ManageEngine
Log360

LOG360 UEBA
BEST PRACTICES GUIDE

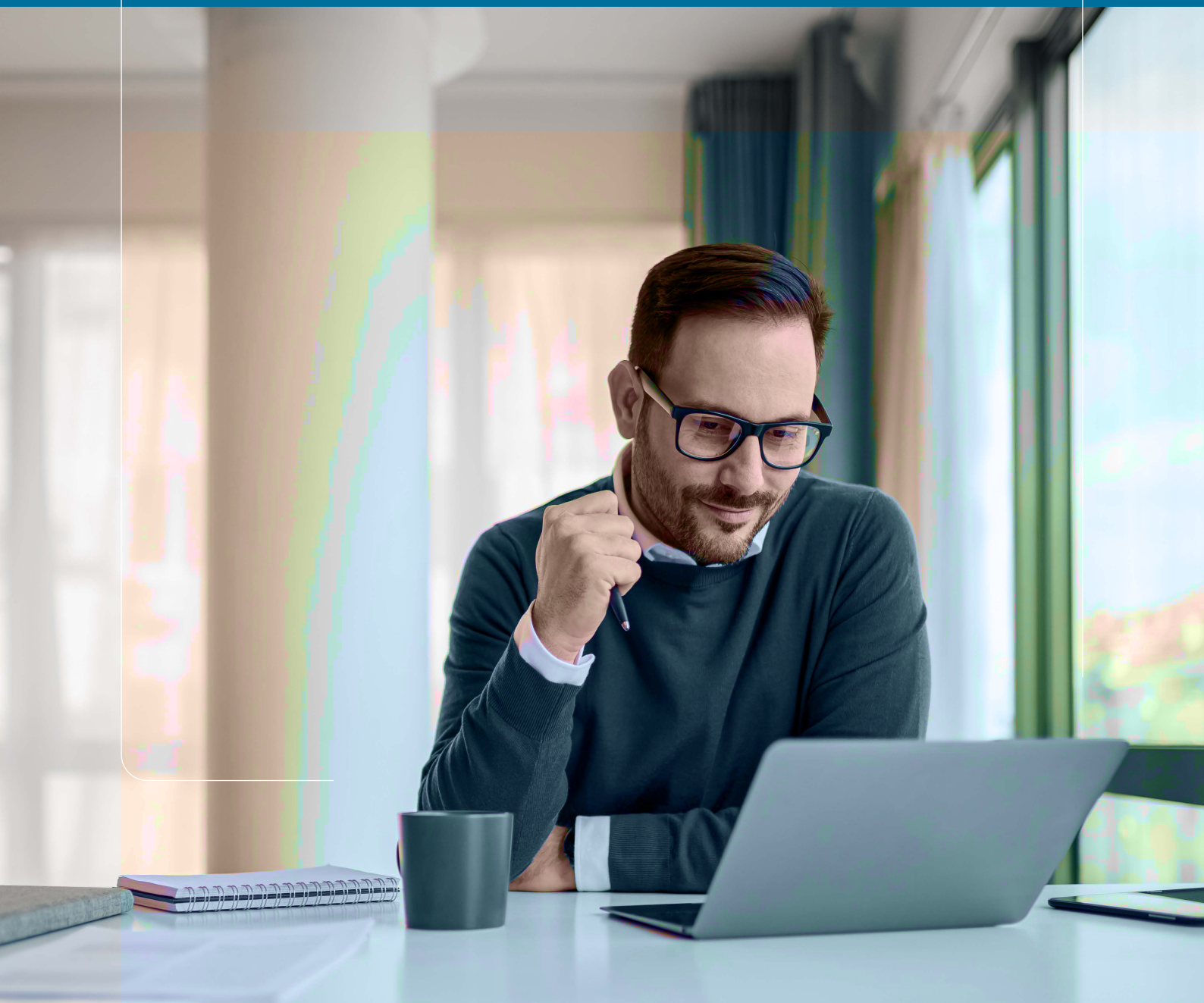

Table of contents

This guide details best practices which, if followed, ensure smooth operation and optimum performance of Log360 UEBA.

