ManageEngine
Log360

DATASHEET

Rapid and accurate log forensics with Log360

Log360, ManageEngine's comprehensive security information and event management (SIEM) solution, collects and analyzes logs to gain important, actionable security information about various events taking place in the network. This information aids the security team in detecting security breaches or malicious activities in the network efficiently.

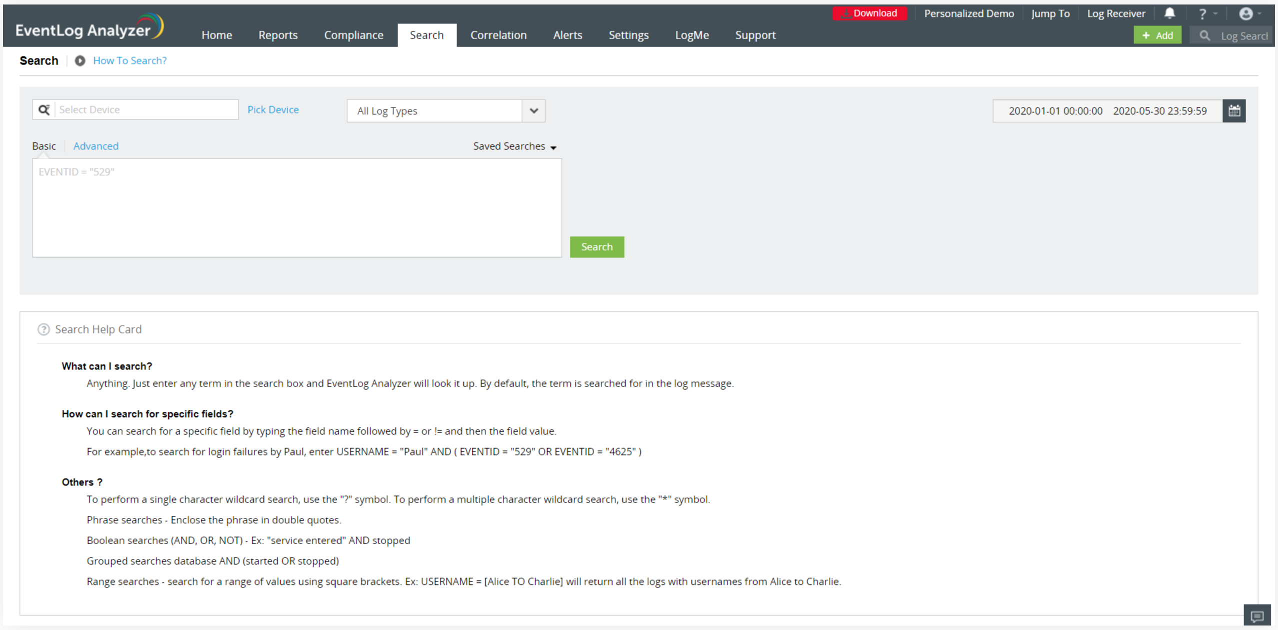
Rapid and accurate log forensics with Log360

You have a gut feeling that something isn't quite right with your network, and you can't stop it until you get to the bottom of it. A critical network device, say, a web server, goes down repeatedly. Is it mechanical failure? A hardware issue? Or is someone working from within to bring it down? Allow Log360 to figure it all out for you.

A security information and event management (SIEM) solution like Log360 aggregates, securely stores, and efficiently analyzes the log data generated by your network devices to detect treats and mitigate attacks. With this, you can audit changes in Active Directory, Azure Active Directory, network devices, workstations, servers, and your public cloud infrastructure, all from a single console. Log360 also has a set of purpose-built capabilities for log forensics that can help you discover the hidden risks and vulnerabilities in your network.

Super-fast log search engine

Chosen by most organizations, this technique is easy to configure and employed as the default log collection method by Log360. In this method, Log360 listens to the log data received on specific ports using protocols like Windows Management Instrumentation (WMI).



2020-01-01 00:00:00 2020-05-30 23:59:59

EVENTID = "529"

What can I search?

Anything. Just enter any term in the search box and EventLog Analyzer will look it up. By default, the term is searched for in the log message.

How can I search for specific fields?

You can search for a specific field by typing the field name followed by = or != and then the field value.

For example,to search for login failures by Paul, enter USERNAME = "Paul" AND (EVENTID = "529" OR EVENTID = "4625")

Others ?

To perform a single character wildcard search, use the "?" symbol. To perform a multiple character wildcard search, use the "*" symbol.

Phrase searches - Enclose the phrase in double quotes.

