ManageEngine
EventLog Analyzer

Seamless security incident management with SIEM

www.eventloganalyzer.com

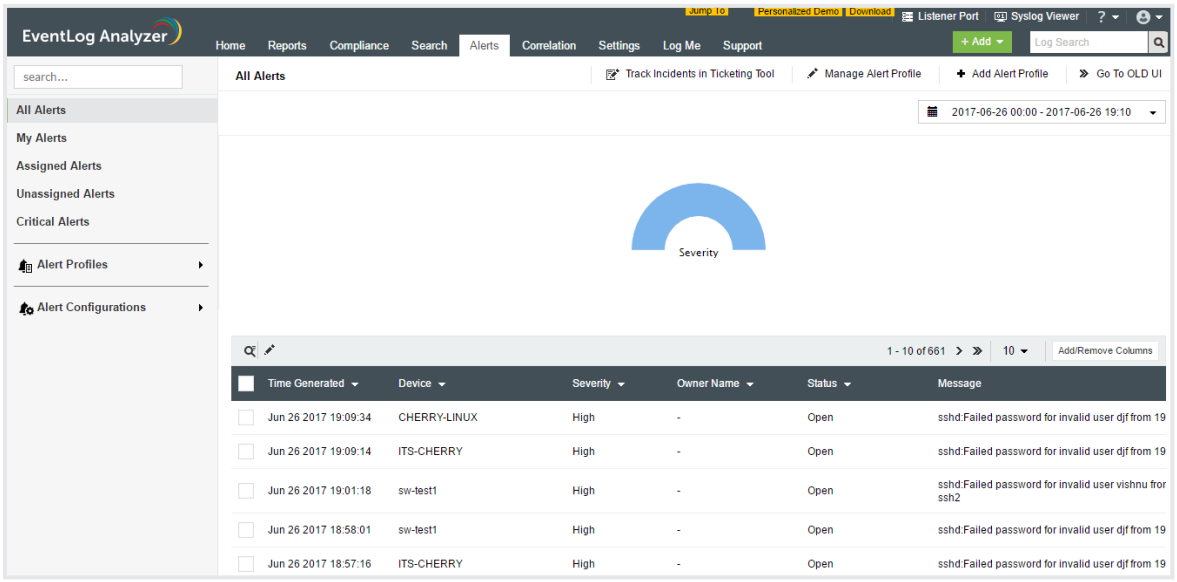
Seamless security incident management with SIEM

Incident detection and incident response are two equally critical sides of the same coin. Organizations strive to shorten the time it takes to detect and respond to security incidents in order to limit the time an attacker has to breach or disrupt their network. Using an effective system that can govern both incident detection and response, organizations can do just that. Incident management is the bridge that connects the two, allowing you to oversee an incident from detection to closure.

EventLog Analyzer's incident management module enables administrators to seamlessly manage security incidents in real time. Key features include:

- An intuitive incident dashboard that displays security incidents sorted by priority and source.
- A fully integrated internal system to assign incidents to responsible users and track their status.
- Automatic ticket assignment based on the device or device group that caused the alert, or manual assignment directly from the dashboard.
- Integration with popular external incident management tools, ManageEngine ServiceDesk Plus and ServiceNow.

