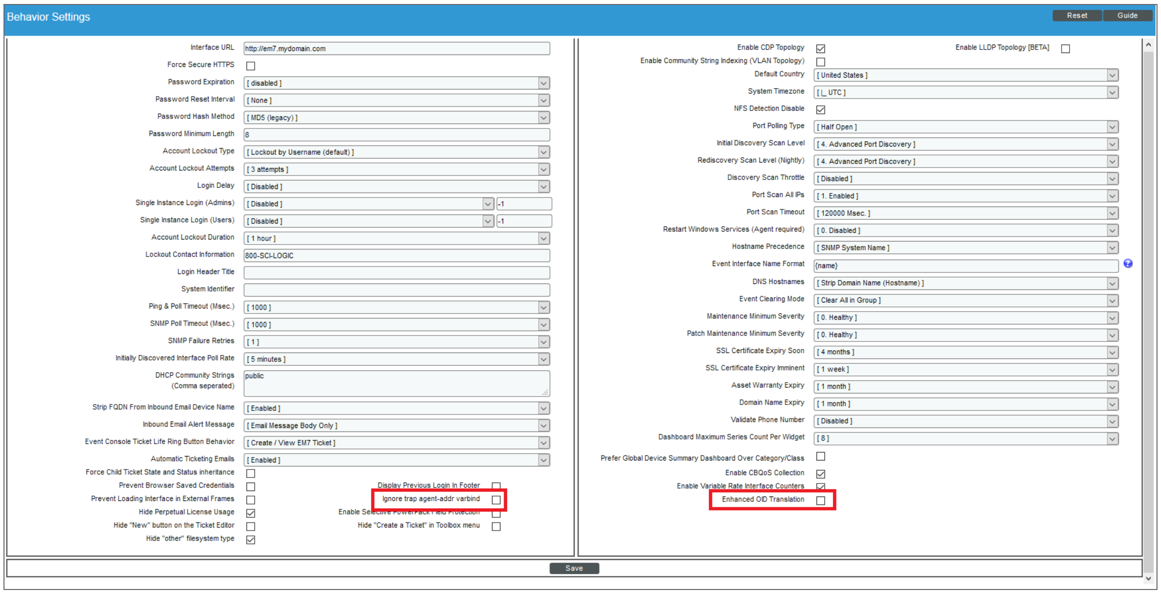
The following system setting affects how SL1 processes SNMP traps:

- ***Ignore trap agent-addr varbind***. If you select this checkbox, SL1 will align the SNMP trap with the forwarder (last hop) instead of searching for the IP address of the originator of the trap.
- ***Enhanced OID Translation***. If selected, ensures that varbind OIDs that use multi-dimensional indexes are translated correctly. The symbolic translation of the known portion of the OID is included in the log message associated with the trap.

NOTE: Enabling the ***Enhanced OID Translation*** option might affect performance on large environments with a large number of traps.

To enable these settings:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Select the checkbox next to the setting or settings you want to enable:



Interface URL: http://em7.mydomain.com
Force Secure HTTPS ☐
Password Expiration: [disabled]
Password Reset Interval: [None]
Password Hash Method: [MD5 (legacy)]
Password Minimum Length: 8
Account Lockout Type: [Lockout by Username (default)]
Account Lockout Attempts: [3 attempts]
Login Delay: [Disabled]
Single Instance Login (Admins): [Disabled] -1
Single Instance Login (Users): [Disabled] -1
Account Lockout Duration: [1 hour]
Lockout Contact Information: 800-SCI-LOGIC
Login Header Title:
System Identifier:
Ping & Poll Timeout (Msec.): [1000]
SNMP Poll Timeout (Msec.): [1000]
SNMP Failure Retries: [1]
Initially Discovered Interface Poll Rate: [5 minutes]
DHCP Community Strings (Comma seperated): public
Strip FQDN From Inbound Email Device Name: [Enabled]
Inbound Email Alert Message: [Email Message Body Only]
Event Console Ticket Life Ring Button Behavior: [Create / View EM7 Ticket]
Automatic Ticketing Emails: [Enabled]
Force Child Ticket State and Status inheritance ☐
Prevent Browser Saved Credentials ☐
Prevent Loading Interface in External Frames ☐
Hide Perpetual License Usage ☑
Hide "New" button on the Ticket Editor ☐
Hide "other" filesystem type ☑
Display Previous Login In Footer ☐
Ignore trap agent-addr varbind ☐
Enable Selective PowerPack Field Protection ☐
Hide "Create a Ticket" in Toolbox menu ☐

Enable CDP Topology ☑
Enable LLDP Topology [BETA] ☐
Enable Community String Indexing (VLAN Topology) ☐
Default Country: [United States]
System Timezone: [L_ UTC]
NFS Detection Disable ☑
Port Polling Type: [Half Open]
Initial Discovery Scan Level: [4. Advanced Port Discovery]
Rediscovery Scan Level (Nightly): [4. Advanced Port Discovery]
Discovery Scan Throttle: [Disabled]
Port Scan All IPs: [1. Enabled]
Port Scan Timeout: [120000 Msec.]
Restart Windows Services (Agent required): [0. Disabled]
Hostname Precedence: [SNMP System Name]
Event Interface Name Format: {name}
DNS Hostnames: [Strip Domain Name (Hostname)]
Event Clearing Mode: [Clear All in Group]
Maintenance Minimum Severity: [0. Healthy]
Patch Maintenance Minimum Severity: [0. Healthy]
SSL Certificate Expiry Soon: [4 months]
SSL Certificate Expiry Imminent: [1 week]
Asset Warranty Expiry: [1 month]
Domain Name Expiry: [1 month]
Validate Phone Number: [Disabled]
Dashboard Maximum Series Count Per Widget: [8]
Prefer Global Device Summary Dashboard Over Category/Class ☐
Enable CBQoS Collection ☑
Enable Variable Rate Interface Counters ☑
Enhanced OID Translation ☐

3. Click **[Save]** to save the settings.

Manually Updating Varbind OIDs

By default, Message Collectors and Data Collectors are not populated with information about all varbind OIDs. The first time a Message Collector or Data Collector attempts to translate a specific varbind OID, that varbind OID will not be translated, but information about that varbind OID will be added to the Message Collector or Data Collector. All instances of a varbind OID after the first will then be translated correctly.

To make SL1 translate the first occurrence of a varbind OID correctly, you can manually run a process that pre-populates Message Collectors and Data Collectors with information about all varbind OIDs. You should run this process after adding new MIBs to SL1.

To manually populates Message Collectors and Data Collectors with information about all varbind OIDs, perform the following steps:

1. Go to the **OID Browser** page (System > Tools > OID Browser).
2. Select the **[Update]** button.

Configuring SNMPv3 Traps

To configure a Message Collector or Data Collector to accept an SNMPv3 trap or inform, SL1 automatically configures the trap configuration file on the Message Collector or Data Collector. SL1 automatically populates the SNMPv3 trap and inform credentials including the engine ID of the recipient, the Message Collector or Data Collector.

To configure an SNMPv3 Trap:

1. Go to the **Credentials** page (Manage > Credentials.
2. Click the **SNMPv3 Trap Configuration Reset** icon (🔄).
3. SL1 automatically configures the etc/snmptrapd.con file to receive SNMPv3 traps from all monitored devices.

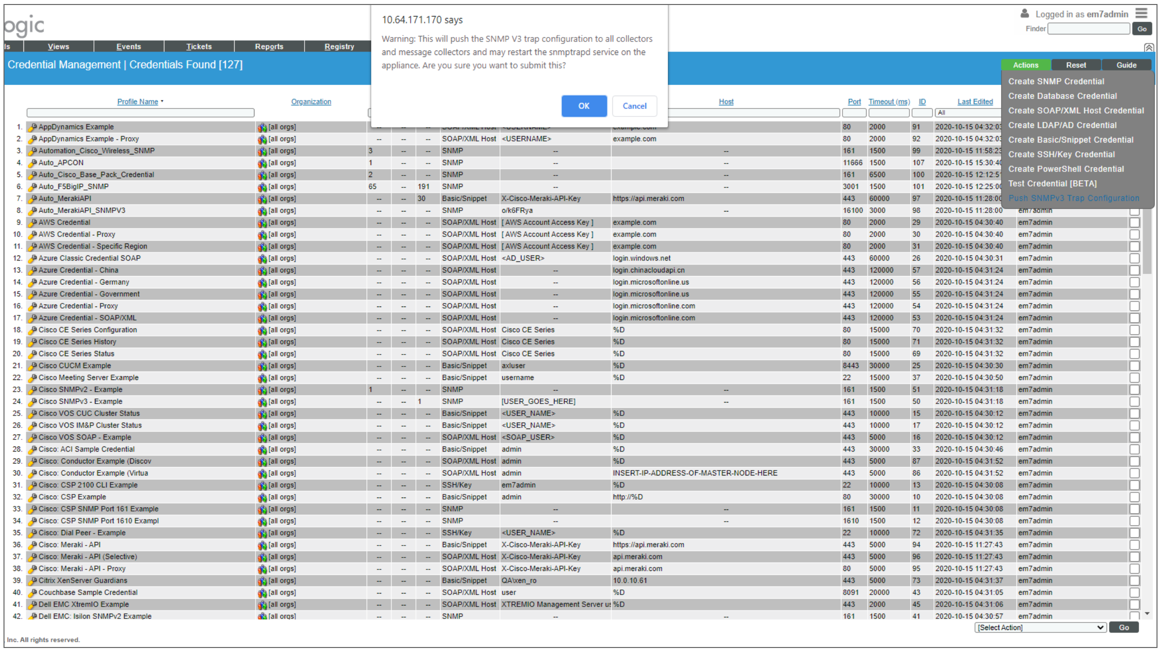
Configuring SNMPv3 Traps in the Classic User Interface

To configure an SNMPv3 Trap in the classic SL1 user interface:

1. Go to the Credential Management page (System > Manage > Credentials).

2. Click the **Actions** button and then select *Push SNMPv3 Trap Configuration*.

3. A warning message appears: "Warning: This will push the SNMP V3 trap configuration to all collectors and message collectors and restart the snmptrapd service on the appliance. Are you sure you want to submit this?"



ogic
ls
Views
Events
Tickets
Reports
Registry
Logged in as em7admin
Finder
Go
Actions
Reset
Guide
Create SNMP Credential
Create Database Credential
Create SOAP/XML Host Credential
Create LDAP/AD Credential
Create Basic/Snippet Credential
Create SSH/Key Credential
Create PowerShell Credential
Test Credential [BETA]
Push SNMPv3 Trap Configuration
OK
Cancel
[Select Action]
Go
Inc. All rights reserved.

10.64.171.170 says

Warning: This will push the SNMP V3 trap configuration to all collectors and message collectors and may restart the snmptrapd service on the appliance. Are you sure you want to submit this?

Credential Management | Credentials Found [127]

