ManageEngine
Log360

A comprehensive security information and event management (SIEM) solution

Table of contents

What's Log360

Log360, a comprehensive SIEM solution, is an integration of two powerful auditing tools—EventLog Analyzer and ADAudit Plus. Log360 helps security professionals promptly detect, prioritize, and mitigate both internal and external attacks. With this solution:

- Track Active Directory changes—GPO, OU, security group, and permission changes—in real-time to secure your network from internal threats.
- Analyze log data from sources across the network to track down malicious incidents.
- Detect suspicious logon and logon attacks. Audit privileged user activities and sessions.
- Report security incidents with finer details that make forensic analysis easier.
- Detect suspicious user activities instantly to pre-emptively block insider attacks.

What does EventLog Analyzer do?

EventLog Analyzer, the log management module of Log360, is capable of collecting, analyzing, correlating, searching, and archiving log data from sources across the network including—perimeter devices such as routers, switches, firewalls, and IDS/IPS, applications such as databases, web servers, and vulnerability scanners, Linux/Unix machines, Windows servers, AWS EC2 instances, Hyper-Vs, and more. You name any device in the network, EventLog Analyzer processes its logs with its custom log parser. This tool also comes with a built-in correlation engine and threat intelligence platform that's capable of detecting external security attacks in real-time.

What does ADAudit Plus do?

ADAudit Plus, the real-time Active Directory (AD) auditing module of Log360, is capable of reporting any changes happening in your AD environment, including—changes to security groups, GPOs, OUs, and user permissions. This tool is capable of extensively auditing user activities in your domain to provide instant reports plus alerts on user logons, logoffs, failed logons, account lockouts, and more. Additionally, this tool provides reports on the reasons for logon failures, helping identify possible attacks from legitimate logon failures. ADAudit Plus comes with an account lockout analyzer that's capable of analyzing the account lockouts in your environment to track down logon attacks.

With the option to dig through both internal and external security attacks from a single console, Log360 is your best bet to defend your network.

Log360 Benefits

- **All-in-one solution:** Brings real-time AD auditing, log management, IT compliance management, file integrity monitoring, and threat intelligence in a single console.

- **Pay for what you use:** Depending on your needs, choose log management, AD auditing component, or both. We charge only for what you use and do not limit the volume of log data being collected and processed.

- **Tight license integration:** Log360's licensing is flexible. If you already use any of the components, it's easy to switch to Log360 without much effort.

How is Log360 licensed?

Log360 is licensed based on the number of log sources. Abiding by the pay for what you use model, Log360's base pack only includes the log management component. The Active Directory auditing and file integrity monitoring components are available as add-ons.

Components of Log360 license

<table>
<tr>
<td rowspan="2">

Log360 base pack

- **Devices**
  - Routers
  - Switches
  - Fire calls
  - IDS/IPS
  - Syslog servers
  - IBM AS400
- **Applications**
  - IIS web servers
  - Apache web servers
  - MS SQL database
  - Oracle database
  - Vulnerability scanners
  - Threat intelligent solutions
- **Windows servers**
- **Workstations**

</td>
<td>

Active Directory auditing
Add-on pack

- **Domain controllers**

</td>
</tr>
<tr>
<td>

File integrity monitoring
Or
File server auditing
Add-on pack

- **File servers**
- **NetApp/EMC**

</td>
</tr>
</table>

Why EventLog Analyzer users should consider Log360?

Log360 provides in-depth, real-time Active Directory auditing. Upgrade to Log360 and unlock:

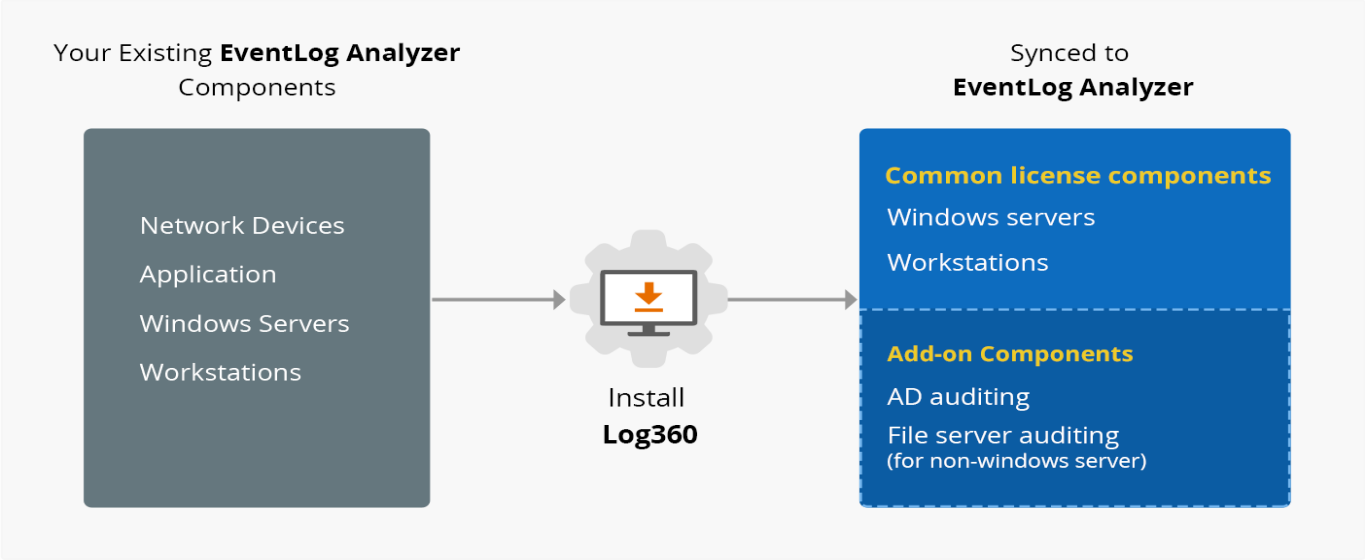
- **Real-time Active Directory auditing:** Track changes to GPO, security groups, OUs,DNS, ACL, and permissions.

- **Extensive user monitoring:** Audit user logon activities, analyze the reason for logon failures, monitor account lockouts, and more with predefined reports and real-time alerts.

- **Monitor files and folders:** Ensure integrity of confidential files stored in NetApp servers, EMC server, Windows file cluster, and more.

License benefit

EventLog Analyzer users can use their existing license to unlock the functionalities of the ADAudit Plus component in Log360. The common license components (Windows server and workstation) will be automatically synchronized with Log360 and come at no additional cost.



Why ADAudit Plus users should consider Log360?

Log360 provides comprehensive log management and network auditing. Upgrade to Log360 to:

- **Audit logs from network devices and apps:** Collect, analyze, correlate, and search logs from routers, switches, firewall, IDS/IPS, databases, web servers, and more to detect anomalies. With the built-in custom log parser, analyze any human readable log format.

- **Monitor database activities:** Track changes happening to database tables, schemas, and user accounts. Audit DML/DDL activities and ensure confidentiality of data stored in Microsoft SQL and Oracle databases.