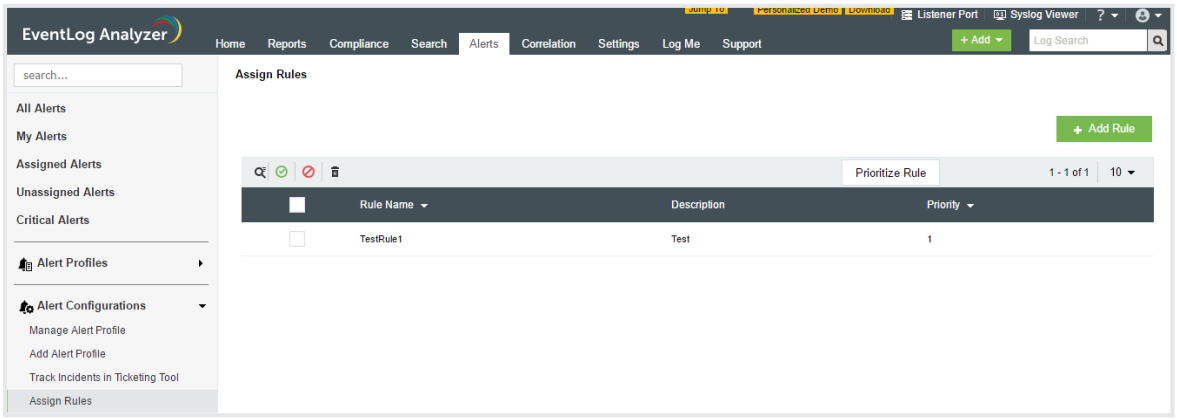
The incident dashboard



The main incident management dashboard can be accessed under the **Alerts** tab in EventLog Analyzer. Administrators can use this dashboard to:

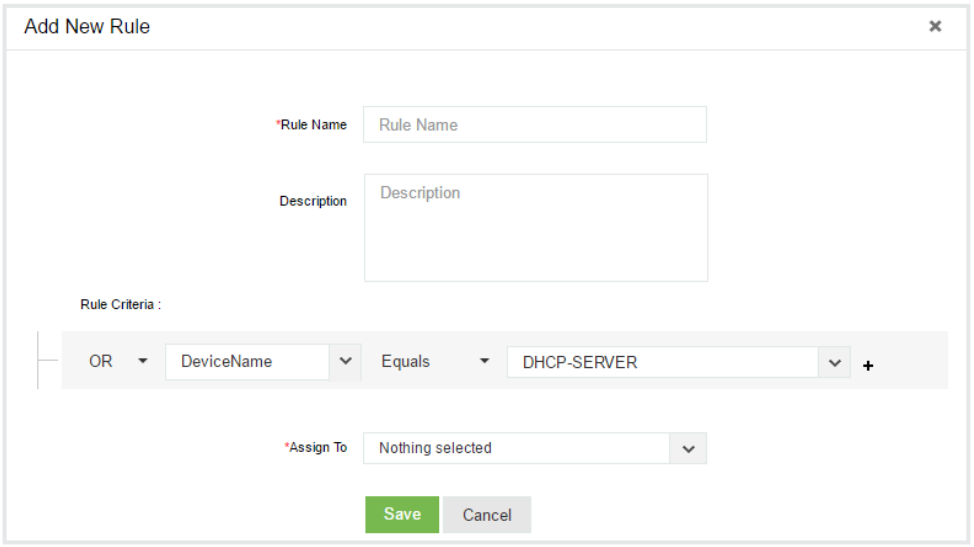
- View a report of all security incidents (or alerts) presented as a graph or table.
- Perform several ticket-related actions, including assigning tickets to specific users, updating the status (open, in progress, or closed), or adding any relevant notes using the update icon (✎).
- Select one of many different views of the information—namely, all alerts, alerts assigned to the logged-in user, assigned or unassigned alerts, all high-priority alerts, and all alerts belonging to a specific alert profile—from the left-hand menu.

Automatic ticket assignment



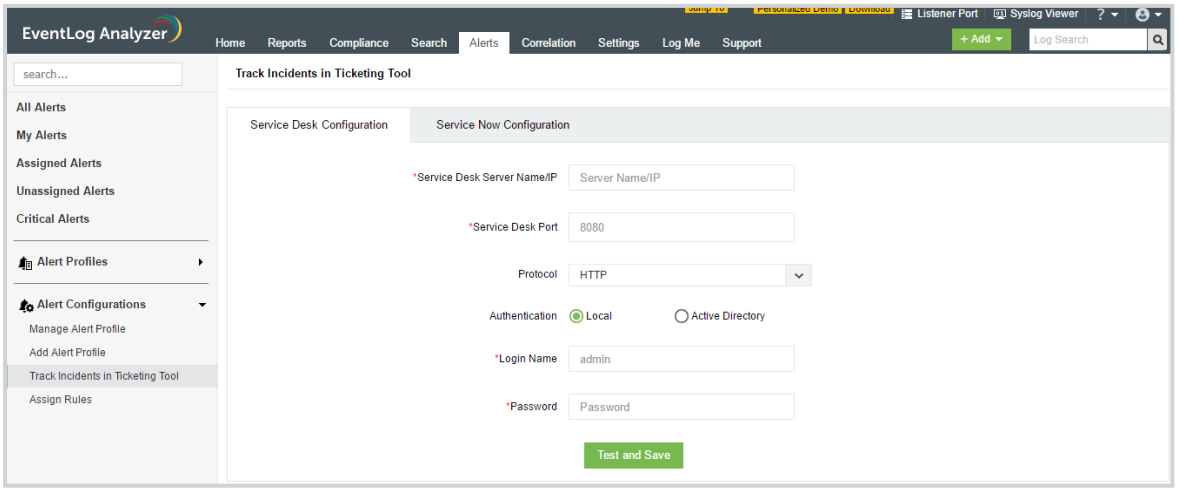
Using rules, EventLog Analyzer can automatically generate tickets as soon as an alert is triggered. Rules assign incidents to users based on the device or device group that triggered the alert. The list of rules can be accessed by selecting **Assign Rules** under **Alert Configurations** on the left-hand side of the incident dashboard. From here, administrators can:

- Add new rules by selecting the **Add Rule** button.
- Prioritize rules by selecting the **Prioritize Rule** button. If more than one rule is applicable to any device, the rule with the highest priority is used to assign the ticket.
- Enable, disable, or delete rules as needed.



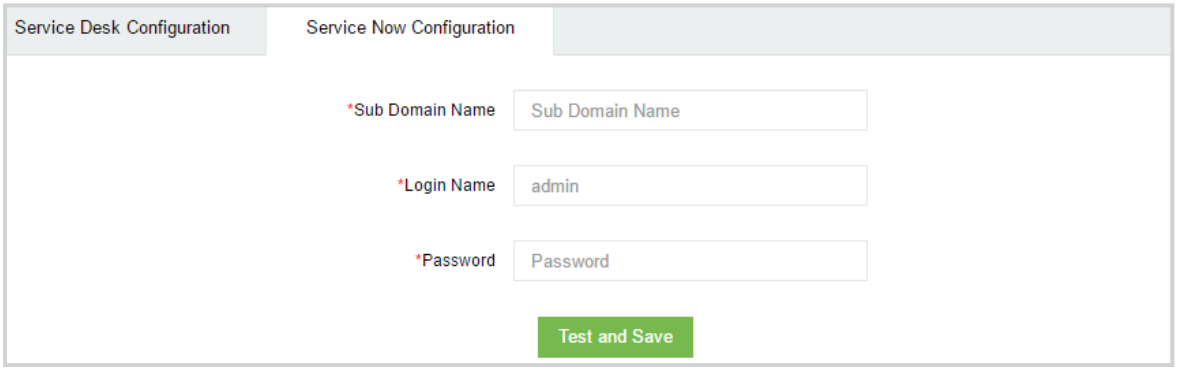
To add a new rule, enter a rule name, description (optional), the set of devices or device groups to which the rule applies, and the user the incident tickets will be assigned to.

External help desk integration



EventLog Analyzer also integrates with two popular help desk solutions, ManageEngine ServiceDesk Plus and ServiceNow. To set up an integration, select **Track Incidents in Ticketing Tool** from the main incident dashboard.

To integrate EventLog Analyzer with ServiceDesk Plus, enter the server name (or IP address), port number on which to send the incident information, communication protocol, and a pair of valid administrator credentials.



To integrate with ServiceNow, enter the sub domain name and a pair of valid administrator credentials.

Once EventLog Analyzer is integrated with either of these help desks, all incident information is forwarded to the ticketing software where it can be handled as needed.

EventLog Analyzer thus allows efficient incident management and ensures organizations stay on top of the entire life cycle of an incident, from detection to resolution.

About EventLog Analyzer

EventLog Analyzer is a comprehensive IT compliance and log management software for SIEM. It provides detailed insightsinto your machine logs in the form of reports to help mitigate threats in order to achieve complete network security.

Blog - https://blogs.manageengine.com/eventloganalyzer

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-timeservices and support. Worldwide, more than 60,000 established and emerging enterprises — including more than60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure,including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with officesworldwide, including the United States, United Kingdom, India, Japan and China.

Email:

support@eventloganalyzer.com

Or

Dial Toll Free:

+1 925 924 9500 (Toll Free)

+1-408-352-9254 (Direct)

Or

Visit www.eventloganalyzer.com for in-depth information about the solution and all its features.