	Profile Name	Organization						Host	Port	Timeout (ms)	ID	Last Edited		
												All		
1.	AppDynamics Example	[all orgs]	--	--	--	SOAP/XML Host	<USERNAME>	example.com	80	2000	91	2020-10-15 04:32:03		
2.	AppDynamics Example - Proxy	[all orgs]	--	--	--	SOAP/XML Host	<USERNAME>	example.com	80	2000	92	2020-10-15 04:32:03		
3.	Automation_Cisco_Wireless_SNMP	[all orgs]	3	--	--	SNMP	--	--	161	1500	99	2020-10-15 11:58:23		
4.	Auto_APCON	[all orgs]	1	--	--	SNMP	--	--	11666	1500	107	2020-10-15 15:30:40		
5.	Auto_Cisco_Base_Pack_Credential	[all orgs]	2	--	--	SNMP	--	--	161	6500	100	2020-10-15 12:12:51		
6.	Auto_F5BigIP_SNMP	[all orgs]	65	--	191	SNMP	--	--	3001	1500	101	2020-10-15 12:25:00		
7.	Auto_MerakiAPI	[all orgs]	--	--	30	Basic/Snippet	X-Cisco-Meraki-API-Key	https://api.meraki.com	443	60000	97	2020-10-15 11:28:00		
8.	Auto_MerakiAPI_SNMPV3	[all orgs]	--	--	--	SNMP	o/k6FRya	--	16100	3000	98	2020-10-15 11:28:00	em7admin	□
9.	AWS Credential	[all orgs]	--	--	--	SOAP/XML Host	[AWS Account Access Key]	example.com	80	2000	29	2020-10-15 04:30:40	em7admin	□
10.	AWS Credential - Proxy	[all orgs]	--	--	--	SOAP/XML Host	[AWS Account Access Key]	example.com	80	2000	30	2020-10-15 04:30:40	em7admin	□
11.	AWS Credential - Specific Region	[all orgs]	--	--	--	SOAP/XML Host	[AWS Account Access Key]	example.com	80	2000	31	2020-10-15 04:30:40	em7admin	□
12.	Azure Classic Credential SOAP	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	26	2020-10-15 04:30:31	em7admin	□
13.	Azure Credential - China	[all orgs]	--	--	--	SOAP/XML Host	--	login.chinacloudapi.cn	443	120000	57	2020-10-15 04:31:24	em7admin	□
14.	Azure Credential - Germany	[all orgs]	--	--	--	SOAP/XML Host	--	login.microsoftonline.us	443	120000	56	2020-10-15 04:31:24	em7admin	□
15.	Azure Credential - Government	[all orgs]	--	--	--	SOAP/XML Host	--	login.microsoftonline.us	443	120000	55	2020-10-15 04:31:24	em7admin	□
16.	Azure Credential - Proxy	[all orgs]	--	--	--	SOAP/XML Host	--	login.microsoftonline.com	443	120000	54	2020-10-15 04:31:24	em7admin	□
17.	Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	--	login.microsoftonline.com	443	120000	53	2020-10-15 04:31:24	em7admin	□
18.	Cisco CE Series Configuration	[all orgs]	--	--	--	SOAP/XML Host	Cisco CE Series	%D	80	15000	70	2020-10-15 04:31:32	em7admin	□
19.	Cisco CE Series History	[all orgs]	--	--	--	SOAP/XML Host	Cisco CE Series	%D	80	15000	71	2020-10-15 04:31:32	em7admin	□
20.	Cisco CE Series Status	[all orgs]	--	--	--	SOAP/XML Host	Cisco CE Series	%D	80	15000	69	2020-10-15 04:31:32	em7admin	□
21.	Cisco CUCM Example	[all orgs]	--	--	--	Basic/Snippet	axluser	%D	8443	30000	25	2020-10-15 04:30:30	em7admin	□
22.	Cisco Meeting Server Example	[all orgs]	--	--	--	Basic/Snippet	username	%D	22	15000	37	2020-10-15 04:30:50	em7admin	□
23.	Cisco SNMPv2 - Example	[all orgs]	1	--	--	SNMP	--	--	161	1500	51	2020-10-15 04:31:18	em7admin	□
24.	Cisco SNMPv3 - Example	[all orgs]	--	--	1	SNMP	[USER_GOES_HERE]	--	161	1500	50	2020-10-15 04:31:18	em7admin	□
25.	Cisco VOS CUC Cluster Status	[all orgs]	--	--	--	Basic/Snippet	<USER_NAME>	%D	443	10000	15	2020-10-15 04:30:12	em7admin	□
26.	Cisco VOS IM&P Cluster Status	[all orgs]	--	--	--	Basic/Snippet	<USER_NAME>	%D	443	10000	17	2020-10-15 04:30:12	em7admin	□
27.	Cisco VOS SOAP - Example	[all orgs]	--	--	--	SOAP/XML Host	<SOAP_USER>	%D	443	5000	16	2020-10-15 04:30:12	em7admin	□
28.	Cisco: ACI Sample Credential	[all orgs]	--	--	--	Basic/Snippet	admin	%D	443	30000	33	2020-10-15 04:30:46	em7admin	□
29.	Cisco: Conductor Example (Discov	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	443	5000	87	2020-10-15 04:31:52	em7admin	□
30.	Cisco: Conductor Example (Virtua	[all orgs]	--	--	--	SOAP/XML Host	admin	INSERT-IP-ADDRESS-OF-MASTER-NODE-HERE	443	5000	86	2020-10-15 04:31:52	em7admin	□
31.	Cisco: CSP 2100 CLI Example	[all orgs]	--	--	--	SSH/Key	em7admin	%D	22	10000	13	2020-10-15 04:30:08	em7admin	□
32.	Cisco: CSP Example	[all orgs]	--	--	--	Basic/Snippet	admin	http://%D	80	30000	10	2020-10-15 04:30:08	em7admin	□
33.	Cisco: CSP SNMP Port 161 Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	11	2020-10-15 04:30:08	em7admin	□
34.	Cisco: CSP SNMP Port 1610 Exampl	[all orgs]	--	--	--	SNMP	--	--	1610	1500	12	2020-10-15 04:30:08	em7admin	□
35.	Cisco: Dial Peer - Example	[all orgs]	--	--	--	SSH/Key	<USER_NAME>	%D	22	10000	72	2020-10-15 04:31:35	em7admin	□
36.	Cisco: Meraki - API	[all orgs]	--	--	--	Basic/Snippet	X-Cisco-Meraki-API-Key	https://api.meraki.com	443	5000	94	2020-10-15 11:27:43	em7admin	□
37.	Cisco: Meraki - API (Selective)	[all orgs]	--	--	--	SOAP/XML Host	X-Cisco-Meraki-API-Key	api.meraki.com	443	5000	96	2020-10-15 11:27:43	em7admin	□
38.	Cisco: Meraki - API - Proxy	[all orgs]	--	--	--	SOAP/XML Host	X-Cisco-Meraki-API-Key	api.meraki.com	80	5000	95	2020-10-15 11:27:43	em7admin	□
39.	Citrix XenServer Guardians	[all orgs]	--	--	--	Basic/Snippet	QA\xen_ro	10.0.10.61	443	5000	73	2020-10-15 04:31:37	em7admin	□
40.	Couchbase Sample Credential	[all orgs]	--	--	--	SOAP/XML Host	user	%D	8091	20000	43	2020-10-15 04:31:05	em7admin	□
41.	Dell EMC XtremIO Example	[all orgs]	--	--	--	SOAP/XML Host	XTREMIO Management Server us	%D	443	2000	45	2020-10-15 04:31:06	em7admin	□
42.	Dell EMC: Isilon SNMPv2 Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	41	2020-10-15 04:30:57	em7admin	□

4. Click **OK**. SL1 automatically configures the etc/snmptrapd.con file to receive SNMPv3 traps from all monitored devices.

Manually Configuring SNMPv3 Traps

NOTE: These steps are no longer required in SL1 systems later than 8.14.9 or 10.1.4

To configure a Message Collector or Data Collector to accept an SNMPv3 trap or inform, you must edit the trap configuration file on the Message Collector or Data Collector. In the trap configuration file, enter the credentials that allow SL1 to communicate with the device that sends traps to SL1. Enter credentials for each device that sends traps to SL1. This information is configured in a configuration file at the operating-system level.

For SNMPv3 traps, the credential entry must include the engine ID of the device sending the trap. Therefore, there will be an entry in the trap configuration for each device that will send SNMPv3 traps. For SNMPv3 informs, the entry does not need to specify the engine ID. The engine ID of the recipient, the Message Collectoror Data Collector, is used for SNMPv3 informs. Therefore, if all the managed devices use the same credentials to send SNMPv3 informs, you need to add only one entry to the trap configuration file.

> **NOTE**: Existing trap event policies will be triggered by SNMPv3 traps and SNMPv3 informs with no additional configuration.

To add a credential entry to the trap configuration file:

1. Either go to the console of the the Message Collector or Data Collector or use SSH to access the server.
2. Log in as user ***em7admin*** with the appropriate password.
3. Open the /etc/snmp/snmptrapd.conf file in a text editor.
4. At the end of the file, add a new "createUser" line. See the section below for the appropriate syntax.
5. Save the file.
6. Restart the trap engine by executing the following command:

   ```
   sudo service snmptrapd restart
   ```

The syntax of createUser is different for each security level and whether you are configuring traps or informs:

- Informs, no authentication, no encryption (noAuthNoPriv):

  ```
  createUser <security name>
  ```

  For example:

  ```
  createUser em7defaultv3
  ```

- Informs, authentication, no encryption (authNoPriv):

  ```
  createUser <security name> <auth protocol> <security passphrase>
  ```

  For example:

  ```
  createUser em7defaultv3 SHA em7authpass
  ```

> NOTE: For FIPS-compliant systems, authentication with MD5 will fail.

- Informs, authentication and encryption (authPriv):

```
createUser <security name> <auth protocol> <security passphrase> <privacy
protocol> <privacy pass phrase>
```

For example:

```
createUser em7defaultv3 SHA em7authpass DES em7privpass
```

- Traps, no authentication, no encryption (noAuthNoPriv):

```
createUser -e <engine ID> <security name>
```

For example:

```
createUser -e 0x0102030405 em7defaultv3
```

- Traps, authentication, no encryption (authNoPriv):

```
createUser -e <engine ID> <security name> <auth protocol> <security
passphrase>
```

For example:

```
createUser -e 0x0102030405 em7defaultv3 SHA em7authpass
```

- Traps, authentication and encryption (authPriv):

```
createUser -e <engine ID> <security name> <auth protocol> <security
passphrase> <privacy protocol> <privacy pass phrase>
```

For example:

```
createUser -e 0x0102030405 em7defaultv3 SHA em7authpass DES em7privpass
```

Here are some example commands for how to send a test coldStart trap from a SL1 appliance using authPriv and the credential information from the examples above:

```
snmptrap -e 0x0102030405 -v3 -u em7defaultv3 -a SHA -A em7authpass -x DES -X
em7privpass <message collector ip> 0 .1.3.6.1.6.3.1.1.5.1
```

```
snmpinform -v3 -u em7defaultv3 -a SHA -A em7authpass -x DES -X em7privpass <message
collector ip> 0 .1.3.6.1.6.3.1.1.5.1
```

Chapter

3

Syslog Messages

Overview

When an Appliance that performs Message Collection receives a Syslog message, it performs the following:

1. Matches the IP address of the sender to an IP address of a device monitored by a collector group that includes the Appliance.
    - If the IP address of the sender does not match an IP address of a device monitored by a collector group that includes the Appliance, the message is discarded and an event is generated. See *Syslogs From Unknown Devices*.
2. Compares the syslog to the defined syslog event policies:
    - If the syslog does not match an event policy, the syslog is logged in the Device Logs for the device that sent the syslog. See *Syslogs That Do Not Match Event Policies*.
    - If the syslog matches an event policy, the event is generated. The generated event is aligned with the device the syslog was matched with in step 1.

For more information on syslog events, see the *Events* manual.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all the menu options, click the Advanced menu icon (⋯).

This chapter includes the following topics:

Syslogs That Do Not Match Event Policies

If an Appliance that performs Message Collection receives a syslog that:

- Is from a device that is monitored by a collection group that includes the Appliance.
- Does not generate an event.

SL1 will log the receipt of the syslog in the device logs for the device. The message field for the Device Log will be the same as the syslog message field.

NOTE: Device Logs that are not associated with an Event are retrieved from Collection Units at five-minute intervals. It may take up to five minutes for syslogs that do not match event policies to appear in the Device Logs.

Syslogs From Unknown Devices

If an Appliance the performs Message Collection receives a syslog from an unknown device, a "From unknown device: <*ip-address-of-unknown-device*>, received the following syslog message:" event will be generated. An unknown device is defined as either:

- A device monitored by the SL1 system, but by a collector group that does not include the Appliance.
- A device not monitored by the SL1 system.

The "From unknown device: <*ip-address-of-unknown-device*>, received the following syslog message:" event will appear in the **Event Console** page associated with the System organization.

For the first syslog received from an unknown device, the message will have a Severity value of "Notice". If multiple syslogs are received from different unknown devices, additional events will be generated at the following thresholds:

- ***10, 25 Syslogs Received***. Severity value of "Minor".
- ***100 Syslogs Received, and every 100 syslogs up to and including 900 Syslogs Received***. Severity value of "Minor".
- ***1,000 Syslogs Received, and every 1,000 syslogs up to and including 9,000 Syslogs Received***. Severity value of "Minor".
- ***10,000 Syslogs Received, and every 10,000 syslogs received thereafter***. Severity value of "Major".

NOTE: Multiple messages received from the same unknown device will not increase the event count of syslog messages received or the event severity.

NOTE: The counters for the number of syslogs received from unknown devices will be reset to zero if the Event Engine on an Appliance that performs Message Collection is restarted, or the Appliance is restarted.

NOTE: The default threshold for incoming syslogs is set to 25 messages per second to prevent degraded performance.

Chapter 4

IP Address Conflicts

Overview

This chapter describes how SL1 handles IP address conflicts.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all the menu options, click the Advanced menu icon (•••).

This chapter includes the following topics:

IP Addresses Associated with Devices

There are three types of IP addresses that can be associated with a device:

- ***Admin Primary***. This is the IP address that SL1 used to discover a device, and is used by Data Collectors to communicate with a device. This IP address is always the ***Admin Primary*** address and cannot be demoted to a secondary address.
- ***Primary***. One or more IP addresses that SL1 uses to match incoming syslog an trap messages with a device.
- ***Secondary***. SL1 gathers information about this IP address, but does not use this IP address to communicate with the device or match incoming syslog or trap messages with a device.

SL1 will allow devices with the same admin primary IP address to be monitored; however, devices with the same admin primary IP address must be in separate collector groups. The admin primary IP address is the IP address SL1 uses to monitor a device, and is listed in the "IP Address" column in the **Device Manager** page (Registry > Devices > Device Manager).

A Message Collector can be aligned with multiple collector groups. Because Message Collectors can be included in multiple collection groups, it is possible for the IP address associated with a syslog or trap to match multiple devices.

This chapter describes how a Message Collector reports IP conflicts in this situation.

NOTE: The information in this chapter does not apply to Data Collectors and All-In-One Appliances because Data Collectors and All-In-One Appliances can be in only one Collector Group.

IP Conflict Events

For each Message Collector, daily maintenance compares the IP addresses for all devices monitored by the collector groups that include the Message Collector. If the daily maintenance task finds duplicate admin primary IP addresses, SL1 generates the following event, with a default severity of major:

```
Primary IP address overlap on devices managed by Message Collector: <appliance-id-
of-message-collection-unit> | Collector Groups: <id-of-collector-groups> | IP
Address: <duplicate-ip-address> | Device IDs: <device-ids-using-ip-address>
```

If the daily maintenance task finds duplicate secondary IP addresses, SL1 generates the following event, with a default severity of minor:

```
Secondary IP address overlap on devices managed by Message Collector: <appliance-id-
of-message-collection-unit> | Collector Groups: <id-of-collector-groups> | IP
Address: <duplicate-ip-address> | Device IDs: <device-ids-using-ip-address>
```

When a Message Collector is:

- Aligned with multiple collector groups
- Receives a syslog or trap from a primary IP address associated with multiple devices
- The IP address is associated with multiple devices, all of which are are monitored by the same collector group that contains the the Message Collector

SL1 generates the following event, with a default severity of minor:

```
Could not match asynchronous message to a device due to a primary IP address
ambiguity address: <duplicate-ip-address>
```

If a received syslog or trap triggers the address ambiguity event, and the Message Collector is discovered on the system, any events or logs generated by the syslog or trap are aligned with the Message Collector. If a received syslog or trap causes the address ambiguity event to be generated, and the Message Collector is not on the system, any events or logs generated by the syslog or trap are aligned with the System organization.

Resolving IP Conflicts

To prevent syslog and trap messages from aligning with the Message Collector or System organization because of an IP conflict, every device monitored by the same Message Collector must use a unique IP address to send syslog and trap messages. Even if these devices that share an IP address are in different collector groups, if the devices share one or more Message Collectors, the devices should use unique IP addresses to send syslog and trap messages.

By default, SL1 uses only the admin primary IP address to align syslog and trap messages to devices. If the admin primary IP address for a device is not unique, you can configure a secondary IP address for use as a primary IP address for message collection.

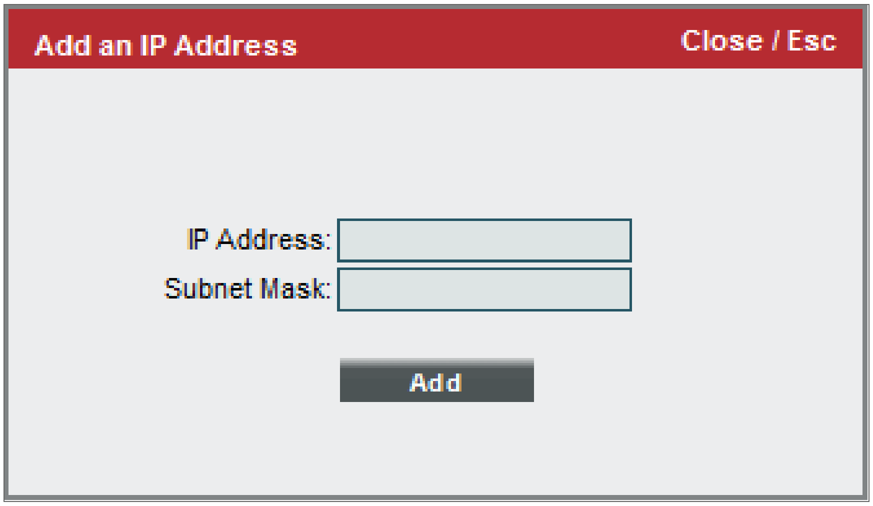
NOTE: Configuring a secondary IP address as a primary IP address for message collection will not affect any data collection performed byData Collectors. Data Collectors will always use the admin primary IP address when polling devices.