Boolean searches (AND, OR, NOT) - Ex: "service entered" AND stopped

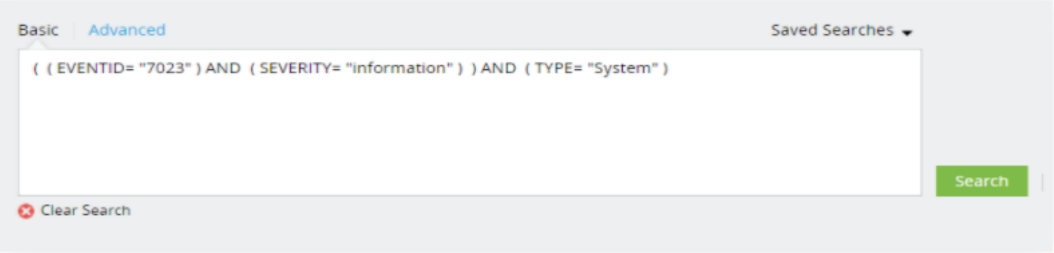
Grouped searches database AND (started OR stopped)

Range searches - search for a range of values using square brackets. Ex: USERNAME = [Alice TO Charlie] will return all the logs with usernames from Alice to Charlie.

Log360's search engine, powered by elastic search, makes forensic investigation simpleand quick. It has both basic and advanced options to search through raw and normalized logs, and instantly generates forensic reports based on the search results. Unlike traditional SIEM solutions, you don't have to write scripts or code for querying logs. All searches can be performed from the user interface.

Basic search

This search option lets you build your search queries with Boolean operators, comparison operators, wild-card characters, ranges, phrases, or grouped fields.

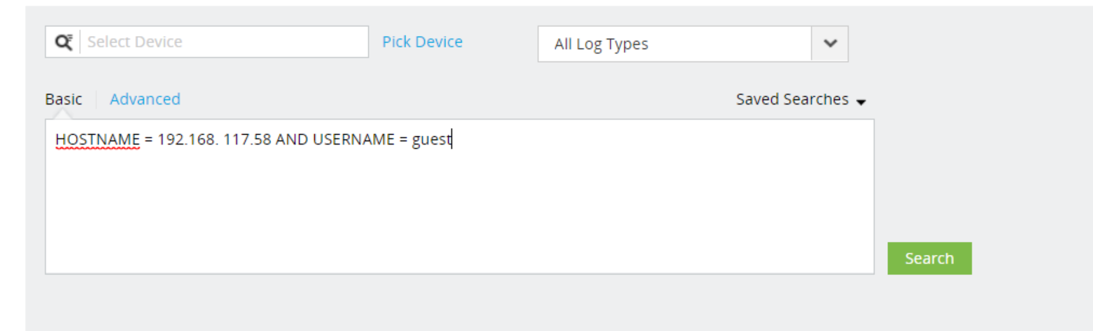


((EVENTID= "7023") AND (SEVERITY= "information")) AND (TYPE= "System")

Using Boolean operators

An expression with Boolean operators looks like this: <field name>=<field value> <Boolean> <field name>=<field value>. You can use the following Boolean operators: AND, OR, NOT. This option can be used when you are looking for a specific instance in a specific machine.

Example: HOSTNAME = 192.168.117.59 AND USERNAME = guest

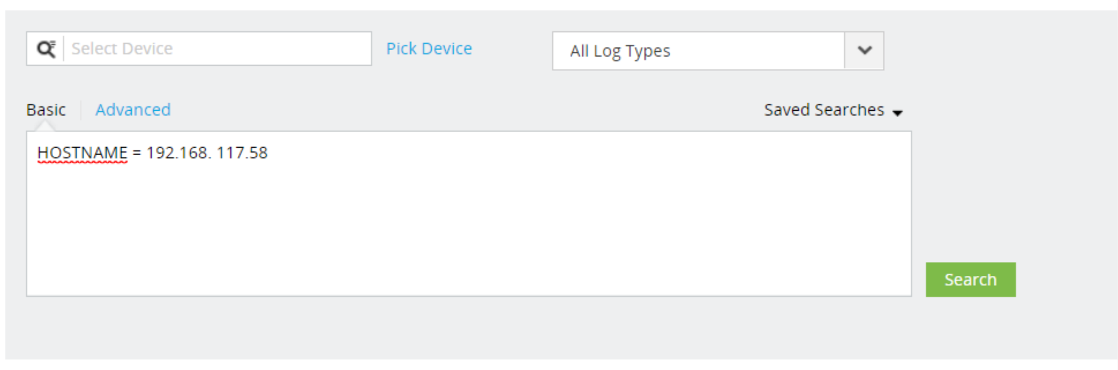


HOSTNAME = 192.168. 117.58 AND USERNAME = guest

Using comparison operators

An expression with comparison operators looks like the following: <field name> <comparison operator> <field value>. You can use the following comparison operators: =, !=, >, <, >=, <=.