System requirements

Hardware requirements

A dedicated server with the following hardware configuration,

Hardware	Minimum	Recommended
Processor	2.0 GHz	2.4 GHz
Core	Dual core	8 Core
RAM	4 GB	8 GB
Disk Space	40 GB	100 GB

Operating Systems

ManageEngine Log360 UEBA supports the following Microsoft Windows operating system versions:

- Microsoft Windows 2003
- Microsoft Windows 2008
- Microsoft Windows 2008 R2
- Microsoft Windows 2012
- Microsoft Windows 2012 R2
- Microsoft Windows 2019
- Microsoft Windows 2022
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows 11

Web Browsers

ManageEngine Log360 UEBA requires one of the following browsers to be installed on the system to access the Log360 UEBA web client.

- Internet Explorer 9 and above
- Firefox 4 and above
- Chrome 10 and above
- Safari 5 and above

Databases

- Microsoft SQL Sever 2005
- Microsoft SQL Sever 2008
- Microsoft SQL Sever 2014
- Microsoft SQL Sever 2016
- Microsoft SQL Sever 2019
- Microsoft SQL Sever 2022
- PostgreSQL 10.21

General Recommendations

VM infrastructure

- Allocate 100 percent RAM/CPU to the virtual machine running Log360 UEBA. Sharing memory /CPU with other virtual machines on the same host may result in RAM/CPU starvation and may negatively impact Log360 UEBA's performance.

- Employ thick provisioning, as thin provisioning increases I/O latency. In case of VMware, Select Thick provisioned, eagerly zeroed as lazily zeroed is lower in performance.

- Enabling VM snapshots is not recommended as the host duplicates data in multiple blocks by increasing reads and writes, resulting in increased IO latency and degraded performance.

CPU & RAM

- Server CPU utilization should always be maintained below 85% to ensure optimal performance.

- 50% of server RAM should be kept free for off-heap utilization of Elasticsearch for optimal performance.

Installation server

- UEBA solutions are resource-intensive. It is recommended to provide a dedicated server for their optimal performance.

- Log360 UEBA uses Elasticsearch. Elasticsearch process is expected to utilize off-heap memory for better performance. Off-heap memory is maintained by the operating system and will free up when necessary.

Optimizing hard disk space

The two main contributing factors to hard disk space are the database and archive files. The database (or index) files contain the most recent log or anomaly data, which can be reported on and searched, while the archive files contain the older, historic log or anomaly data. Archive files need to be loaded into the product first before they can be searched or reported on.

Anomaly data is stored in the database and is periodically compressed and stored among the archive files. The longer the retention period in the database, the greater is the hard disk space needed and lower is the database performance. The default retention period is 32 days and is configurable (Settings > Admin settings > DB retention settings). Minimize this value to obtain optimum performance.

Securing Log360 UEBA

Installation configuration

The operating system user account used to install and run the product must be the same and must have permissions on all installed folders and subfolders. While it is not necessary for the root account to be used on a Windows system, only the default administrator account must be used.

User configuration

It is best to change the default passwords for the admin and guest user accounts in the Log360 UEBA web client (My Account -> Change Password)).

SSL certification

Log360 UEBA server-client communication can be secured using the SSL (Secure Sockets Layer) protocol. The SSL certification guide offers detailed steps on how to obtain SSL certification.

Two-factor authentication

Two-factor authentication strengthens the security posture of Log360 UEBA. Upon enabling two-factor authentication, users will be authenticated using secondary authentication mechanisms in addition to their Active Directory credentials. These authentication mechanisms include:

- Email verification
- SMS verification
- Google authenticator
- RSA SecurID
- Duo Security
- RADIUS Authentication
- Backup Verification Code

Database best practices

Secure database

For smooth and seamless installation, Log360 UEBA makes use of the MS SQL or PostgreSQL database default root/postgres user without password. It is recommended to assign a password to this account in order to further secure the database.

