

EventLog Analyzer **incident management with SIEM**

Solution guide



Seamless security incident management with a SIEM solution

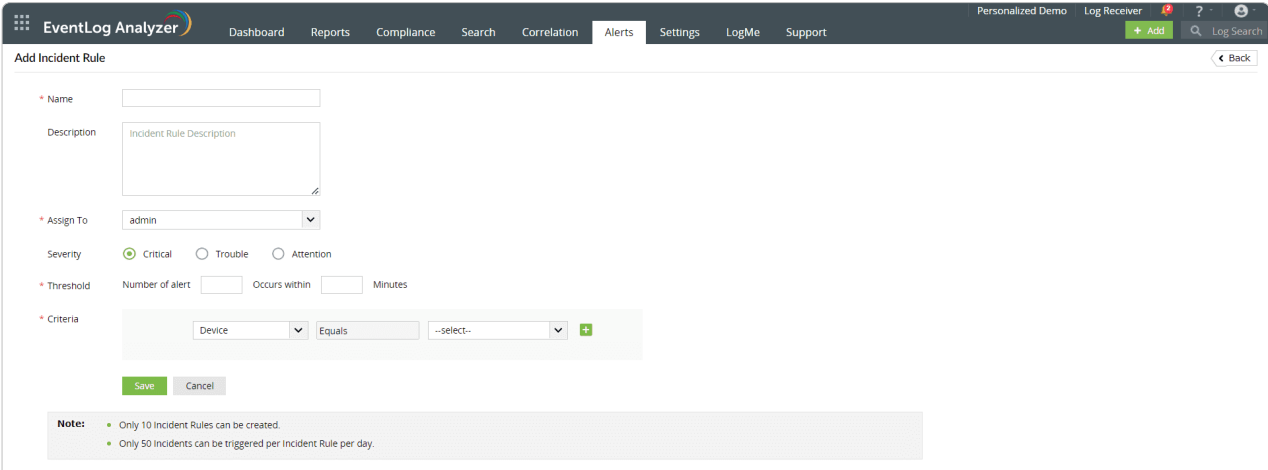
Incident detection and incident response are two equally critical sides of the same coin. Organizations strive to shorten the time it takes to detect and respond to security incidents in order to limit the time an attacker spends within their networks.

Using an effective solution that governs 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. It is a set of actions done to identify, investigate, and tackle the critical incidents that cause challenges for organizations.

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 their priority and source.
- A fully integrated internal system to assign incidents to specific technicians and track their statuses.
- Automatic ticket assignment based on the device or device group that caused the alert, as well as manual assignment directly from the dashboard.
- Integrations with popular external incident management tools like ManageEngine ServiceDesk Plus and ServiceNow.
- The execution of workflows to automate responses to an incident from a wide range of [supported actions](#).

Incident rule creation



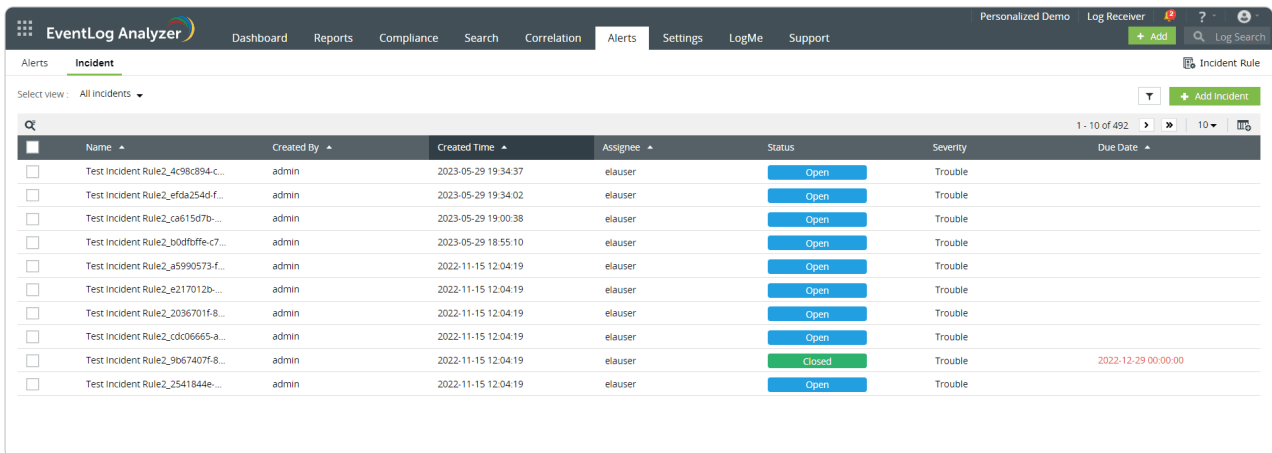
The screenshot shows the 'Add Incident Rule' form in the EventLog Analyzer interface. The form includes the following fields and options:

- Name:** A text input field.
- Description:** A text area with the placeholder text 'Incident Rule Description'.
- Assign To:** A dropdown menu currently set to 'admin'.
- Severity:** Radio buttons for 'Critical' (selected), 'Trouble', and 'Attention'.
- Threshold:** Two input fields: 'Number of alert' and 'Occurs within' (with 'Minutes' as a unit).
- Criteria:** A row of three dropdown menus: 'Device', 'Equals', and '--select--', followed by a plus sign icon.
- Buttons:** 'Save' and 'Cancel' buttons.
- Note:** A grey box containing two bullet points: 'Only 10 Incident Rules can be created.' and 'Only 50 Incidents can be triggered per Incident Rule per day.'

EventLog Analyzer automatically assigns a specific technician to a ticket with the help of incident rules. An incident rule includes the rule name, description, assignee, severity, threshold, and alert criteria. An incident gets identified and assigned to the appropriate technician if any of the alert criteria are met.

The Incident dashboard

The main **Incident** dashboard can be accessed under the **Alerts** tab in EventLog Analyzer.

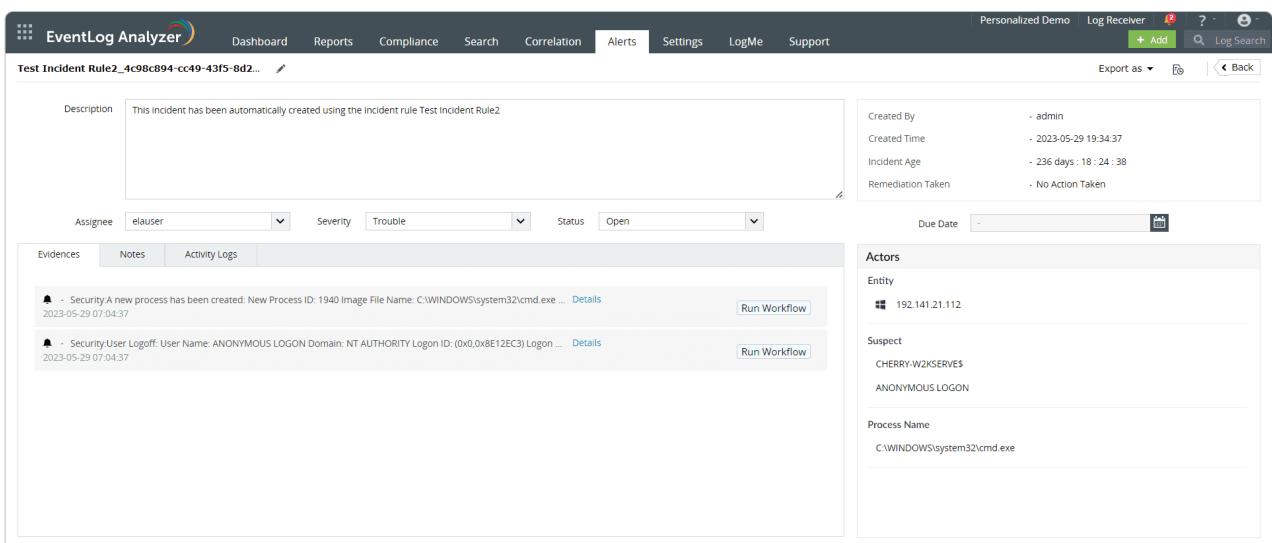