To configure a secondary IP address for a device as a primary IP address for message collection:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Select the wrench icon (🔧)for the device you want to configure. The **Device Properties** window will be displayed.

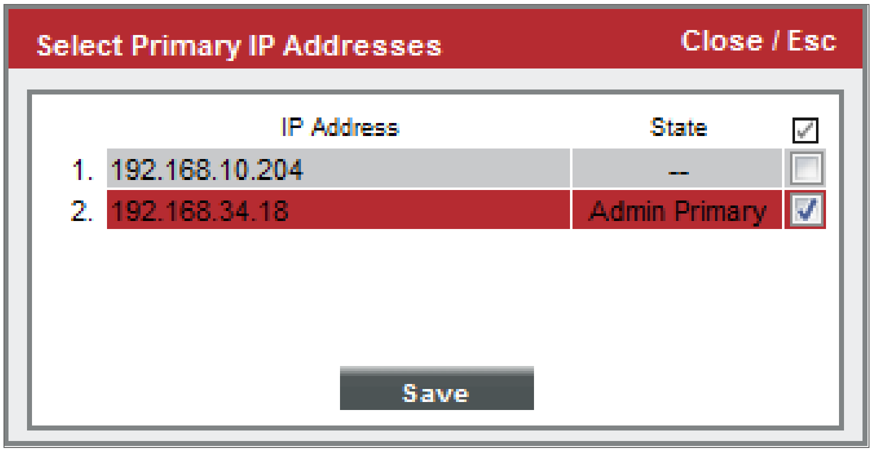
3. To check that SL1 has discovered the secondary IP address that you want to configure as the primary IP address for message collection, select the ***IP Address*** drop down list. If the secondary IP address is not displayed in the list of IP addresses, you can add it manually:

   - Select the plus icon to the right of the ***IP Address*** drop down list. The **Add IP Address** modal window is displayed:



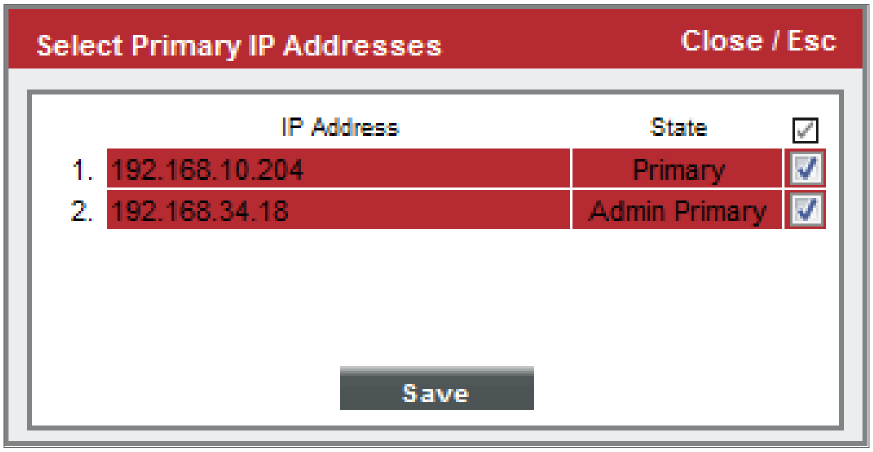
   - Enter the secondary IP address in the ***IP Address*** field.
   - Enter the subnet mask for the secondary IP address in the ***Subnet Mask*** field.
   - Select the **[Save]** button. The **Add IP Address** modal window will close and the message "Unverified IP Added to Device" is displayed.

4. From the **[Actions]** menu, select ***Select Primary IP Addresses***. The **Select Primary IP Addresses** modal window is displayed:



	IP Address	State	☑
1.	192.168.10.204	--	□
2.	192.168.34.18	Admin Primary	☑

5. Select the checkbox for the secondary IP address you want to configure as a primary IP address. Select the **[Save]** button. The *State* of the selected IP address is now "Primary":



	IP Address	State	☑
1.	192.168.10.204	Primary	☑
2.	192.168.34.18	Admin Primary	☑

NOTE: You cannot change the state of the admin primary address. If a listed IP address is already in use as an admin primary or primary IP address for another device in the same collector group, you cannot set it as a primary IP address and the checkbox will not be displayed. You can select multiple secondary IP addresses to set as primary addresses.

Chapter 5

Event Policies for Syslogs and Traps

Overview

This chapter describes how to set up Event Policies for events with a source of Syslog and Trap messages.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all the menu options, click the Advanced menu icon (⋯).

This chapter includes the following topics:

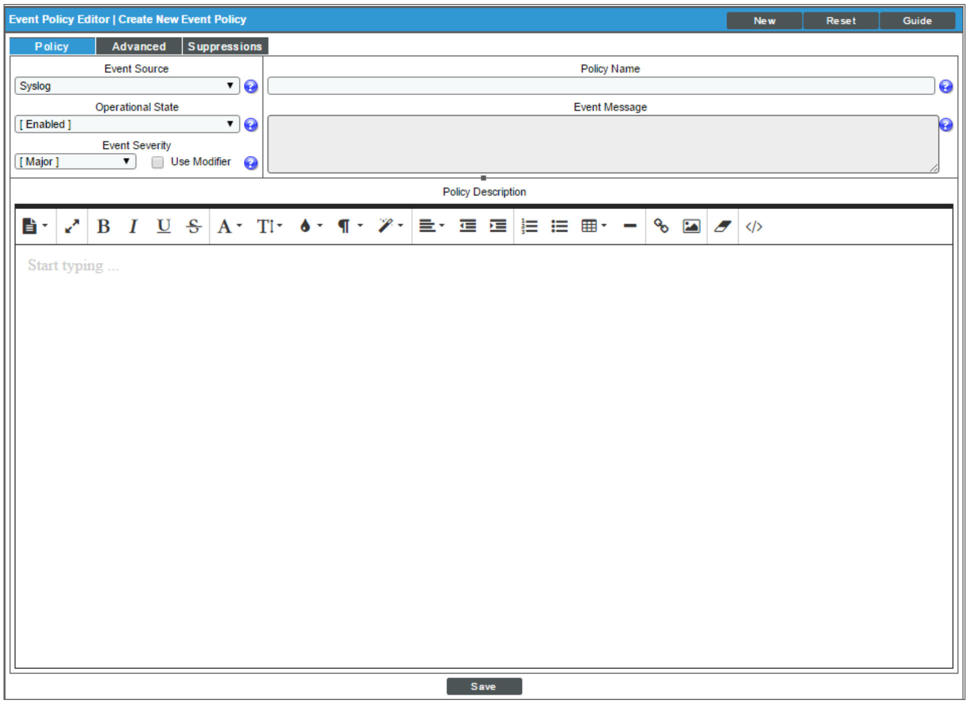
Creating a Trap Event Policy

SL1 includes pre-defined events for the most commonly encountered conditions on the most common platforms. However, if the pre-defined events do not meet the needs of your organization, you can define new events that better suit your needs.

From the **Event Policies** page (or the **Event Policy Manager** page in the classic SL1 user interface), you can define a new event. You can define custom events to meet your business requirements. You can also define events to be triggered by any custom Dynamic Application alerts you have created.

To create an event definition:

1. Go to **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, click the **[Create]** button. The **Event Policy Editor** page appears:



Event Policy Editor | Create New Event Policy

Event Source: Syslog

Operational State: [Enabled]

Event Severity: [Major] □ Use Modifier

Policy Name

Event Message

Policy Description

Start typing ...

3. In the **Event Policy Editor** page and set of tabs, you can define a new event. The **Event Policy Editor** page contains three tabs:

    - ***Policy***. Allows you to define basic parameters for the event. This tab is described in the following section.
    - ***Advanced***. Allows you to define pattern-matching for the event and also define event roll-ups and suppressions.

- ***Suppressions***. Allows you to suppress the event on selected devices. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event will not appear in the **Event Console** page or the **Viewing Events** page for the device.

4. Supply values in the following fields:

   - ***Event Source***. Select *Trap*.
   - ***Policy Name***. The name of the event. Can be any combination of alphanumeric characters, up to 48 characters in length.
   - ***Operational State***. Specifies whether event is to be operational or not. Choices are *Enabled* or *Disabled*.
   - ***Event Message***. The message that appears in the **Event Console** page or the **Viewing Events** page when this event occurs. Can be any combination of alphanumeric characters. Variables include the characters "%" (percent) and "|" (bar). You can also use regular expressions and variables that represent text from the original log message to create the ***Event Message***:

     - To include regular expressions in the Event Message:

       Surround the regular expression with %R and %/R. For example:

       %RFilename: .*? %/R

       Would search for the first instance of the string "Filename: " (Filename-colon-space) followed by any number of any characters up to the line break. The %R indicates the beginning of a regular expression. The %/R indicates the end of a regular expression.

       SL1 will use the regular expression to search the log message and use the matching text in the event message.

       For details on the regular expression syntax allowed by SL1, see http://www.python.org/doc/howto/.

     - You can also use the following variables in this field:

       - *%I* ("eye").This variable contains the value that matches the ***Identifier Pattern*** field in the **[Advanced]** tab.
       - *%M*. The full text of the log message that triggered the event will be displayed in ***Event Message*** field.
       - *%V*. Data Value from log file will be displayed in the ***Event Message*** field.
       - *%T*. Threshold value from the log file will be displayed in ***Event Message*** field.

   - ***Event Severity***. Defines the severity of the event. Choices are:

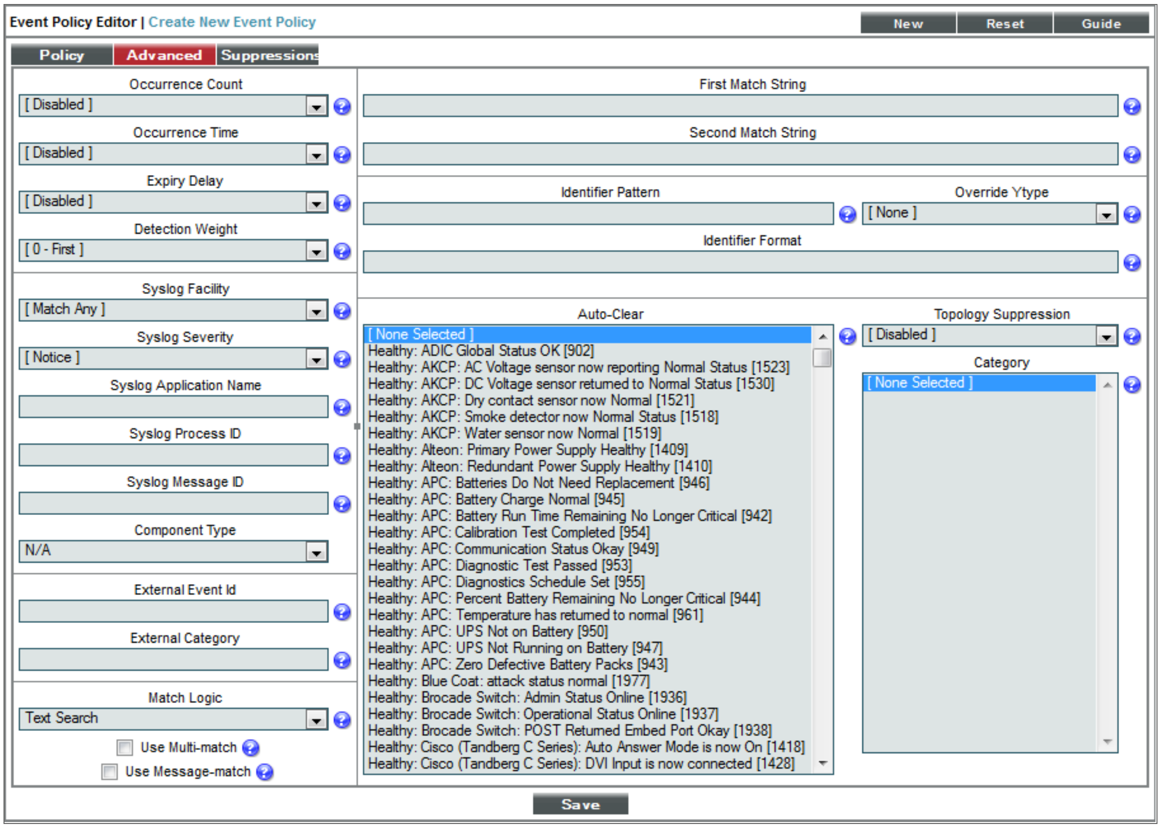
     - *Healthy*. Healthy Events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.
     - *Notice*. Notice Events indicate a condition that does not affect service but about which users should be aware.

- ○ *Minor*. Minor Events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
- ○ *Major*. Major Events indicate a condition that is service impacting and requires immediate investigation.
- ○ *Critical*. Critical Events indicate a condition that can seriously impair or curtail service and require immediate attention (i.e. service or system outages).

- ***Use Modifier***. If selected, when the event is triggered, SL1 will check to see if the interface associated with this event has a custom severity modifier. If so, the event will appear in the **Event Console** with that custom severity modifier applied to the severity in the ***Event Severity*** field. For example, if an interface with an ***Event Severity Adjust*** setting of *Sev -1* triggers an event with an ***Event Severity*** of *Major* and that event has the ***Use Modifier*** checkbox selected, the event will appear in the **Event Console** with a severity of *Minor*.
- ***Policy Description***. Text that explains what the event means and what possible causes are.