Example: If you want to search for devices falling under a certain IP range, conditional operators can be used, i.e., HOSTNAME <=192.168.117.59. For this condition, devices with the IP address 192.168.117.59 and greater will be isolated.

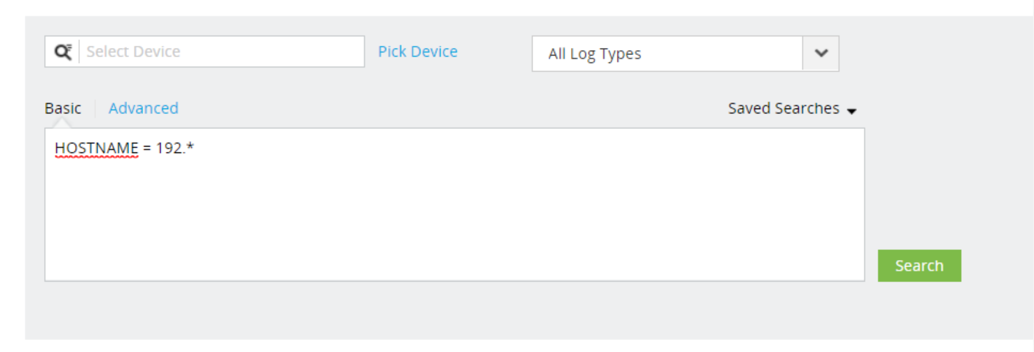


HOSTNAME = 192.168. 117.58

Using wild-card characters

Wild-card search can be used to construct a search query when you have only have partial field values. An expression with wild-card characters looks like this: <field name> = <partial field value> <wild-card character>. You can use the following wild-card characters: ? for a single character, * for multiple characters.

Example: HOSTNAME = 192.* This wild-card search query will give you all hostnames starting with 192.

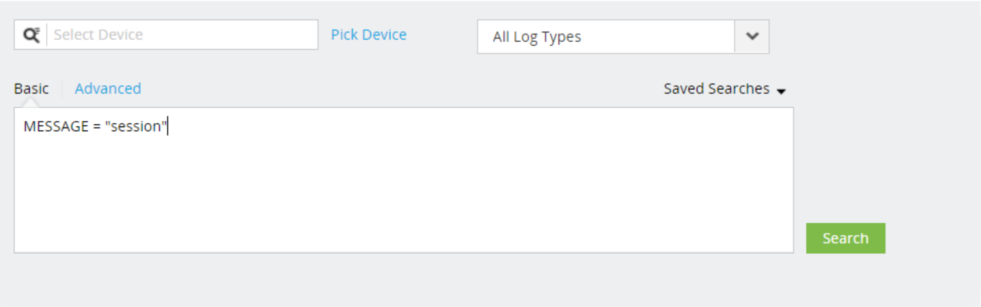


HOSTNAME = 192.*

Using phrases

With phrase search, you can build search queries with phrases rather than field values. An expression with a phrase looks like the following: <field name> = "<partial field value>". Use double quotes ("") to specify a phrase as the field value.

Example: This search query can isolate instances or logs with the required phrase.
MESSAGE = "session"

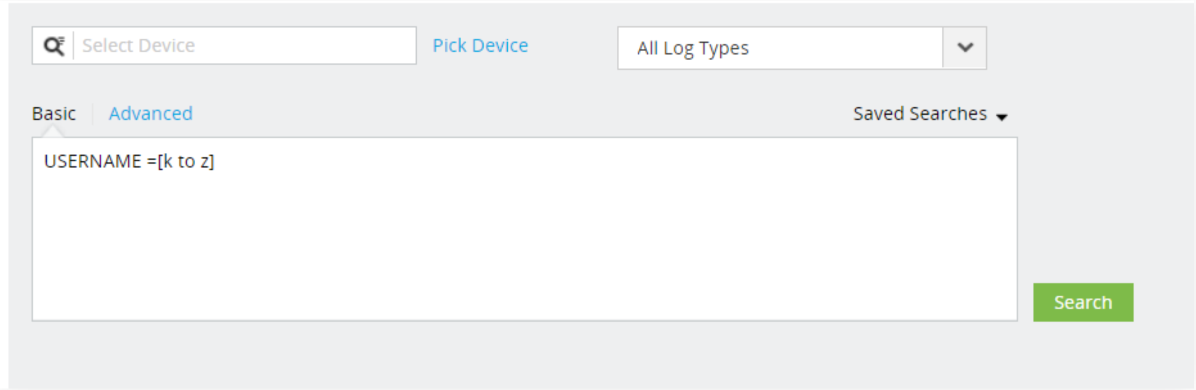


MESSAGE = "session"

Using ranges

This search option can be used to isolate incidents or logs that fall within a well-defined range. An expression with a range of values looks like the following: <field name> = [<from-value> TO <to-value>].

