ManageEngine
Log360

Security hardening

for Log360 UEBA

Table of contents

Abstract

It is crucial for all IT administrators to bolster security within their current infrastructure to prevent potential breaches, given the growing emphasis on information security. This document focuses on the ideal configurations for Log360 UEBA to ensure the safety of your data.

Security hardening for Log360 UEBA

Securing the built-in admin account

Log360 UEBA comes with a built-in admin account with ultimate privileges. By default, this account's password is the same for every customer, which means you need to change this password in order to properly secure it. If this step is overlooked, you will leave your system vulnerable. You can change the default password by navigating to **My Account > Change Password.**

Enabling HTTPS for secure communication

We recommend that you use HTTPS over HTTP to ensure secure transportation of information between your Log360 UEBA database and the web client. You can do this from within the user interface under the Settings tab. Navigate to **Settings > Product Settings**. Select **Log360 UEBA (https)** and enter the HTTPS port number.

These settings can be further optimized from within the following XML file in the installation directory:

- conf\server.xml > Connector (find the HTTPS connector corresponding to your configured port number).

If you choose to allow only a particular version of Transport Layer Security (TLS)—namely TLSv1, TLSv1.1, or TLSv1.2—you can disable the other versions by modifying the following parameter, keeping only the required TLS versions:

- sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

Refer here to learn how to configure SSL for Log360.

With these changes, you can secure all communication through Log360 UEBA.

Restricting logon access to the Log360 UEBA server

To further strengthen Log360 UEBA's security, we recommend that you restrict logon access to the Log360 UEBA server, thereby preventing unwarranted access. You can define the local policy settings in the User Rights Assignment tab within the Group Policy Management Editor to **Allow log on locally** or **Allow log on through Remote Desktop Services**, and do so only to a specific set of users. This way, you reduce the attack surface of your infrastructure.

Restricting access to the Log360 UEBA installation folder

The Log360 UEBA installation directory contains important files required for it to function properly, including files that are used to start and stop the product and the license file.

Unauthorized users can be prevented from accessing the Log360 UEBA installation directory in two ways:

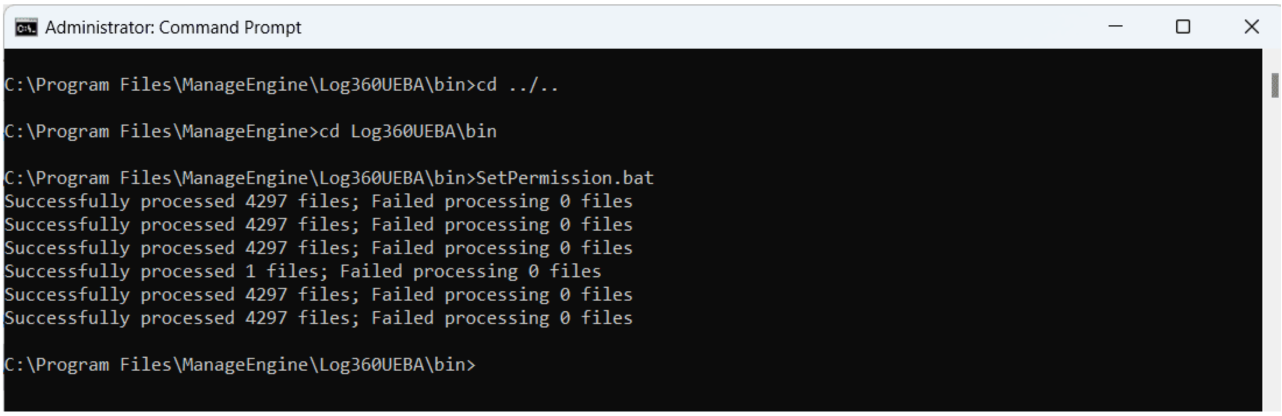
I. Run the SetPermission.bat file
II. Modify required permissions manually

I. Restricting access using SetPermission.bat

By this process, access to the installation directory is automatically restricted to only the necessary accounts. There are two ways to do this:

Option 1: Update to build 4050. Navigate to the "**<Installation Directory>/bin**" folder (by default C:\Program Files\ManageEngine\Log360UEBA\bin) and run the **SetPermission.bat** file from the elevated Command Prompt.