Defining Pattern Matching and Advanced Behavior

The **[Advanced]** tab in the **Event Policy Editor** page allows you to define or edit pattern-matching for the trap event and also define event roll-ups and suppressions. In the **[Advanced]** tab, you can define or edit the following fields that pertain to traps:



Occurrence Count: [Disabled]
Occurrence Time: [Disabled]
Expiry Delay: [Disabled]
Detection Weight: [0 - First]
Syslog Facility: [Match Any]
Syslog Severity: [Notice]
Syslog Application Name:
Syslog Process ID:
Syslog Message ID:
Component Type: N/A
External Event Id:
External Category:
Match Logic: Text Search
□ Use Multi-match
□ Use Message-match
First Match String:
Second Match String:
Identifier Pattern:
Override Ytype: [None]
Identifier Format:
Auto-Clear: [None Selected]
Topology Suppression: [Disabled]
Category: [None Selected]

[None Selected]
Healthy: ADIC Global Status OK [902]
Healthy: AKCP: AC Voltage sensor now reporting Normal Status [1523]
Healthy: AKCP: DC Voltage sensor returned to Normal Status [1530]
Healthy: AKCP: Dry contact sensor now Normal [1521]
Healthy: AKCP: Smoke detector now Normal Status [1518]
Healthy: AKCP: Water sensor now Normal [1519]
Healthy: Alteon: Primary Power Supply Healthy [1409]
Healthy: Alteon: Redundant Power Supply Healthy [1410]
Healthy: APC: Batteries Do Not Need Replacement [946]
Healthy: APC: Battery Charge Normal [945]
Healthy: APC: Battery Run Time Remaining No Longer Critical [942]
Healthy: APC: Calibration Test Completed [954]
Healthy: APC: Communication Status Okay [949]
Healthy: APC: Diagnostic Test Passed [953]
Healthy: APC: Diagnostics Schedule Set [955]
Healthy: APC: Percent Battery Remaining No Longer Critical [944]
Healthy: APC: Temperature has returned to normal [961]
Healthy: APC: UPS Not on Battery [950]
Healthy: APC: UPS Not Running on Battery [947]
Healthy: APC: Zero Defective Battery Packs [943]
Healthy: Blue Coat: attack status normal [1977]
Healthy: Brocade Switch: Admin Status Online [1936]
Healthy: Brocade Switch: Operational Status Online [1937]
Healthy: Brocade Switch: POST Returned Embed Port Okay [1938]
Healthy: Cisco (Tandberg C Series): Auto Answer Mode is now On [1418]
Healthy: Cisco (Tandberg C Series): DVI Input is now connected [1428]

- ***Link-Trap***. For events with a source of *Trap*, displays a list of trap OIDs that are included in the MIB files that have been compiled in SL1. You can either select one of the listed trap OIDs to associate with the event or manually enter a custom trap OID. You can use an asterisk (*) as a wildcard character at the end of the trap OID. If you add the wildcard character to the end of the trap OID, the event policy will match all trap OIDs that start with the specified OID string. This is useful for creating "catch all" event policies.
- ***Source Host Varbind***. For events with a source of *Trap*, specifies an OID that is included in the trap. This OID will contain the IP address or hostname to align with the event.
  - If a value is specified in this field, SL1 examines the OID specified in this field. If the value stored in the OID matches the IP address or hostname of a device in SL1, the resulting event will be aligned with that device.
  - If a value is specified in this field, SL1 examines the OID specified in this field. If the value stored in the OID does not match the IP address or hostname of a device in SL1, the resulting event will be aligned with the device that sent the trap.

    - If no value is specified in this field, but the trap includes the default snmpTrapAddress OID, SL1 will examine the value stored in the snmpTrapAddress OID. If the value stored in the OID matches the IP address or hostname of a device in SL1, the resulting event will be aligned with that device.
    - If no value is specified in this field and the trap does not include the snmpTrapAddress OID, SL1 will align the resulting event with the device that sent the trap.

- ***First Match String***. A string used to correlate the event with a log message. To match this event policy, the text of a log message or alert must match the value you enter in this field. Can be any combination of alphanumeric characters. SL1's expression matching is case sensitive. This field is required for events generated with a source of Syslog, Security, 3rd Party, and Email.
- ***Second Match String***. A secondary string used to match against the originating log message. To match this event policy, the text of a log message or alert must match the value you enter in this field and the value you entered in the ***First Match String*** field. This field is optional.

NOTE: The ***Match Logic*** field specifies whether SL1 should process ***First Match String*** and ***Second Match String*** as simple text matches or as regular expressions.

NOTE: You can define an event so that it is triggered only when it occurs on a specific interface. You can then include the interface name and SL1's unique interface ID for the interface in the event message. When defining an event, you can use the following three fields below to associate an event with an interface.

- ***Identifier Pattern***. A regular expression used to extract the specific subentity (like the name of a network interface) within the log entry. SL1 will use this value as the yName of the interface. By identifying the subentity, SL1 can create a unique event for each subentity, instead of a single event for the entire device. For example, a log message indicating a link has gone down may include the network interface name. So this field could extract the network interface name from the log message. SL1's expression matching is case sensitive. For details on the regular expression syntax allowed by SL1, see http://www.python.org/doc/howto.
- ***Identifier Format***. If the ***Identifier Pattern*** field returns multiple results, users can specify which results to use and in which order. Each result is represented by a variable. This field is optional.
    - %1. First match with identifier pattern. This is the default behavior if no value is supplied in the ***Identifier Format*** field.
    - %2. Second match with identifier pattern.
    - For example, users could specify "%2:%1" for "Interface %2: Peer %1".

Select the **[Save]** button to save your settings when you have finished editing the fields pertaining to your trap event policy.

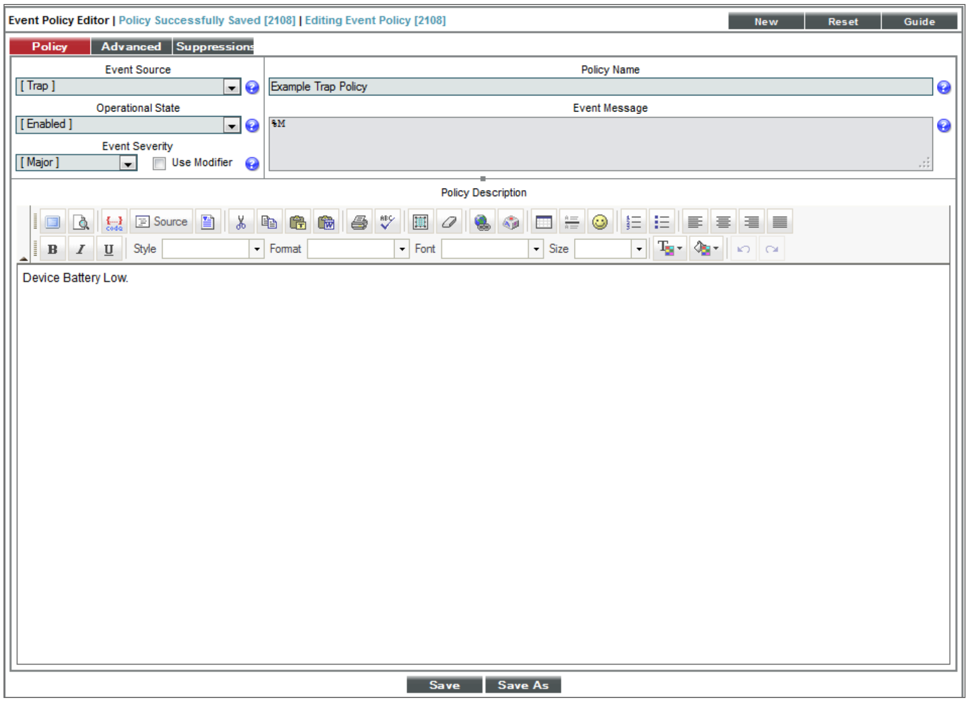
For more information on the remaining fields, as well as the **[Suppressions]** tab, see the ***Events*** manual.

Example Trap Event Policy

Trap messages are sent from devices to SL1 in order to notify the platform of any issues or important events occurring on the device.

To create a Trap Event Policy:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Select the **[Create]** button, and the **Event Policy Editor** page will appear.
3. In the **Event Policy Editor** page, enter these values in the following fields:



Event Policy Editor | Policy Successfully Saved [2108] | Editing Event Policy [2108]

Event Source: [Trap]

Operational State: [Enabled]

Event Severity: [Major] □ Use Modifier

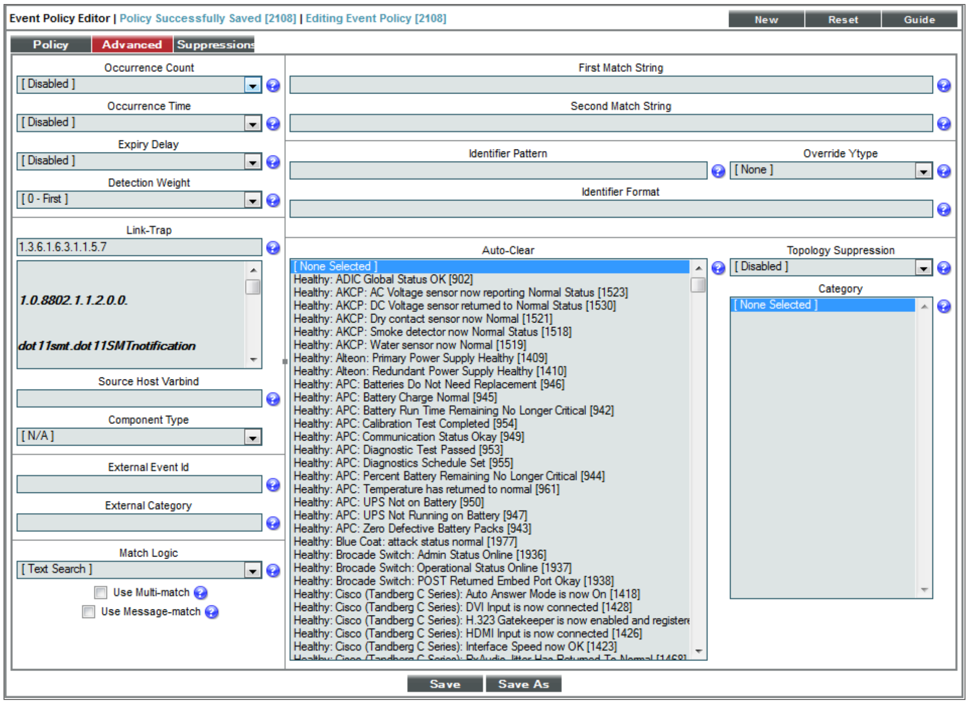
Policy Name: Example Trap Policy

Event Message: %M

Policy Description: Device Battery Low.

   - ***Event Source***. We selected *Trap*.
   - ***Operational State***. We selected *Enabled*.
   - ***Event Severity***. We selected *Notice*.
   - ***Policy Name***. We entered "Example Trap Policy".
   - ***Event Message***. We entered "%M".
   - ***Policy Description***. We entered "Device Battery Low."

4. Select the **[Save]** button.
5. After saving those settings, select the **[Advanced]** tab. We entered the following values in the following fields:



Event Policy Editor | Policy Successfully Saved [2108] | Editing Event Policy [2108]

Occurrence Count	[Disabled]
Occurrence Time	[Disabled]
Expiry Delay	[Disabled]
Detection Weight	[0 - First]
Link-Trap	1.3.6.1.6.3.1.1.5.7
	1.0.8802.1.1.2.0.0. *dot11smt.dot11SMTnotification*
Source Host Varbind	
Component Type	[N/A]
External Event Id	
External Category	
Match Logic	[Text Search]
First Match String	
Second Match String	
Identifier Pattern	
Override Ytype	[None]
Identifier Format	
Topology Suppression	[Disabled]
Category	[None Selected]

☐ Use Multi-match

☐ Use Message-match

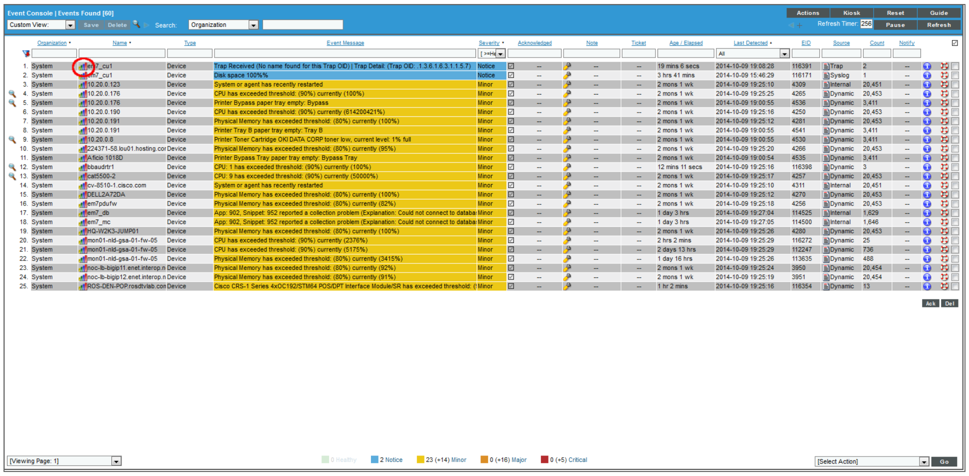
Auto-Clear

[None Selected]
Healthy: ADIC Global Status OK [902]
Healthy: AKCP: AC Voltage sensor now reporting Normal Status [1523]
Healthy: AKCP: DC Voltage sensor returned to Normal Status [1530]
Healthy: AKCP: Dry contact sensor now Normal [1521]
Healthy: AKCP: Smoke detector now Normal Status [1518]
Healthy: AKCP: Water sensor now Normal [1519]
Healthy: Alteon: Primary Power Supply Healthy [1409]
Healthy: Alteon: Redundant Power Supply Healthy [1410]
Healthy: APC: Batteries Do Not Need Replacement [946]
Healthy: APC: Battery Charge Normal [945]
Healthy: APC: Battery Run Time Remaining No Longer Critical [942]
Healthy: APC: Calibration Test Completed [954]
Healthy: APC: Communication Status Okay [949]
Healthy: APC: Diagnostic Test Passed [953]
Healthy: APC: Diagnostics Schedule Set [955]
Healthy: APC: Percent Battery Remaining No Longer Critical [944]
Healthy: APC: Temperature has returned to normal [961]
Healthy: APC: UPS Not on Battery [950]
Healthy: APC: UPS Not Running on Battery [947]
Healthy: APC: Zero Defective Battery Packs [943]
Healthy: Blue Coat: attack status normal [1977]
Healthy: Brocade Switch: Admin Status Online [1936]
Healthy: Brocade Switch: Operational Status Online [1937]
Healthy: Brocade Switch: POST Returned Embed Port Okay [1938]
Healthy: Cisco (Tandberg C Series): Auto Answer Mode is now On [1418]
Healthy: Cisco (Tandberg C Series): DVI Input is now connected [1428]
Healthy: Cisco (Tandberg C Series): H.323 Gatekeeper is now enabled and registere
Healthy: Cisco (Tandberg C Series): HDMI Input is now connected [1426]
Healthy: Cisco (Tandberg C Series): Interface Speed now OK [1423]
Healthy: Cisco (Tandberg C Series): RxAudio Jitter Has Returned To Normal [1468]

- ***Link-Trap***. We entered the device's trap oid of "1.3.6.1.6.3.1.1.5.7".