Example: If you wish to search from devices with the usernames starting from k to z, a range search query will look like this. USERNAME = [k TO z]

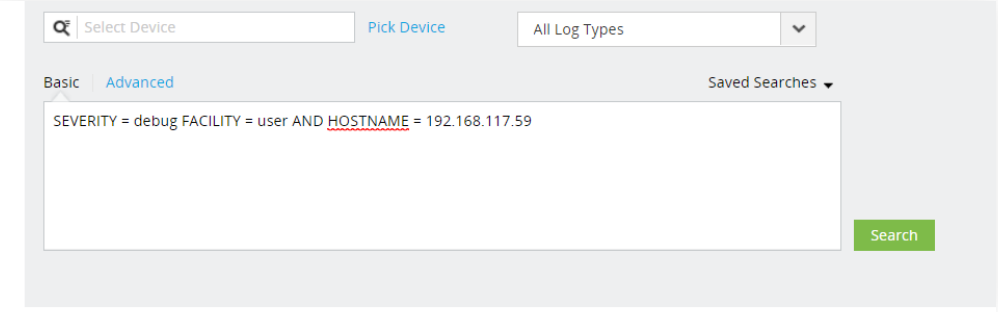


USERNAME =[k to z]

Using grouped fields

Grouped searches can be used when you wish to combine multiple search criteria in a single query. An expression with grouped fields looks like this: (<search criteria group>) <Boolean operator> <search criterion>

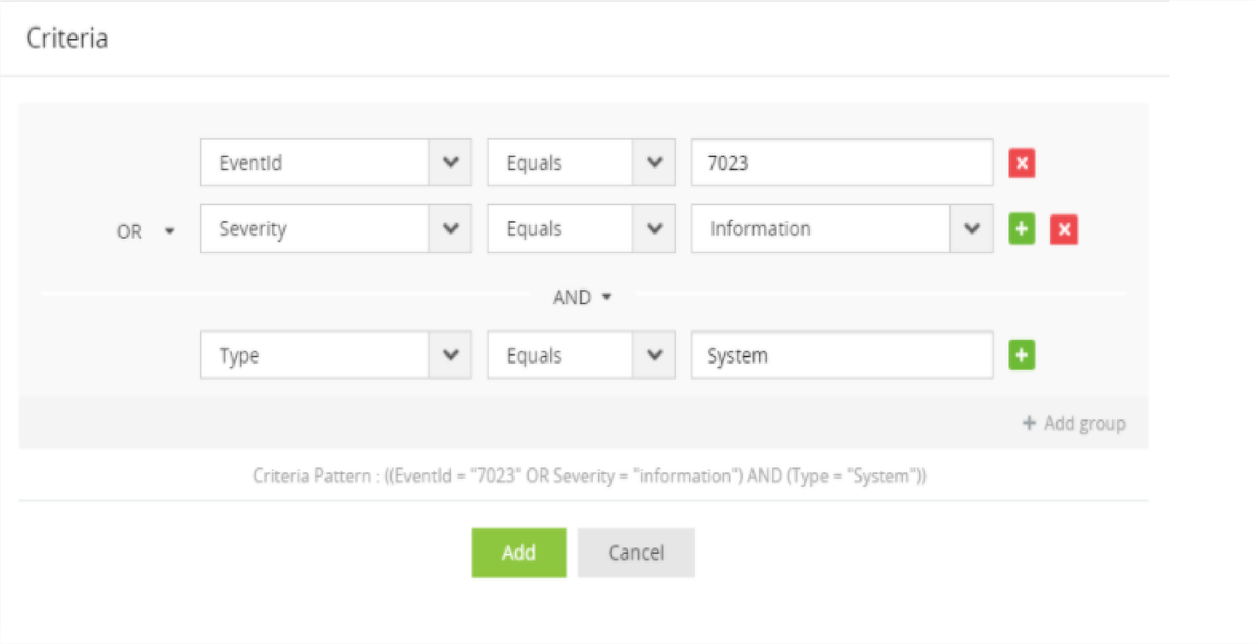
(SEVERITY = debug OR FACILITY = user) and HOSTNAME = 192.168.117.59



SEVERITY = debug FACILITY = user AND HOSTNAME = 192.168.117.59

Advanced search

The advanced search option enables you to build complex search expressions using the interactive search builder. By setting the required conditions listed in the drop-downs, you can create and save your search query for future use.



Criteria

	EventId	Equals	7023
OR	Severity	Equals	Information

AND

Type	Equals	System

Criteria Pattern : ((EventId = "7023" OR Severity = "information") AND (Type = "System"))

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine
Log360

$ Get Quote

⤓ Download