The screenshot shows the 'Incident' dashboard in EventLog Analyzer. It features a table with columns for Name, Created By, Created Time, Assignee, Status, Severity, and Due Date. The table contains 10 rows of test incidents. Most are in 'Open' status, while one is 'Closed'. The interface includes a search bar, a filter dropdown, and a '+ Add Incident' button.

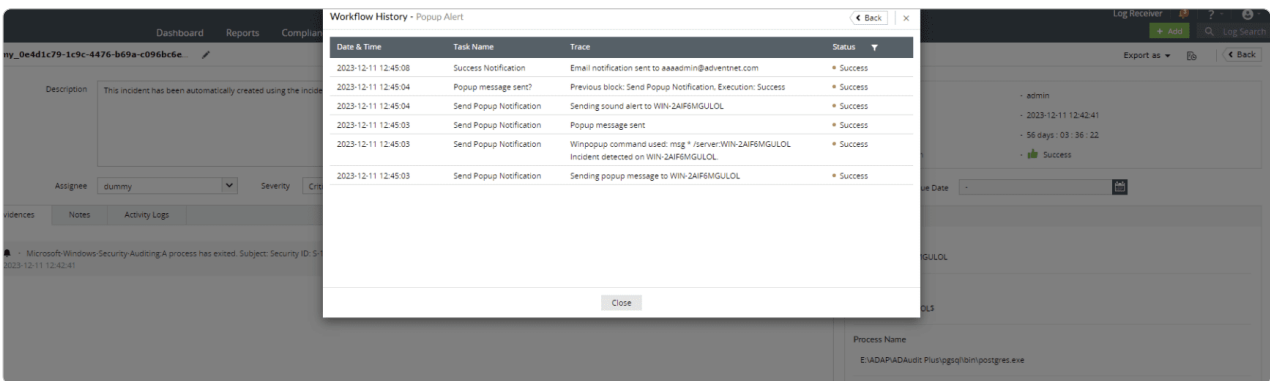
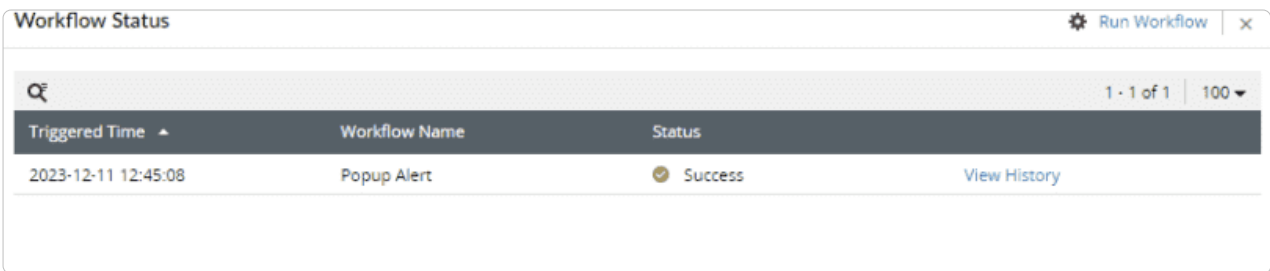
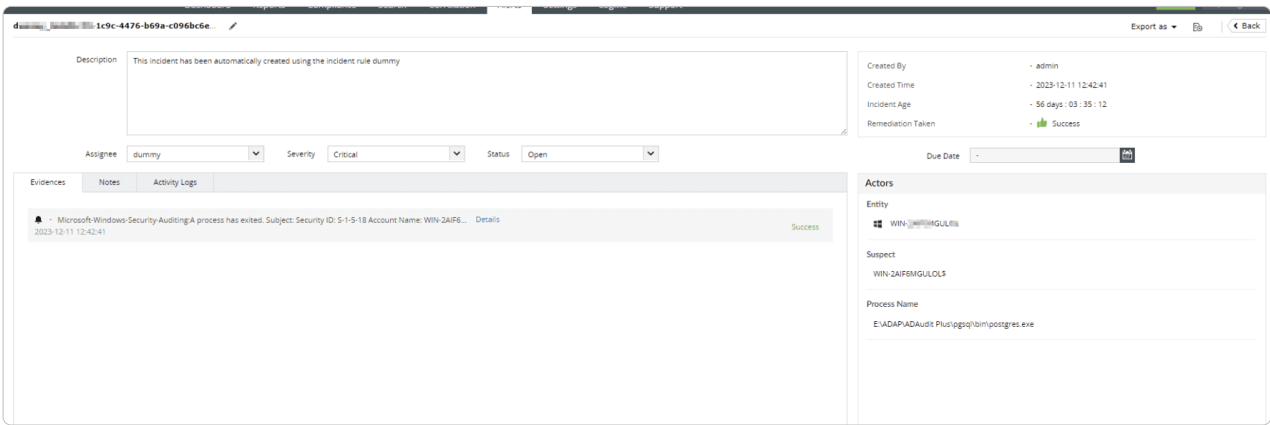
Name	Created By	Created Time	Assignee	Status	Severity	Due Date
Test Incident Rule2_4c98c894-c...	admin	2023-05-29 19:34:37	elauser	Open	Trouble	
Test Incident Rule2_efda254d-f...	admin	2023-05-29 19:34:02	elauser	Open	Trouble	
Test Incident Rule2_c615d7b-...	admin	2023-05-29 19:00:38	elauser	Open	Trouble	
Test Incident Rule2_b0dfbfe-c7...	admin	2023-05-29 18:55:10	elauser	Open	Trouble	
Test Incident Rule2_a5990573-f...	admin	2022-11-15 12:04:19	elauser	Open	Trouble	
Test Incident Rule2_e217012b-...	admin	2022-11-15 12:04:19	elauser	Open	Trouble	
Test Incident Rule2_2036701f-8...	admin	2022-11-15 12:04:19	elauser	Open	Trouble	
Test Incident Rule2_cdc06665-a...	admin	2022-11-15 12:04:19	elauser	Open	Trouble	
Test Incident Rule2_9b67407f-8...	admin	2022-11-15 12:04:19	elauser	Closed	Trouble	2022-12-29 00:00:00
Test Incident Rule2_2541844e-...	admin	2022-11-15 12:04:19	elauser	Open	Trouble	