6. We left the rest of the fields at their default settings, and then selected the **[Save]** button.

7. When the device's battery is low, it will send the trap message and trigger an event, which appears in the **Event Console**. Clicking on the graph icon (📊) will bring up the **Device Summary** page for the device for which the event occurred. Clicking on the life ring icon (🛟) will create a ticket for the event.



Event Console | Events Found [60]

Custom View: | Search: Organization

Refresh Timer: 256

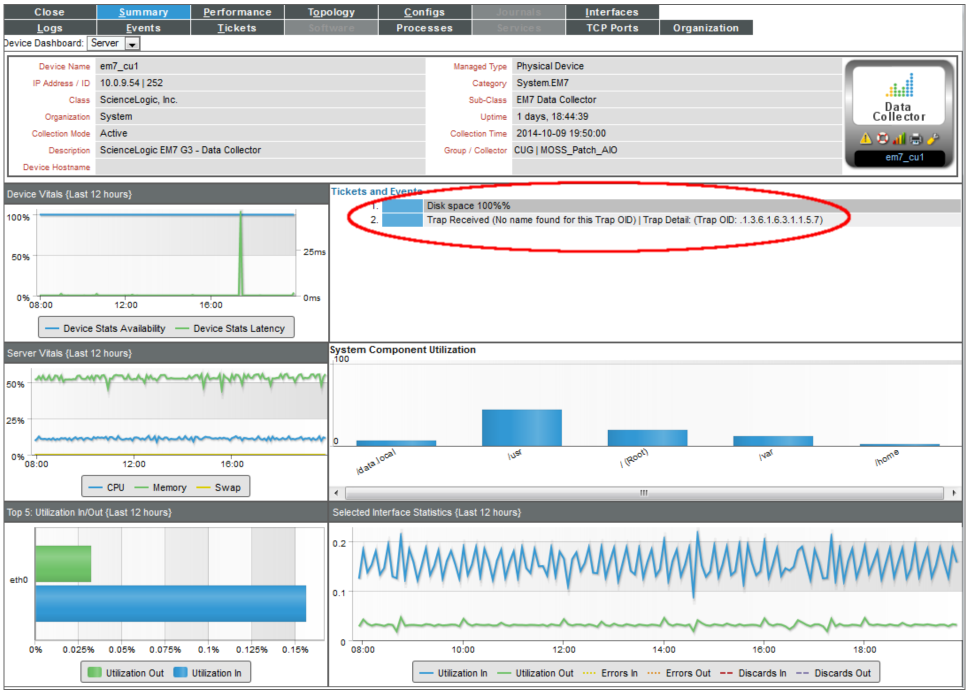
	Organization	Name	Type	Event Message	Severity	Acknowledged	Note	Ticket	Age / Elapsed	Last Detected	EID	Source	Count	Notify	☑
					[>=He					All					
1.	System	em7_cu1	Device	Trap Received (No name found for this Trap OID) | Trap Detail: (Trap OID: .1.3.6.1.6.3.1.1.5.7)	Notice	☑ --	--	--	19 mins 6 secs	2014-10-09 19:08:28	116391	Trap	2	--	☐
2.	System	em7_cu1	Device	Disk space 100%%	Notice	☑ --	--	--	3 hrs 41 mins	2014-10-09 15:46:29	116171	Syslog	1	--	☐
3.	System	10.20.0.123	Device	System or agent has recently restarted	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:10	4309	Internal	20,451	--	☐
4.	System	10.20.0.176	Device	CPU has exceeded threshold: (90%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:25	4265	Dynamic	20,453	--	☐
5.	System	10.20.0.176	Device	Printer Bypass paper tray empty: Bypass	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:00:55	4536	Dynamic	3,411	--	☐
6.	System	10.20.0.190	Device	CPU has exceeded threshold: (90%) currently (614200421%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:16	4250	Dynamic	20,453	--	☐
7.	System	10.20.0.191	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:12	4281	Dynamic	20,453	--	☐
8.	System	10.20.0.191	Device	Printer Tray B paper tray empty: Tray B	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:00:55	4541	Dynamic	3,411	--	☐
9.	System	10.20.0.8	Device	Printer Toner Cartridge OKI DATA CORP toner low, current level: 1% full	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:00:55	4530	Dynamic	3,411	--	☐
10.	System	224371-58.lou01.hosting.cor	Device	Physical Memory has exceeded threshold: (80%) currently (95%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:20	4266	Dynamic	20,453	--	☐
11.	System	Aficio 1018D	Device	Printer Bypass Tray paper tray empty: Bypass Tray	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:00:54	4535	Dynamic	3,411	--	☐
12.	System	bbaudrtr1	Device	CPU: 1 has exceeded threshold: (90%) currently (100%)	Minor	☑ --	--	--	12 mins 11 secs	2014-10-09 19:25:16	116398	Dynamic	3	--	☐
13.	System	cat5500-2	Device	CPU: 9 has exceeded threshold: (90%) currently (50000%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:17	4257	Dynamic	20,453	--	☐
14.	System	cv-8510-1.cisco.com	Device	System or agent has recently restarted	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:10	4311	Internal	20,451	--	☐
15.	System	DELL2A72DA	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:12	4270	Dynamic	20,453	--	☐
16.	System	em7pdufw	Device	Physical Memory has exceeded threshold: (80%) currently (82%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:18	4256	Dynamic	20,453	--	☐
17.	System	em7_db	Device	App: 902, Snippet: 952 reported a collection problem (Explanation: Could not connect to databa	Minor	☑ --	--	--	1 day 3 hrs	2014-10-09 19:27:04	114525	Internal	1,629	--	☐
18.	System	em7_mc	Device	App: 902, Snippet: 952 reported a collection problem (Explanation: Could not connect to databa	Minor	☑ --	--	--	1 day 3 hrs	2014-10-09 19:27:05	114500	Internal	1,646	--	☐
19.	System	HQ-W2K3-JUMP01	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:26	4280	Dynamic	20,453	--	☐
20.	System	mon01-nld-gsa-01-fw-05	Device	CPU has exceeded threshold: (90%) currently (2376%)	Minor	☑ --	--	--	2 hrs 2 mins	2014-10-09 19:25:29	116272	Dynamic	25	--	☐
21.	System	mon01-nld-gsa-01-fw-05	Device	CPU has exceeded threshold: (90%) currently (5175%)	Minor	☑ --	--	--	2 days 13 hrs	2014-10-09 19:25:29	112247	Dynamic	736	--	☐
22.	System	mon01-nld-gsa-01-fw-05	Device	Physical Memory has exceeded threshold: (80%) currently (3415%)	Minor	☑ --	--	--	1 day 16 hrs	2014-10-09 19:25:26	113635	Dynamic	488	--	☐
23.	System	noc-lb-bigip11.enet.interop.n	Device	Physical Memory has exceeded threshold: (80%) currently (92%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:24	3950	Dynamic	20,454	--	☐
24.	System	noc-lb-bigip12.enet.interop.n	Device	Physical Memory has exceeded threshold: (80%) currently (91%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 19:25:19	3951	Dynamic	20,454	--	☐
25.	System	ROS-DEN-POP.rosdtvlab.con	Device	Cisco CRS-1 Series 4xOC192/STM64 POS/DPT Interface Module/SR has exceeded threshold: (	Minor	☑ --	--	--	1 hr 2 mins	2014-10-09 19:25:16	116354	Dynamic	13	--	☐

[Viewing Page: 1]

0 Healthy | 2 Notice | 23 (+14) Minor | 0 (+16) Major | 0 (+5) Critical

[Select Action]

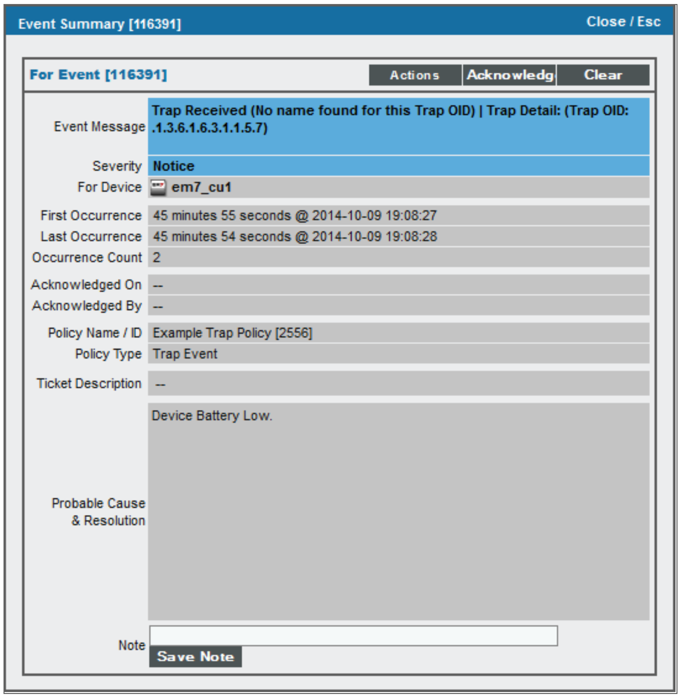
8. Clicking on the graph icon (📊) will bring up the **Device Summary** page. You will see the event listed in the **Device Summary** page, and you can click on the event to view the **Event Summary** modal page.



Device Name	em7_cu1	Managed Type	Physical Device
IP Address / ID	10.0.9.54 | 252	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	EM7 Data Collector
Organization	System	Uptime	1 days, 18:44:39
Collection Mode	Active	Collection Time	2014-10-09 19:50:00
Description	ScienceLogic EM7 G3 - Data Collector	Group / Collector	CUG | MOSS_Patch_AIO
Device Hostname			

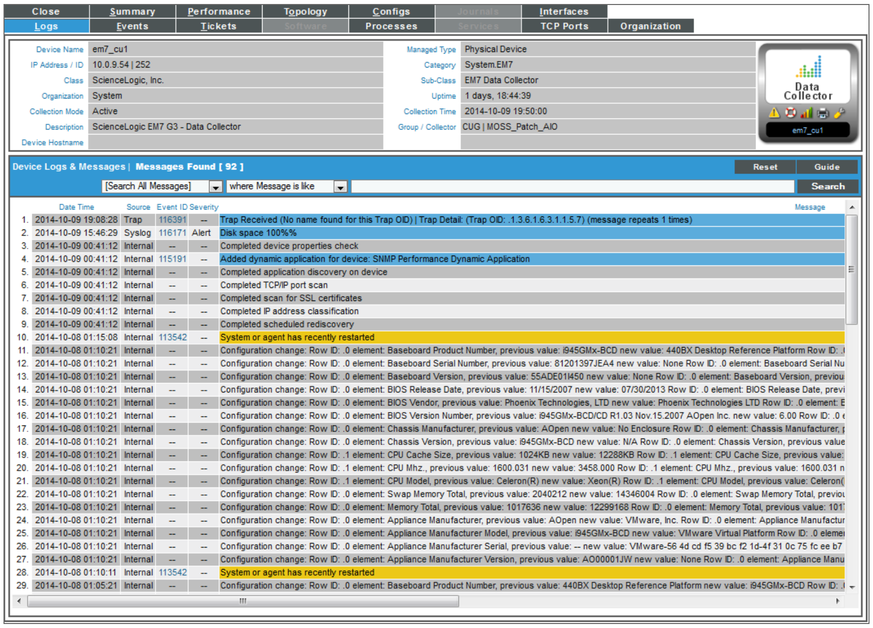
Tickets and Events

1. Disk space 100%%
2. Trap Received (No name found for this Trap OID) | Trap Detail: (Trap OID: .1.3.6.1.6.3.1.1.5.7)



Event Message	Trap Received (No name found for this Trap OID) | Trap Detail: (Trap OID: .1.3.6.1.6.3.1.1.5.7)
Severity	Notice
For Device	em7_cu1
First Occurrence	45 minutes 55 seconds @ 2014-10-09 19:08:27
Last Occurrence	45 minutes 54 seconds @ 2014-10-09 19:08:28
Occurrence Count	2
Acknowledged On	--
Acknowledged By	--
Policy Name / ID	Example Trap Policy [2556]
Policy Type	Trap Event
Ticket Description	--
Probable Cause & Resolution	Device Battery Low.
Note	

9. You can also select the **[Logs]** tab from the **Device Summary** page to view the **Device Logs & Messages** page. The trap message will appear in the device logs, and you can select the View Events icon (⚠) which will take you to the **Viewing Active Events** page for that device.