This is not needed in case of MS SQL, as a valid user account with credentials needs to be provided during installation itself.

Backup database

It is recommended to back up the Log360 UEBA database every fortnight, so that data is not lost in case of any disaster. The database files are located in the <ManageEngine>/<Log360 UEBA>/mssql or <ManageEngine>/<Log360 UEBA>/pgsql folder, as applicable to the build number. To back up the data, stop the Log360 UEBA service, and take a copy of all files and folders in the location. This can be done manually or using any third-party back up software. If restoring data from a backup, ensure that the build number of the product is the same as when the backup was taken.

Optimizing log search performance

Give sufficient heap to the Elasticsearch

To ensure fair performance maintain the heap to data ratio of 1:60. This means that you can allocate approximately 1GB of memory (heap) for every 60GB of data in the Elasticsearch node (the maximum ratio). But for better performance, you can lower this ratio (i.e., 1:30 is better than 1:60) and increase speed.

Elasticsearch also uses file-system cache to provide faster searches. It is recommended to have enough free space on your RAM equivalent to that of the heap memory allocated for Elasticsearch. If this is not feasible, then ensure at least 30% of the server's RAM is free. OS will use this free RAM to cache the Elasticsearch's indices to provide better performance.

Note: Heap allocated to Elasticsearch shouldn't exceed 16GB.

Example:

Suppose we have **100GB of search data**, then the heap size for Elasticsearch should be at least **→ 100/30 ~ 4GB**.

Insufficient heap is the underlying reason for several performance issues such as

- Slow alert processing / indexing performance
- Cached record
- Delayed search results
- Failed searches

Steps to check the Elasticsearch data size

1. Navigate to **<ManageEngine>/<Log360 UEBA>/ES/config.**
2. Open the **elasticsearch.yml** file in the config folder.
3. Look for **path.data** setting in this file. Navigate to the data folder specified in the **path.data** setting and check the size of the folder.

Steps to adjust heap (memory)

1. Navigate to **<ManageEngine>/<Log360 UEBA>/conf.**
2. Open the configuration file **→ wrapper.conf** and view the heap size.

Note: Make sure the logged in user has permissions to write.

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=256

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024
```

3. Heap size is written in MB. Edit wrapper.java.initmemory and wrapper.java.maxmemory values to increase the heap size. Here it is set at 256 and 1024 respectively.
4. If it has to be increased to 16 GB, then we need to set wrapper.java.maxmemory to 16 * 1024 = 16384.

Note:

- In the event of **OutOfMemory** and **LowMemory** errors, the Elasticsearch heap will automatically expand up to one-third of the available RAM on the machine.
- It's important to note that increasing the heap size isn't always the solution to improve performance. Apart from heap, other factors like Disk and CPU may also cause performance problems. Ensure that the System Requirements are met.
- It is also important to monitor the memory usage regularly to ensure that the system is performing efficiently and to adjust the settings if necessary.
- Keep in mind that increasing the Elasticsearch heap size should be done with careful consideration of the available resources on your machine.

Ensure that disk is not the bottleneck

If the server is generating cached records (i.e., log processing is slow) or if the searches are slow, then you can:

a. Use faster storage as mentioned in the System Requirements page.

b. Check if the disk where the data is stored is not fragmented.

c. In **Windows Resource Monitor**, you can check the **Disk** tab. If the **Disk Activity** shows the **Highest Active Time** to be always 100%, it indicates that the disk might have issues or is not fast enough.

Support best practices

Create Support Information File (SIF)

When support is required, creating a Support Information File (SIF) to send to the support team (support@log360.com) would be helpful and time saving. To create a SIF from the web client, go to the Support tab of the product. Click on 'Create Support Information File', wait 30-40 seconds, and click on the Support tab again. Click on download and send the downloaded SIF to the support team, or click 'Upload to FTP Server', provide the required details and submit. If the server or web client is not working, zip the files found at <ManageEngine>/<Log360 UEBA>/logs and upload the zip file in this FTP link.