Option 2: Download the zip file using this link. Extract the zip and move "**SetPermission.bat**" to the "**<Installation Directory>/bin**" folder. Run the **SetPermission.bat** file from the elevated command prompt. (See figure below)



```
C:\Program Files\ManageEngine\Log360UEBA\bin>cd ../..

C:\Program Files\ManageEngine>cd Log360UEBA\bin

C:\Program Files\ManageEngine\Log360UEBA\bin>SetPermission.bat
Successfully processed 4297 files; Failed processing 0 files
Successfully processed 4297 files; Failed processing 0 files
Successfully processed 4297 files; Failed processing 0 files
Successfully processed 1 files; Failed processing 0 files
Successfully processed 4297 files; Failed processing 0 files
Successfully processed 4297 files; Failed processing 0 files

C:\Program Files\ManageEngine\Log360UEBA\bin>
```

II) Modify required permissions manually

To modify access permissions on the Log360 UEBA installation directory for unnecessary user accounts manually, follow the steps below:

- Disable Inheritance for the installation directory (by default C:\Program Files\ManageEngine\Log360UEBA). Refer to the Appendix for step-by-step instructions.
- Remove access permissions for all the unnecessary users. Refer to the Appendix for step-by-step instructions.
- Assign **Modify** Control permission for the installation directory folder to users who can start or stop the product. Refer to the Appendix for step-by-step instructions.
- If the product is installed as a service, ensure that the account configured under the **Log On** tab of the service's properties has been assigned **Modify** permission for the installation directory.

Securing your database with additional password protection

Log360 UEBA comes with a built-in, password-protected PostgreSQL database, allowing only authorized personnel access. By default, the PostgreSQL service creates a user account with unrestricted privileges (similar to a domain administrator account in AD) to perform various administrative actions. Log360 UEBA changes the default password of this account and creates another user account with limited privileges. This new account with restricted permission is used to connect to the database, and is encrypted to ensure security.

Delegating and auditing technicians

Technician roles can be configured to limit access to certain reports. These roles can also restrict technicians from performing administrative functions such as adding or removing sources for auditing, modifying configuration settings, etc. In addition, Log360 UEBA provides a detailed user-based audit trail of all actions performed.

Restricting database access from within the UI

Log360 UEBA, by default, disables database access from within its user interface and permits only the default administrator account to enable this option. The default admin account can access the database by appending /runQuery.do to the product instance URL. The administrator can also choose which other accounts have this privilege while creating the corresponding user accounts. This prevents other technician accounts from modifying or deleting information from the database.

Protecting exported and scheduled reports

When a user exports a report in a particular format (PDF, CSV, etc.), or when a user schedules a particular report to be saved locally, the files are password protected by Log360 UEBA. It's also recommended that you modify the folder permissions for the folder that contains these files to prevent unwarranted access.

Need help?

If you have trouble configuring any of the above settings, please contact us at support@log360.com. You can also schedule a free personalized demo to receive expert guidance in bolstering your IT infrastructure's security.

Appendix

Steps to disable inheritance

1. Right-click the folder and select **Properties.**
2. Go to the **Security** tab and click **Advanced.**
3. Click **Disable** inheritance.
4. Click **Convert inheritance** permission to explicit permissions on this object.

Steps to remove Authenticated Users from ACL

1. Right-click the folder and select **Properties.**
2. Go to the **Security** tab and click **Edit.**
3. Select the **Authenticated Users** group and click **Remove.**
4. Click **Apply** and then **OK.**

To assign modify permissions to users

1. Right-click the folder and select **Properties.**
2. Go to the **Security** tab and click **Edit.**
3. Click **Add.**
4. Enter the name of the user or group, then click **OK.**
5. Under the *Permission for Users* section, check the box under the *Allow* column for the **Modify** permission.
6. Click **Apply** and then **OK.**

About Log360 UEBA

Log360 UEBA is powered by machine learning, and can detect anomalies by recognizing subtle shifts in user and entity activity. It helps you identify and investigate security threats that might otherwise go unnoticed, by extracting more information from your logs. Log360 UEBA analyzes logs from different sources including firewalls, routers, workstations, databases, and file servers. Any deviation from normal behavior is classified as a time, count, or pattern anomaly.

$ Get Quote

Download