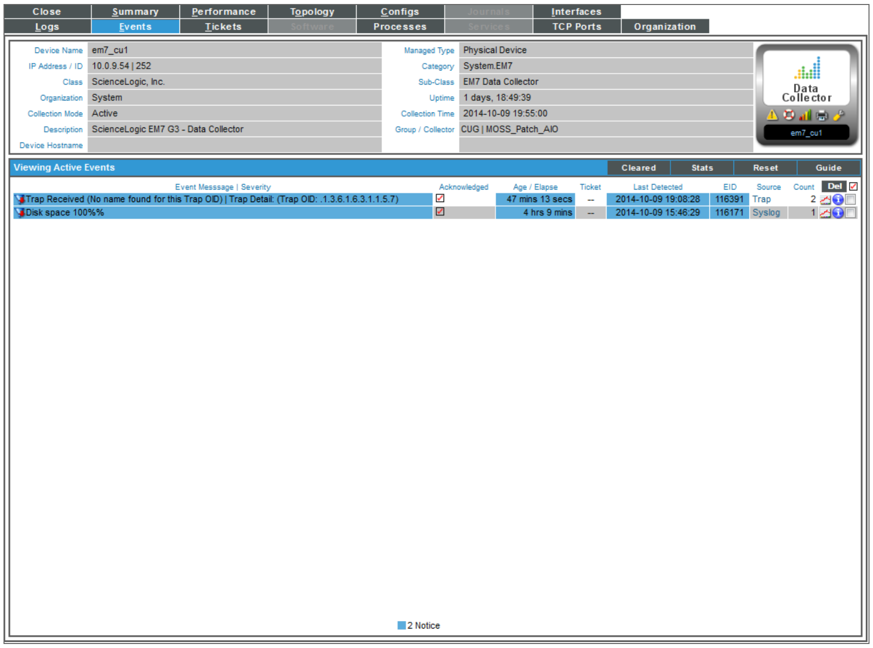
Device Name	em7_cu1	Managed Type	Physical Device
IP Address / ID	10.0.9.54 | 252	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	EM7 Data Collector
Organization	System	Uptime	1 days, 18:44:39
Collection Mode	Active	Collection Time	2014-10-09 19:50:00
Description	ScienceLogic EM7 G3 - Data Collector	Group / Collector	CUG | MOSS_Patch_AIO
Device Hostname			

Device Logs & Messages | Messages Found [92]

[Search All Messages] where Message is like

	Date Time	Source	Event ID	Severity	Message
1.	2014-10-09 19:08:28	Trap	116391	--	Trap Received (No name found for this Trap OID) | Trap Detail: (Trap OID: .1.3.6.1.6.3.1.1.5.7) (message repeats 1 times)
2.	2014-10-09 15:46:29	Syslog	116171	Alert	Disk space 100%%
3.	2014-10-09 00:41:12	Internal	--	--	Completed device properties check
4.	2014-10-09 00:41:12	Internal	115191	--	Added dynamic application for device: SNMP Performance Dynamic Application
5.	2014-10-09 00:41:12	Internal	--	--	Completed application discovery on device
6.	2014-10-09 00:41:12	Internal	--	--	Completed TCP/IP port scan
7.	2014-10-09 00:41:12	Internal	--	--	Completed scan for SSL certificates
8.	2014-10-09 00:41:12	Internal	--	--	Completed IP address classification
9.	2014-10-09 00:41:12	Internal	--	--	Completed scheduled rediscovery
10.	2014-10-08 01:15:08	Internal	113542	--	System or agent has recently restarted
11.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Product Number, previous value: i945GMx-BCD new value: 440BX Desktop Reference Platform Row ID: .
12.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Serial Number, previous value: 81201397JEA4 new value: None Row ID: .0 element: Baseboard Serial Nu
13.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Version, previous value: 55ADE01I450 new value: None Row ID: .0 element: Baseboard Version, previou
14.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: BIOS Release Date, previous value: 11/15/2007 new value: 07/30/2013 Row ID: .0 element: BIOS Release Date, previ
15.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: BIOS Vendor, previous value: Phoenix Technologies, LTD new value: Phoenix Technologies LTD Row ID: .0 element: E
16.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: BIOS Version Number, previous value: i945GMx-BCD/CD R1.03 Nov.15.2007 AOpen Inc. new value: 6.00 Row ID: .0 e
17.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Chassis Manufacturer, previous value: AOpen new value: No Enclosure Row ID: .0 element: Chassis Manufacturer, p
18.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Chassis Version, previous value: i945GMx-BCD new value: N/A Row ID: .0 element: Chassis Version, previous value
19.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .1 element: CPU Cache Size, previous value: 1024KB new value: 12288KB Row ID: .1 element: CPU Cache Size, previous value:
20.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .1 element: CPU Mhz., previous value: 1600.031 new value: 3458.000 Row ID: .1 element: CPU Mhz., previous value: 1600.031 n
21.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .1 element: CPU Model, previous value: Celeron(R) new value: Xeon(R) Row ID: .1 element: CPU Model, previous value: Celeron(
22.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Swap Memory Total, previous value: 2040212 new value: 14346004 Row ID: .0 element: Swap Memory Total, previou
23.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Memory Total, previous value: 1017636 new value: 12299168 Row ID: .0 element: Memory Total, previous value: 101
24.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer, previous value: AOpen new value: VMware, Inc. Row ID: .0 element: Appliance Manufactur
25.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer Model, previous value: i945GMx-BCD new value: VMware Virtual Platform Row ID: .0 eleme
26.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer Serial, previous value: -- new value: VMware-56 4d cd f5 39 bc f2 1d-4f 31 0c 75 fc ee b7
27.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer Version, previous value: AO00001JW new value: None Row ID: .0 element: Appliance Manu
28.	2014-10-08 01:10:11	Internal	113542	--	System or agent has recently restarted
29.	2014-10-08 01:05:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Product Number, previous value: 440BX Desktop Reference Platform new value: i945GMx-BCD Row ID: .

10. From the **Viewing Active Events** page, you can select the information icon (ℹ) to view the **Event Information** modal page, filter the device's events based on event type, or view graphical reports about that device's events based on type.



Device Name	em7_cu1	Managed Type	Physical Device
IP Address / ID	10.0.9.54 | 252	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	EM7 Data Collector
Organization	System	Uptime	1 days, 18:49:39
Collection Mode	Active	Collection Time	2014-10-09 19:55:00
Description	ScienceLogic EM7 G3 - Data Collector	Group / Collector	CUG | MOSS_Patch_AIO
Device Hostname			

Viewing Active Events

Event Messsage | Severity	Acknowledged	Age / Elapse	Ticket	Last Detected	EID	Source	Count	Del ☑
Trap Received (No name found for this Trap OID) | Trap Detail: (Trap OID: .1.3.6.1.6.3.1.1.5.7)	☑	47 mins 13 secs	--	2014-10-09 19:08:28	116391	Trap	2	□
Disk space 100%%	☑	4 hrs 9 mins	--	2014-10-09 15:46:29	116171	Syslog	1	□

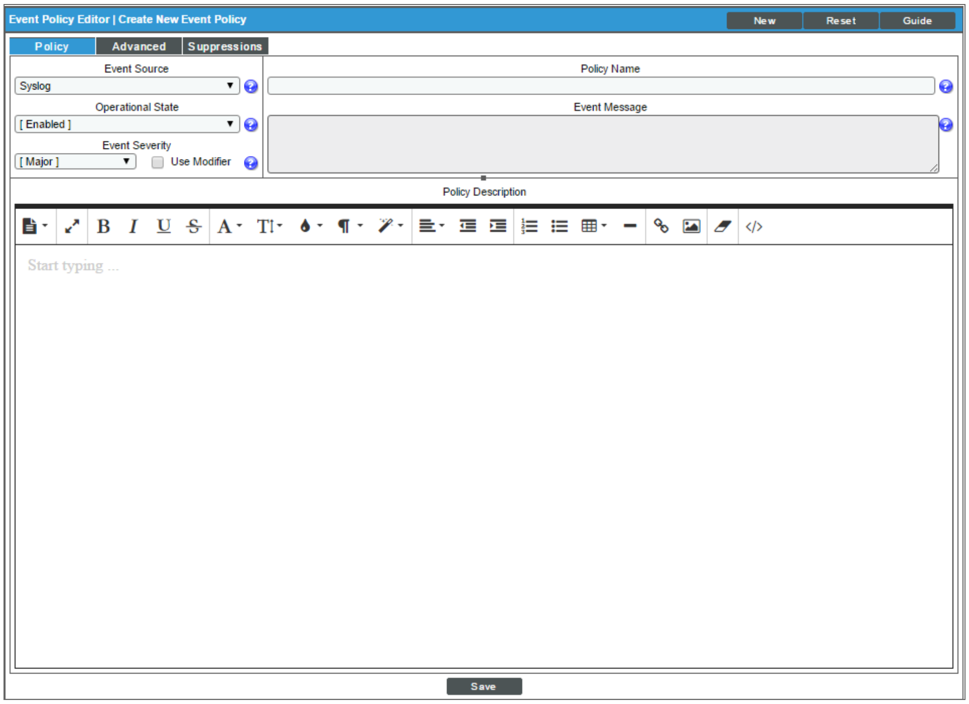
Creating a Syslog Event Policy

SL1 includes pre-defined events for the most commonly encountered conditions on the most common platforms. However, if the pre-defined events do not meet the needs of your organization, you can define new events that better suit your needs.

From the **Event Policies** page (or the **Event Policy Manager** page in the classic SL1 user interface), you can define a new event. You can define custom events to meet your business requirements. You can also define events to be triggered by any custom Dynamic Application alerts you have created.

To create an event definition:

1. Go to **Event Policy Manager** page (Registry > Events > Event Manager).
2. In the **Event Policy Manager** page, click the **[Create]** button. The **Event Policy Editor** page appears:



Event Policy Editor | Create New Event Policy

Event Source: Syslog

Operational State: [Enabled]

Event Severity: [Major] ☐ Use Modifier

3. In the **Event Policy Editor** page and set of tabs, you can define a new event. The **Event Policy Editor** page contains three tabs:

   - ***Policy***. Allows you to define basic parameters for the event. This tab is described in the following section.
   - ***Advanced***. Allows you to define pattern-matching for the event and also define event roll-ups and suppressions.

- ***Suppressions***. Allows you to suppress the event on selected devices. When you suppress an event, you are specifying that, in the future, if this event occurs again on a specific device, the event will not appear in the **Event Console** page or the **Viewing Events** page for the device.

4. Supply values in the following fields:
   - ***Event Source***. Select *Syslog*.
   - ***Policy Name***. The name of the event. Can be any combination of alphanumeric characters, up to 48 characters in length.
   - ***Operational State***. Specifies whether event is to be operational or not. Choices are *Enabled* or *Disabled*.
   - ***Event Message***. The message that appears in the **Event Console** page or the **Viewing Events** page when this event occurs. Can be any combination of alphanumeric characters. Variables include the characters "%" (percent) and "|" (bar). You can also use regular expressions and variables that represent text from the original log message to create the ***Event Message***:
     - To include regular expressions in the Event Message:

       Surround the regular expression with %R and %/R. For example:

       %RFilename: .*? %/R

       Would search for the first instance of the string "Filename: " (Filename-colon-space) followed by any number of any characters up to the line break. The %R indicates the beginning of a regular expression. The %/R indicates the end of a regular expression.

       SL1 will use the regular expression to search the log message and use the matching text in the event message.

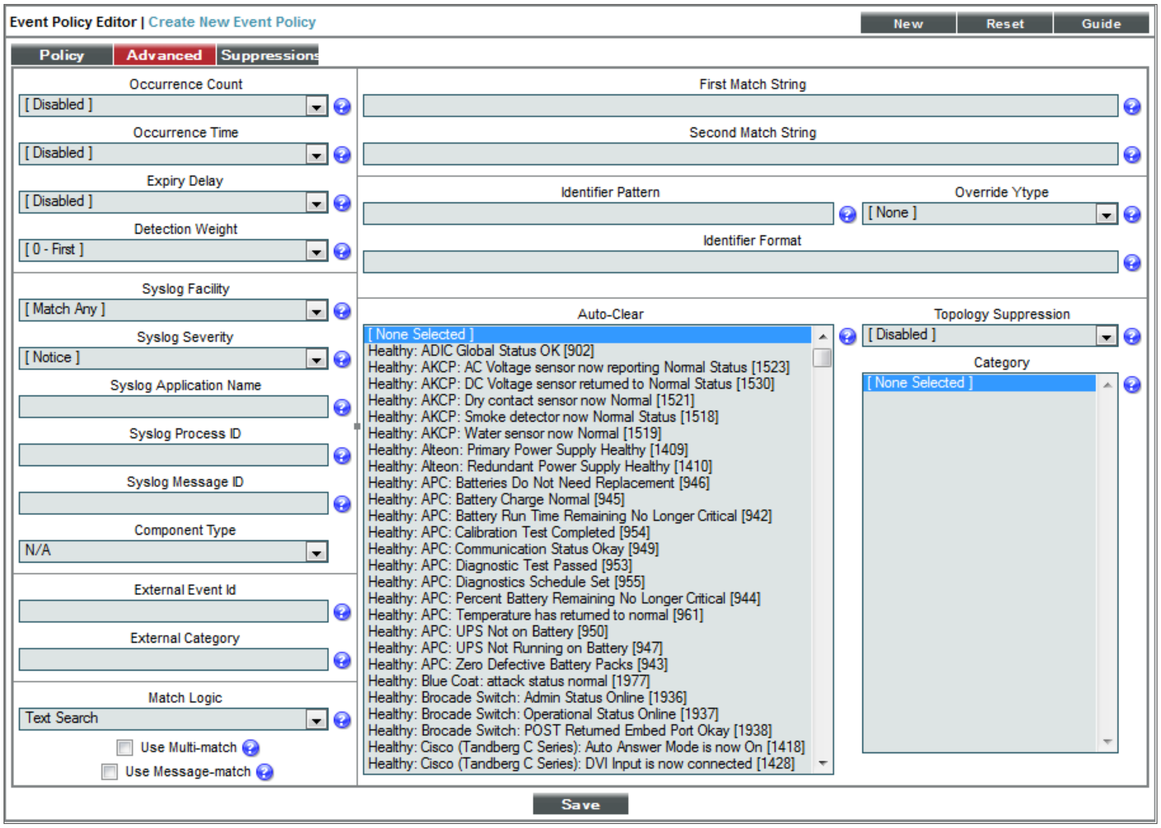
       For details on the regular expression syntax allowed by SL1, see http://www.python.org/doc/howto/.
     - You can also use the following variables in this field:
       - *%I* ("eye").This variable contains the value that matches the ***Identifier Pattern*** field in the **[Advanced]** tab.
       - *%M*. The full text of the log message that triggered the event will be displayed in ***Event Message*** field.
       - *%V*. Data Value from log file will be displayed in the ***Event Message*** field.
       - *%T*. Threshold value from the log file will be displayed in ***Event Message*** field.
   - ***Event Severity***. Defines the severity of the event. Choices are:
     - *Healthy*. Healthy Events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.

- ◦ *Notice*. Notice Events indicate a condition that does not affect service but about which users should be aware.
- ◦ *Minor*. Minor Events indicate a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
- ◦ *Major*. Major Events indicate a condition that is service impacting and requires immediate investigation.
- ◦ *Critical*. Critical Events indicate a condition that can seriously impair or curtail service and require immediate attention (i.e. service or system outages).

- ***Use Modifier***. If selected, when the event is triggered, SL1 will check to see if the interface associated with this event has a custom severity modifier. If so, the event will appear in the **Event Console** with that custom severity modifier applied to the severity in the ***Event Severity*** field. For example, if an interface with an ***Event Severity Adjust*** setting of *Sev -1* triggers an event with an ***Event Severity*** of *Major* and that event has the ***Use Modifier*** checkbox selected, the event will appear in the **Event Console** with a severity of *Minor*.
- ***Policy Description***. Text that explains what the event means and what possible causes are.