Administrators can use this dashboard to:

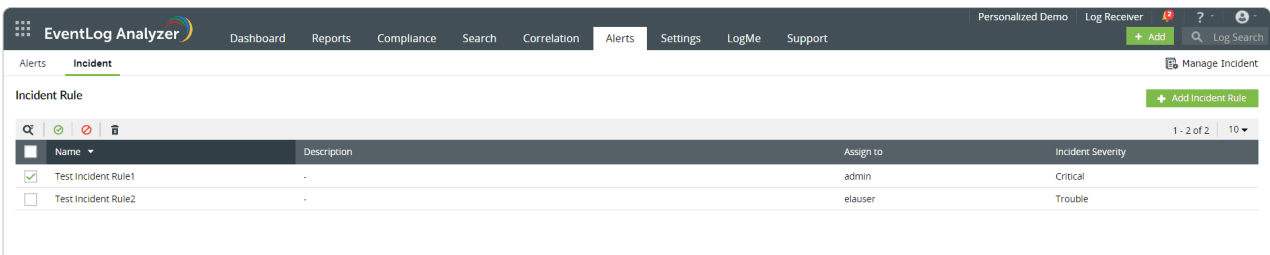
- Perform several ticket-related actions, including assigning tickets to specific technicians, setting the severity (*Critical, Trouble, or Attention*), updating the status (*Open, In Progress, or Closed*), or adding any relevant notes using the **update icon**.
- Attach evidence and notes related to the incident.
- Create activity logs that record and display the events pertaining to the creation, modification, and deletion of incidents.
- Select one of the many different views of the information from the left-hand menu: all alerts, alerts assigned to the logged-in technician, assigned alerts, unassigned alerts, all high priority alerts, and all alerts belonging to a specific alert profile.
- Execute workflows by selecting the sequence of steps from a wide-range of pre-defined actions that EventLog Analyzer shall perform in the event of an incident being detected.



