ManageEngine
Log360

Log360 license components

Explained

Component	When you need this	What you need to do	Pricing criteria
Log sources	To collect logs from Syslog devices Window servers, IIS sites, MSSQL servers, Linux file servers, other applications and VMs .	Specify the number of log sources in your network. If a machine's OS and applications are both being monitored, only one log source license is needed for that system.	Based on the number of devices added as log sources, with a minimum of 10 log sources required.
Endpoints	For auditing your Windows and Mac endpoints.	Mention the number of endpoints that you wish to audit.	Available as a pack of 100. Base pack - 100 workstations.
Cloud accounts	To monitor and audit events happening in cloud sources such as Office 365 tenants and AWS accounts.	Specify the number of Office 365 tenants and AWS accounts.	There's no base pack or minimum value for cloud tenants.
Domain controllers	To audit the activities happening in your Active Directory	Mention the number of domain controllers you wish to audit.	Based on the number of domain controllers added, with a minimum of 2 domain controllers.
File servers	To audit file servers including, Windows File Servers, NetApp, EMC, Huawei, CTERA, Synology, QNAP, Nutanix, Azure File Share, and Amazon FSx servers.	Specify the number of file servers for which you need to perform file auditing.	There's no base pack or minimum value for the number of file servers

Add-ons

Component	When you need this	What you need to do	Pricing criteria
AD backup and recovery	To back up and restore Active Directory objects, attributes, and domain configurations.	Enable the add-on	Based on the number of domain controllers purchased

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus | Exchange Reporter Plus | M365 Manager Plus

About Log360

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, an analytical Incident Workbench, 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.

$ Get Quote

⤓ Download