Defining Pattern Matching and Advanced Behavior

The **[Advanced]** tab in the **Event Policy Editor** page allows you to define or edit pattern-matching for the syslog event and also define event roll-ups and suppressions. In the **[Advanced]** tab, you can define or edit the following fields that pertain to syslogs:



Event Policy Editor | Create New Event Policy

Occurrence Count: [Disabled]
Occurrence Time: [Disabled]
Expiry Delay: [Disabled]
Detection Weight: [0 - First]
Syslog Facility: [Match Any]
Syslog Severity: [Notice]
Syslog Application Name:
Syslog Process ID:
Syslog Message ID:
Component Type: N/A
External Event Id:
External Category:
Match Logic: Text Search
□ Use Multi-match
□ Use Message-match

First Match String:
Second Match String:
Identifier Pattern:
Override Ytype: [None]
Identifier Format:

Auto-Clear:
[None Selected]
Healthy: ADIC Global Status OK [902]
Healthy: AKCP: AC Voltage sensor now reporting Normal Status [1523]
Healthy: AKCP: DC Voltage sensor returned to Normal Status [1530]
Healthy: AKCP: Dry contact sensor now Normal [1521]
Healthy: AKCP: Smoke detector now Normal Status [1518]
Healthy: AKCP: Water sensor now Normal [1519]
Healthy: Alteon: Primary Power Supply Healthy [1409]
Healthy: Alteon: Redundant Power Supply Healthy [1410]
Healthy: APC: Batteries Do Not Need Replacement [946]
Healthy: APC: Battery Charge Normal [945]
Healthy: APC: Battery Run Time Remaining No Longer Critical [942]
Healthy: APC: Calibration Test Completed [954]
Healthy: APC: Communication Status Okay [949]
Healthy: APC: Diagnostic Test Passed [953]
Healthy: APC: Diagnostics Schedule Set [955]
Healthy: APC: Percent Battery Remaining No Longer Critical [944]
Healthy: APC: Temperature has returned to normal [961]
Healthy: APC: UPS Not on Battery [950]
Healthy: APC: UPS Not Running on Battery [947]
Healthy: APC: Zero Defective Battery Packs [943]
Healthy: Blue Coat: attack status normal [1977]
Healthy: Brocade Switch: Admin Status Online [1936]
Healthy: Brocade Switch: Operational Status Online [1937]
Healthy: Brocade Switch: POST Returned Embed Port Okay [1938]
Healthy: Cisco (Tandberg C Series): Auto Answer Mode is now On [1418]
Healthy: Cisco (Tandberg C Series): DVI Input is now connected [1428]

Topology Suppression: [Disabled]
Category: [None Selected]

- ***Syslog Facility***. Facility information used by syslog to match an event message.
- ***Syslog Severity***. Severity information used by syslog to match an event message.
- ***Syslog Application Name***. Application Name used by syslog to match an event message.
- ***Syslog Process ID***. Process ID used by syslog to match an event message.
- ***Syslog Message ID***. Message ID used by syslog to match an event message.

> **NOTE**: For more information on the syslog fields for events, see http://www.rfc-archive.org/getrfc.php?rfc=5424 .

- ***First Match String***. A string used to correlate the event with a log message. To match this event policy, the text of a log message or alert must match the value you enter in this field. Can be any combination of alphanumeric characters. SL1's expression matching is case sensitive. This field is required for events generated with a source of Syslog, Security, 3rd Party, and Email.
- ***Second Match String***. A secondary string used to match against the originating log message. To match this event policy, the text of a log message or alert must match the value you enter in this field and the value you entered in the ***First Match String*** field. This field is optional.

> **NOTE**: The ***Match Logic*** field specifies whether SL1 should process ***First Match String*** and ***Second Match String*** as simple text matches or as regular expressions.

> **NOTE**: You can define an event so that it is triggered only when it occurs on a specific interface. You can then include the interface name and SL1's unique interface ID for the interface in the event message. When defining an event, you can use the following three fields below to associate an event with an interface.

- ***Identifier Pattern***. A regular expression used to extract the specific subentity (like the name of a network interface) within the log entry. SL1 will use this value as the yName of the interface. By identifying the subentity, SL1 can create a unique event for each subentity, instead of a single event for the entire device. For example, a log message indicating a link has gone down may include the network interface name. So this field could extract the network interface name from the log message. SL1's expression matching is case sensitive. For details on the regular expression syntax allowed by SL1, see http://www.python.org/doc/howto.
- ***Identifier Format***. If the ***Identifier Pattern*** field returns multiple results, users can specify which results to use and in which order. Each result is represented by a variable. This field is optional.
    - %1. First match with identifier pattern. This is the default behavior if no value is supplied in the ***Identifier Format*** field.
    - %2. Second match with identifier pattern.
    - For example, users could specify "%2:%1" for "Interface %2: Peer %1".

Select the **[Save]** button to save your settings when you have finished editing the fields pertaining to your syslog event policy.

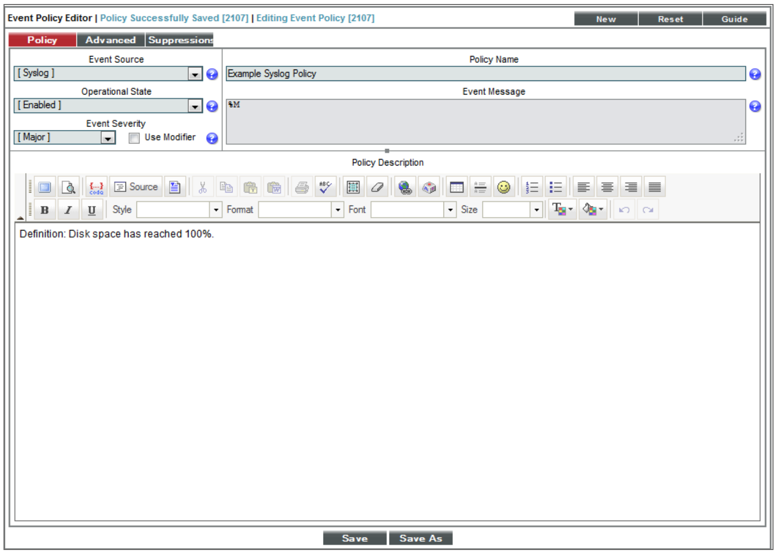
For more information on the remaining fields, as well as the **[Suppressions]** tab, see the ***Events*** manual.

Example Syslog Event Policy

This section will walk through the steps of creating an event policy for syslogs. We will be creating a policy that will send a syslog message when the device's disk space has reached 100% capacity.

To create a Syslog Event Policy:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. Select the **[Create]** button, and the **Event Policy Editor** page will appear.
3. In the **Event Policy Editor** page, enter these values in the following fields:



Event Policy Editor | Policy Successfully Saved [2107] | Editing Event Policy [2107]

Event Source: [Syslog]

Operational State: [Enabled]

Event Severity: [Major] □ Use Modifier

Policy Name: Example Syslog Policy

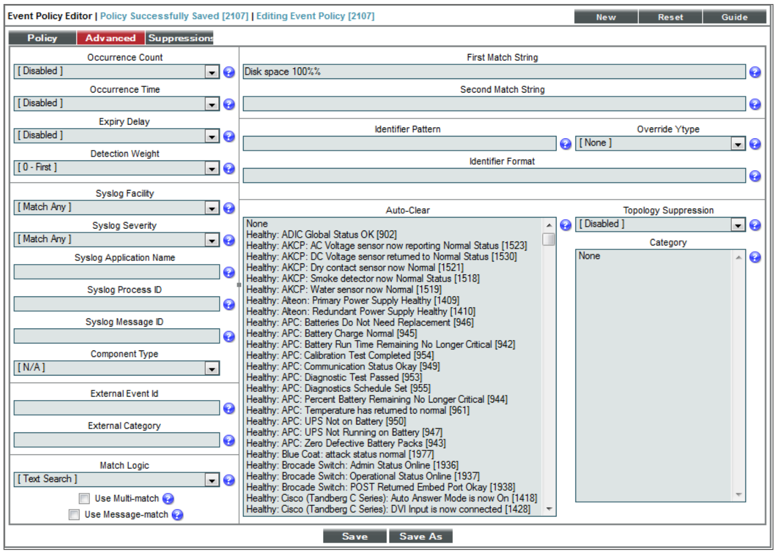
Event Message: %M

Policy Description: Definition: Disk space has reached 100%.

- ***Event Source***. We selected *Syslog*.
- ***Operational State***. We selected *Enabled*.
- ***Event Severity***. We selected *Notice*.
- ***Policy Name***. We entered "Example Syslog Policy".
- ***Event Message***. We entered "%M".
- ***Policy Description***. We entered "Definition: Disk space has reached 100%."

4. Select the **[Save]** button.

5. After saving those settings, select the **[Advanced]** tab. We entered the following values in the following fields:



Event Policy Editor | Policy Successfully Saved [2107] | Editing Event Policy [2107]

New | Reset | Guide

Policy | Advanced | Suppressions

Occurrence Count: [Disabled]

Occurrence Time: [Disabled]

Expiry Delay: [Disabled]

Detection Weight: [0 - First]

Syslog Facility: [Match Any]

Syslog Severity: [Match Any]

Syslog Application Name:

Syslog Process ID:

Syslog Message ID:

Component Type: [N/A]

External Event Id:

External Category:

Match Logic: [Text Search]

□ Use Multi-match

□ Use Message-match

First Match String: Disk space 100%%

Second Match String:

Identifier Pattern:

Override Ytype: [None]

Identifier Format:

Auto-Clear:
None
Healthy: ADIC Global Status OK [902]
Healthy: AKCP: AC Voltage sensor now reporting Normal Status [1523]
Healthy: AKCP: DC Voltage sensor returned to Normal Status [1530]
Healthy: AKCP: Dry contact sensor now Normal [1521]
Healthy: AKCP: Smoke detector now Normal Status [1518]
Healthy: AKCP: Water sensor now Normal [1519]
Healthy: Alteon: Primary Power Supply Healthy [1409]
Healthy: Alteon: Redundant Power Supply Healthy [1410]
Healthy: APC: Batteries Do Not Need Replacement [946]
Healthy: APC: Battery Charge Normal [945]
Healthy: APC: Battery Run Time Remaining No Longer Critical [942]
Healthy: APC: Calibration Test Completed [954]
Healthy: APC: Communication Status Okay [949]
Healthy: APC: Diagnostic Test Passed [953]
Healthy: APC: Diagnostics Schedule Set [955]
Healthy: APC: Percent Battery Remaining No Longer Critical [944]
Healthy: APC: Temperature has returned to normal [961]
Healthy: APC: UPS Not on Battery [950]
Healthy: APC: UPS Not Running on Battery [947]
Healthy: APC: Zero Defective Battery Packs [943]
Healthy: Blue Coat: attack status normal [1977]
Healthy: Brocade Switch: Admin Status Online [1936]
Healthy: Brocade Switch: Operational Status Online [1937]
Healthy: Brocade Switch: POST Returned Embed Port Okay [1938]
Healthy: Cisco (Tandberg C Series): Auto Answer Mode is now On [1418]
Healthy: Cisco (Tandberg C Series): DVI Input is now connected [1428]

Topology Suppression: [Disabled]

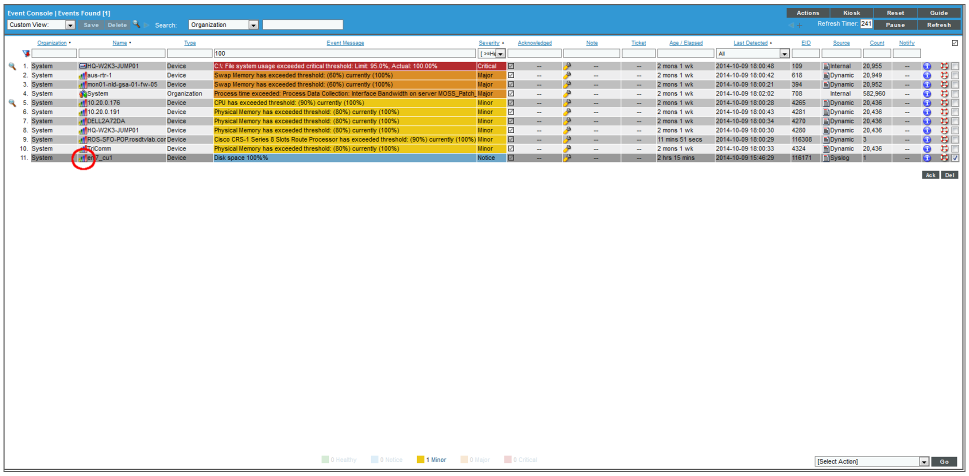
Category: None

Save | Save As

- ***Syslog Facility***. We selected *Match Any*.
- ***Syslog Severity***. We selected *Match Any*.
- ***First Match String***. We entered "Disk space 100%%".

6. We left the rest of the fields at their default settings, and then selected the **[Save]** button.

7. When the device reaches 100% capacity, it will trigger an event, which appears in the **Event Console**. Clicking on the graph icon (📊) will bring up the **Device Summary** page for the device for which the event occurred. Clicking on the life ring icon (🛟) will create a ticket for the event.