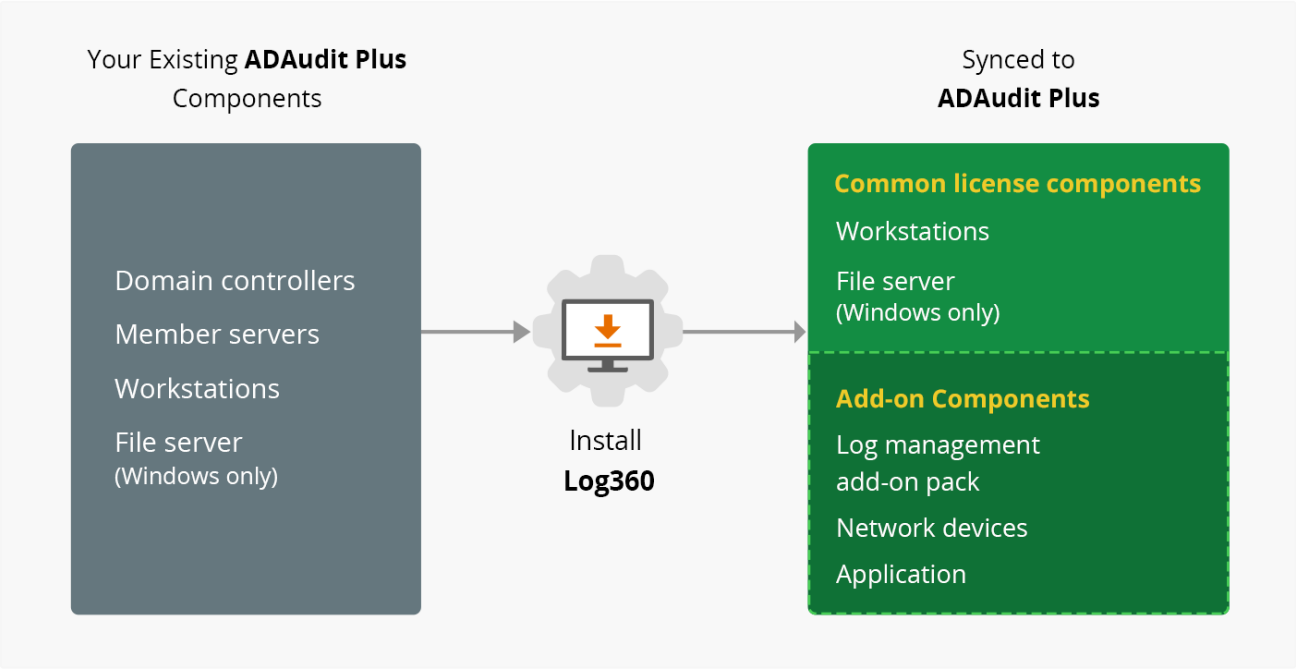
- **Web server log monitoring:** Analyze logs from IIS and Apache web servers, instantly detect DDoS attacks, malicious URL injections, cross-site scripting, and more.

- **Integrated threat management:** Get alerted upon malicious traffic to and from your network with the built-in global IP threat database and STIX/TAXII threat feed processors.

- **Built-in incident management system:** Ensure accountability for security incidents by raising tickets in help desk tools (ServiceDesk Plus and ServiceNow) for every alert triggered.

License benefit

Customer can use their existing ADAudit Plus license and unlock the functionalities of the EventLog Analyzer component in Log360. The common license component (Member servers, workstations, and Windows file servers) will be automatically synchronized with Log360 and be available at no additional cost.



Steps to upgrade to Log360

Existing EventLog Analyzer users:

1. Check whether the EventLog Analyzer build you're using is 11000 and above. If not, upgrade to the latest build or to 11000.

2. Start Log360 as a service.

3. Ensure that Log360 service is running. Open your browser and connect to Log360's web-console by typing localhost:8095. By default, Log360 runs in port 8095.

4. Click on the License link on the top right corner of the web-console. Browse and select your Log360 license file and click Apply.

5. Now, integrate your existing EventLog Analyzer installation with this Log360 installation by following the steps below:

    a. Click on Admin tab.

    b. In the Integration Settings page that opens, click on EventLog Analyzer tab.

    c. In the Server Name or IP field, provide the server name or the IP address of the machine wherein your EventLog Analyzer installation is running.

    d. In the Port field, specify the port number of EventLog Analyzer. By default, EventLog Analyzer runs in port 8400.

    e. Select the protocol (HTTP/HTTPS) in the Protocol field.

    f. Click on the Integrate button.

Existing ADAudit Plus users:

1. Download Log360 from our site.
2. Install and start Log360 as a service.
3. Open your browser and connect to Log360's web-console by typing localhost:8095.
4. Click on the License link on the top right corner of the web-console. Browse and select your Log360 license file and click Apply.
5. Now, to integrate your existing ADAudit Plus installation with this Log360, navigate to Admin tab.
    a. In the Integration Settings page that opens by default, click on ADAudit Plus tab.
    b. In the Server Name or IP field, provide the server name or the IP address of the machine wherein your ADAudit Plus installation is running.
    c. In the Port field, specify the port number of ADAudit Plus installation. By default, ADAudit Plus runs in port 8081.
    d. Select the protocol (HTTP/HTTPS) in the Protocol field.
    e. Click on the Integrate button.

Benefits to resellers

- Single package for SIEM, which means it's an easy security product to push.
- Integrated licensing model for effortless and seamless upgrading.
- Future security enhancements (Office 365 auditing, Exchange auditing, user entity behavioral analysis, threat intelligence enhancements, and the like) will get included in this console to make Log360 a strong SIEM solution.
- Security package at an affordable price.