ManageEngine
Log360

Log360 license components

Explained

Component	When you need this	What you need to do	Pricing criteria
Domain controller	To audit the activities happening in your Active Directory	Mention the number of domain controllers you wish to audit.	There's no minimum limit for the number of domain controllers.
Member server	To audit the activities happening in your Windows servers.	Specify the number of member servers you wish to audit.	Base pack: 5 member servers. To get a quote/purchase Log360 for less than 5 member servers, contact log360-support@manageengine.com
Workstation	For auditing your workstations.	Mention the number of workstations that you wish to audit.	Available as a pack of 100. Base pack - 100 workstations.
Applications	To monitor and audit security events happening in business-critical applications such as Oracle databases, Apache web servers, DHCP Linux/Windows applications, vulnerability scanners, threat intelligence solutions, and more, choose this component.	Collectively specify the number of applications that you wish to monitor. **Note:** Separate add-ons are available for in-depth SQL server auditing and IIS server auditing. Refer to those components for further details.	Base pack: 5 applications. To get a quote/purchase Log360 for less than 5 member servers, contact log360-support@manageengine.com

Other devices	To audit Linux/Unix devices, IBM AS400 systems, routers, switches, firewalls, IDS/IPS, and other syslog devices.	Collectively specify the total number of syslog devices that you wish to audit using Log360.	Base pack: 5 devices. To get quote/purchase Log360 support for less than 5 devices, contact log360-support@manageengine.com
Add-ons			
User and Entity Behavior Analytics (UEBA)	To identify anomalies in user and entity behavior.	Simply select the feature. No need to specify any other details.	There are no criteria.
FIM/File server auditing	To audit file servers including Linux file servers, Windows file servers, and NetApp servers.	Specify the number of Linux, Windows, and NetApp file servers for which you need to perform file auditing.	There's no base pack or minimum value for this add-on.
SQL server auditing	This add-on helps audit activities happening in SQL servers and also performs SQL database activity monitoring.	Specify the number of SQL servers that you wish to audit exclusively using the **Microsoft SQL database auditing** add-on.	There's no base pack or minimum value for this add-on.

IIS server auditing	This add-on helps audit the IIS servers and sites that are available in your network.	Specify the number of IIS sites available in your network.	There's no base pack or minimum value for this add-on.
Advanced threat analytics	To accurately identify and assess the severity of threats posed by potentially malicious URLs, domains, and IP addresses intruding into your network by corroborating data from third-party threat intelligence services.	Simply select the feature. No other details are needed.	There are no criteria.
Azure AD/Office 365 auditing	This add-on helps you audit Azure AD, Exchange Online, Microsoft Teams and other Office 365 services used in your organization.	Specify the number of Office 365 tenants.	There's no base pack or minimum value for this add-on.
Active Directory Reporting	To closely monitor your Active Directory objects.	Simply select the feature. No need to specify any other details.	There are no criteria.
Exchange server auditing	To audit the Exchange server environment.	Specify the number of Exchange servers that you want to audit.	There's no base pack or minimum value for this add-on.