Event Console | Events Found [1]

Custom View: | Save | Delete | Search: Organization

Actions | Kiosk | Reset | Guide

Refresh Timer: 241 | Pause | Refresh

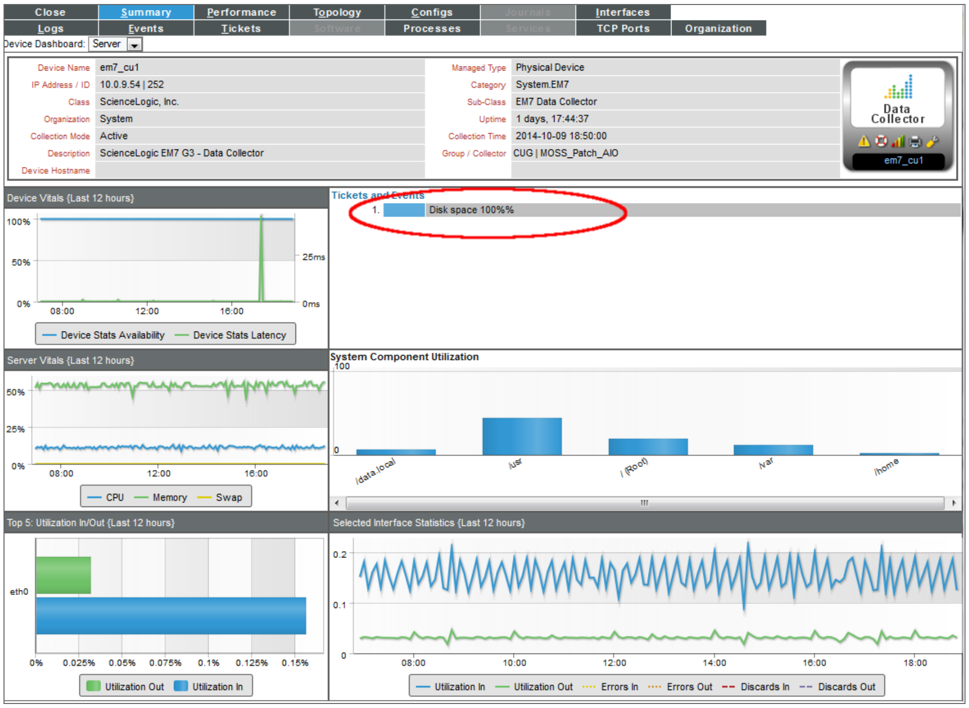
	Organization	Name	Type	Event Message	Severity	Acknowledged	Note	Ticket	Age / Elapsed	Last Detected	EID	Source	Count	Notify	☑
				100	[>=He					All					
1.	System	HQ-W2K3-JUMP01	Device	C:\: File system usage exceeded critical threshold: Limit: 95.0%, Actual: 100.00%	Critical	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:48	109	Internal	20,955	--	□
2.	System	aus-rtr-1	Device	Swap Memory has exceeded threshold: (60%) currently (100%)	Major	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:42	618	Dynamic	20,949	--	□
3.	System	mon01-nld-gsa-01-fw-05	Device	Swap Memory has exceeded threshold: (60%) currently (100%)	Major	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:21	394	Dynamic	20,952	--	□
4.	System	System	Organization	Process time exceeded: Process Data Collection: Interface Bandwidth on server MOSS_Patch_	Major	☑ --	--	--	2 mons 1 wk	2014-10-09 18:02:02	708	Internal	582,960	--	□
5.	System	10.20.0.176	Device	CPU has exceeded threshold: (90%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:28	4265	Dynamic	20,436	--	□
6.	System	10.20.0.191	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:43	4281	Dynamic	20,436	--	□
7.	System	DELL2A72DA	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:34	4270	Dynamic	20,436	--	□
8.	System	HQ-W2K3-JUMP01	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:30	4280	Dynamic	20,436	--	□
9.	System	ROS-SFO-POP.rosdtvlab.cor	Device	Cisco CRS-1 Series 8 Slots Route Processor has exceeded threshold: (90%) currently (100%)	Minor	☑ --	--	--	11 mins 51 secs	2014-10-09 18:00:29	116308	Dynamic	3	--	□
10.	System	TriComm	Device	Physical Memory has exceeded threshold: (80%) currently (100%)	Minor	☑ --	--	--	2 mons 1 wk	2014-10-09 18:00:33	4324	Dynamic	20,436	--	□
11.	System	em7_cu1	Device	Disk space 100%%	Notice	☑ --	--	--	2 hrs 15 mins	2014-10-09 15:46:29	116171	Syslog	1	--	☑

Ack | Del

0 Healthy | 0 Notice | 1 Minor | 0 Major | 0 Critical

[Select Action] | Go

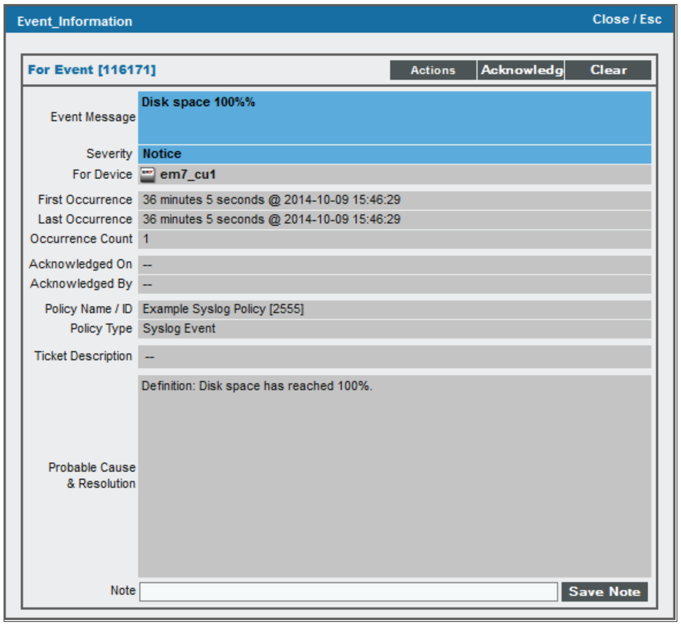
8. Clicking on the graph icon (📊) will bring up the **Device Summary** page. You will see the event listed in the **Device Summary** page, and you can click on the event to view the **Event Summary** modal page.



Device Name	em7_cu1	Managed Type	Physical Device
IP Address / ID	10.0.9.54 | 252	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	EM7 Data Collector
Organization	System	Uptime	1 days, 17:44:37
Collection Mode	Active	Collection Time	2014-10-09 18:50:00
Description	ScienceLogic EM7 G3 - Data Collector	Group / Collector	CUG | MOSS_Patch_AIO
Device Hostname			

Tickets and Events

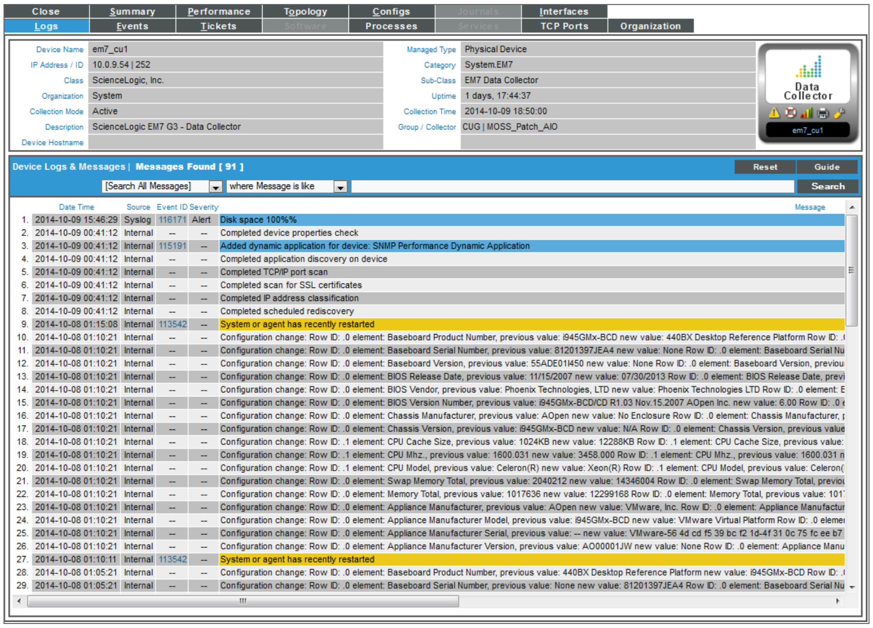
1. Disk space 100%%



For Event [116171]

Event Message	Disk space 100%%
Severity	Notice
For Device	em7_cu1
First Occurrence	36 minutes 5 seconds @ 2014-10-09 15:46:29
Last Occurrence	36 minutes 5 seconds @ 2014-10-09 15:46:29
Occurrence Count	1
Acknowledged On	--
Acknowledged By	--
Policy Name / ID	Example Syslog Policy [2555]
Policy Type	Syslog Event
Ticket Description	--
Probable Cause & Resolution	Definition: Disk space has reached 100%.
Note	

9. You can also select the **[Logs]** tab from the **Device Summary** page to view the **Device Logs & Messages** page. The syslog message will appear in the device logs, and you can select the View Events icon (⚠) which will take you to the **Viewing Active Events** page for that device.



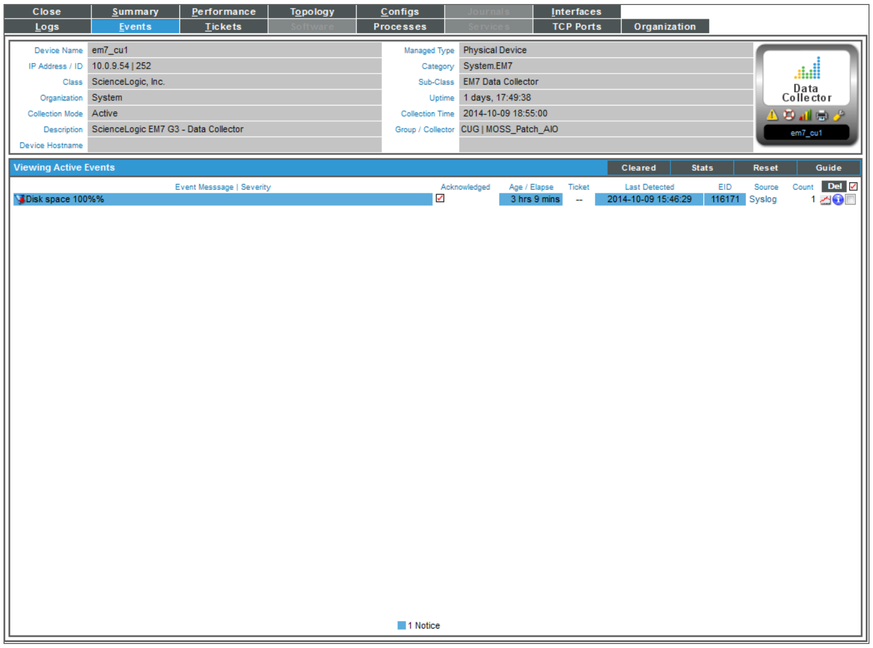
Device Name	em7_cu1	Managed Type	Physical Device
IP Address / ID	10.0.9.54 | 252	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	EM7 Data Collector
Organization	System	Uptime	1 days, 17:44:37
Collection Mode	Active	Collection Time	2014-10-09 18:50:00
Description	ScienceLogic EM7 G3 - Data Collector	Group / Collector	CUG | MOSS_Patch_AIO
Device Hostname			

Device Logs & Messages | Messages Found [91]

[Search All Messages] where Message is like

	Date Time	Source	Event ID	Severity	Message
1.	2014-10-09 15:46:29	Syslog	116171	Alert	Disk space 100%%
2.	2014-10-09 00:41:12	Internal	--	--	Completed device properties check
3.	2014-10-09 00:41:12	Internal	115191	--	Added dynamic application for device: SNMP Performance Dynamic Application
4.	2014-10-09 00:41:12	Internal	--	--	Completed application discovery on device
5.	2014-10-09 00:41:12	Internal	--	--	Completed TCP/IP port scan
6.	2014-10-09 00:41:12	Internal	--	--	Completed scan for SSL certificates
7.	2014-10-09 00:41:12	Internal	--	--	Completed IP address classification
8.	2014-10-09 00:41:12	Internal	--	--	Completed scheduled rediscovery
9.	2014-10-08 01:15:08	Internal	113542	--	System or agent has recently restarted
10.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Product Number, previous value: i945GMx-BCD new value: 440BX Desktop Reference Platform Row ID: .
11.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Serial Number, previous value: 81201397JEA4 new value: None Row ID: .0 element: Baseboard Serial Nu
12.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Version, previous value: 55ADE01I450 new value: None Row ID: .0 element: Baseboard Version, previou
13.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: BIOS Release Date, previous value: 11/15/2007 new value: 07/30/2013 Row ID: .0 element: BIOS Release Date, previ
14.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: BIOS Vendor, previous value: Phoenix Technologies, LTD new value: Phoenix Technologies LTD Row ID: .0 element: E
15.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: BIOS Version Number, previous value: i945GMx-BCD/CD R1.03 Nov.15.2007 AOpen Inc. new value: 6.00 Row ID: .0 e
16.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Chassis Manufacturer, previous value: AOpen new value: No Enclosure Row ID: .0 element: Chassis Manufacturer, p
17.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Chassis Version, previous value: i945GMx-BCD new value: N/A Row ID: .0 element: Chassis Version, previous value
18.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .1 element: CPU Cache Size, previous value: 1024KB new value: 12288KB Row ID: .1 element: CPU Cache Size, previous value:
19.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .1 element: CPU Mhz., previous value: 1600.031 new value: 3458.000 Row ID: .1 element: CPU Mhz., previous value: 1600.031 n
20.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .1 element: CPU Model, previous value: Celeron(R) new value: Xeon(R) Row ID: .1 element: CPU Model, previous value: Celeron(
21.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Swap Memory Total, previous value: 2040212 new value: 14346004 Row ID: .0 element: Swap Memory Total, previou
22.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Memory Total, previous value: 1017636 new value: 12299168 Row ID: .0 element: Memory Total, previous value: 101
23.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer, previous value: AOpen new value: VMware, Inc. Row ID: .0 element: Appliance Manufactur
24.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer Model, previous value: i945GMx-BCD new value: VMware Virtual Platform Row ID: .0 eleme
25.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer Serial, previous value: -- new value: VMware-56 4d cd f5 39 bc f2 1d-4f 31 0c 75 fc ee b7
26.	2014-10-08 01:10:21	Internal	--	--	Configuration change: Row ID: .0 element: Appliance Manufacturer Version, previous value: AO00001JW new value: None Row ID: .0 element: Appliance Manu
27.	2014-10-08 01:10:11	Internal	113542	--	System or agent has recently restarted
28.	2014-10-08 01:05:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Product Number, previous value: 440BX Desktop Reference Platform new value: i945GMx-BCD Row ID: .
29.	2014-10-08 01:05:21	Internal	--	--	Configuration change: Row ID: .0 element: Baseboard Serial Number, previous value: None new value: 81201397JEA4 Row ID: .0 element: Baseboard Serial Nu

10. From the **Viewing Active Events** page, you can select the information icon (ℹ) to view the **Event Information** modal page, filter the device's events based on event type, or view graphical reports about that device's events based on type.



Device Name	em7_cu1	Managed Type	Physical Device
IP Address / ID	10.0.9.54 | 252	Category	System.EM7
Class	ScienceLogic, Inc.	Sub-Class	EM7 Data Collector
Organization	System	Uptime	1 days, 17:49:38
Collection Mode	Active	Collection Time	2014-10-09 18:55:00
Description	ScienceLogic EM7 G3 - Data Collector	Group / Collector	CUG | MOSS_Patch_AIO
Device Hostname			

Viewing Active Events

Event Messsage | Severity	Acknowledged	Age / Elapse	Ticket	Last Detected	EID	Source	Count	Del ☑
Disk space 100%%	☑	3 hrs 9 mins	--	2014-10-09 15:46:29	116171	Syslog	1	☐

🟦 1 Notice

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010