The screenshot shows the details of an incident in EventLog Analyzer. The incident title is 'Test Incident Rule2_4c98c894-cc49-43f5-8d2...'. The description states: 'This incident has been automatically created using the incident rule Test Incident Rule2'. The interface includes fields for Assignee (elauser), Severity (Trouble), and Status (Open). There are also fields for Created By (admin), Created Time (2023-05-29 19:34:37), Incident Age (236 days : 18 : 24 : 38), and Remediation Taken (No Action Taken). The 'Evidences' section shows two security events: 'Security-A new process has been created' and 'Security-User Logoff'. The 'Actors' section lists the Entity (192.141.21.112), Suspect (CHERRY-WZKSERVES\ANONYMOUS LOGON), and Process Name (C:\WINDOWS\system32\cmd.exe).

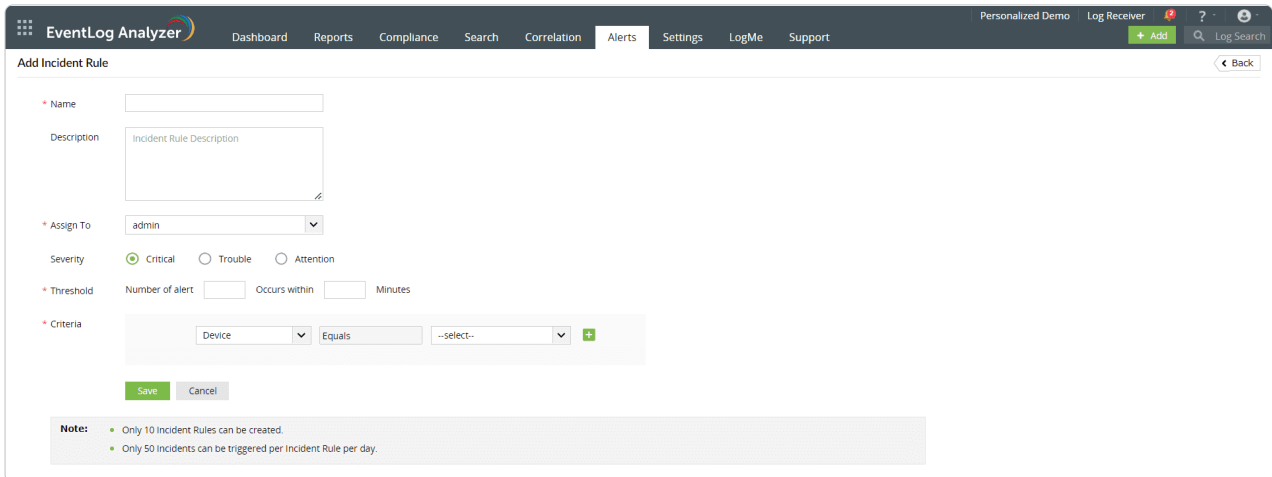


Automatic ticket assignment



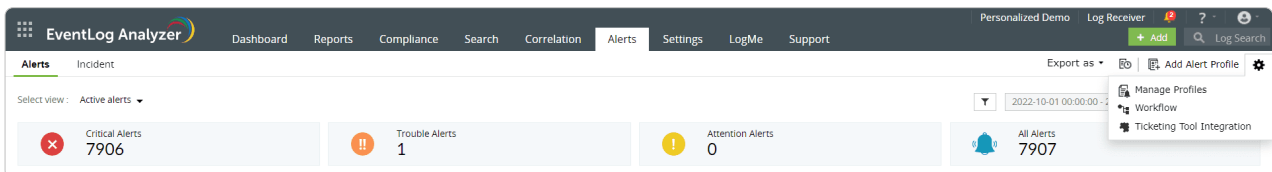
Using rules, EventLog Analyzer can automatically generate a ticket as soon as an alert is triggered. Rules assign incidents to technicians based on the set alert criteria, which are the devices or device groups that triggered the alert. The list of rules can be accessed by going to the **Incident** dashboard on the **Alerts** tab and clicking **Incident Rule** in the top-right corner. From here, administrators can:

- Add new rules by clicking the **Add Incident Rule** button.
- Prioritize rules based on an incident's severity.
- Enable, disable, or delete rules as needed.

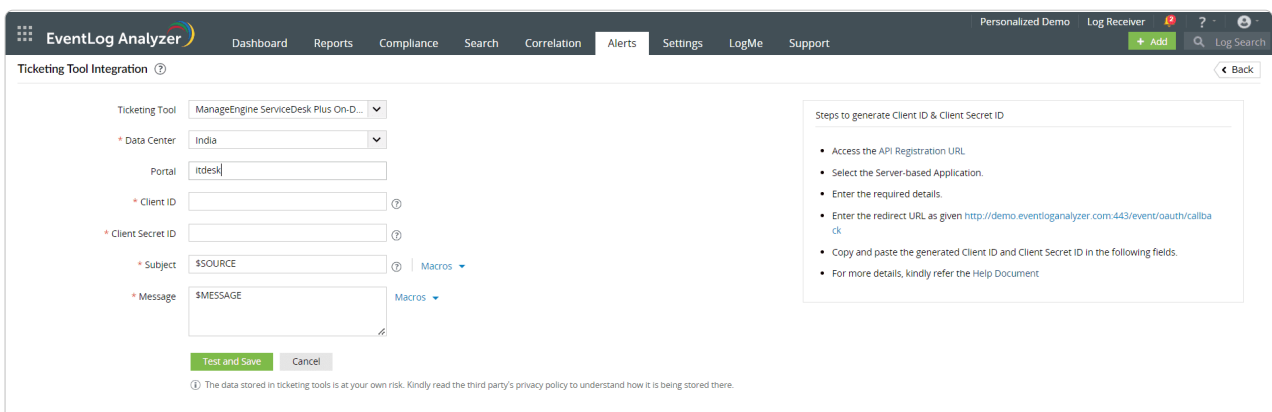


External help desk integrations

EventLog Analyzer also integrates with 11 popular help desk solutions. To set up an integration, go to the **Alerts** tab, click the **More tools** icon, and select **Ticketing Tool Integration**.



To integrate EventLog Analyzer with the respective help desk solution, click **Edit** in the top-right corner. Now, you can select the *Ticketing Tool* that has to be integrated and the *Data Center*, then enter the *Portal*, *Client ID*, *Client Secret ID*, *Subject*, and *Message* details.



Once EventLog Analyzer is integrated with the help desk solution, 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 that organizations stay on top of the entire life cycle of an incident, from detection to resolution.

Our Products

AD360 | Log360 | ADAudit Plus | DataSecurity Plus | Exchange Reporter Plus
SharePoint Manager Plus

ManageEngine EventLog Analyzer

EventLog Analyzer is complete log management software that provides holistic cybersecurity. It collects, analyzes, and manages log data from over 700 log sources. With real-time security auditing capabilities, it's easier to monitor critical changes in all your end-user devices. EventLog Analyzer offers instant threat detection to uncover security threats using event correlation and threat feed analysis, and instant mitigation using automated workflows. For more information about EventLog Analyzer, visit <https://www.manageengine.com/products/eventlog/>.

\$ Get Quote

↓ Download