How to manage logs for Comodo clients

- Comodo Client Security (CCS) keeps detailed records of all antivirus, HIPS, containment, VirusScope and firewall events.
- These logs are invaluable for monitoring and troubleshooting on managed endpoints.
- The 'Logging' interface lets you specify the location to store logs, the maximum size of log files, and how CCS should react if the maximum file size is exceeded.

Process in brief

- Login to ITairian.
- Click ‘Applications’ > 'Endpoint Manager’
- Click ‘Configuration Templates’ > ‘Profiles'
- Click the profile you want to modify
- Click the 'Logging Settings' tab
    - Or click 'Add Profile Section' > 'Logging Settings' if you haven't yet added this section
- Click the 'Comodo Client Security' tab > 'Edit'
- Click 'Save' to apply settings.

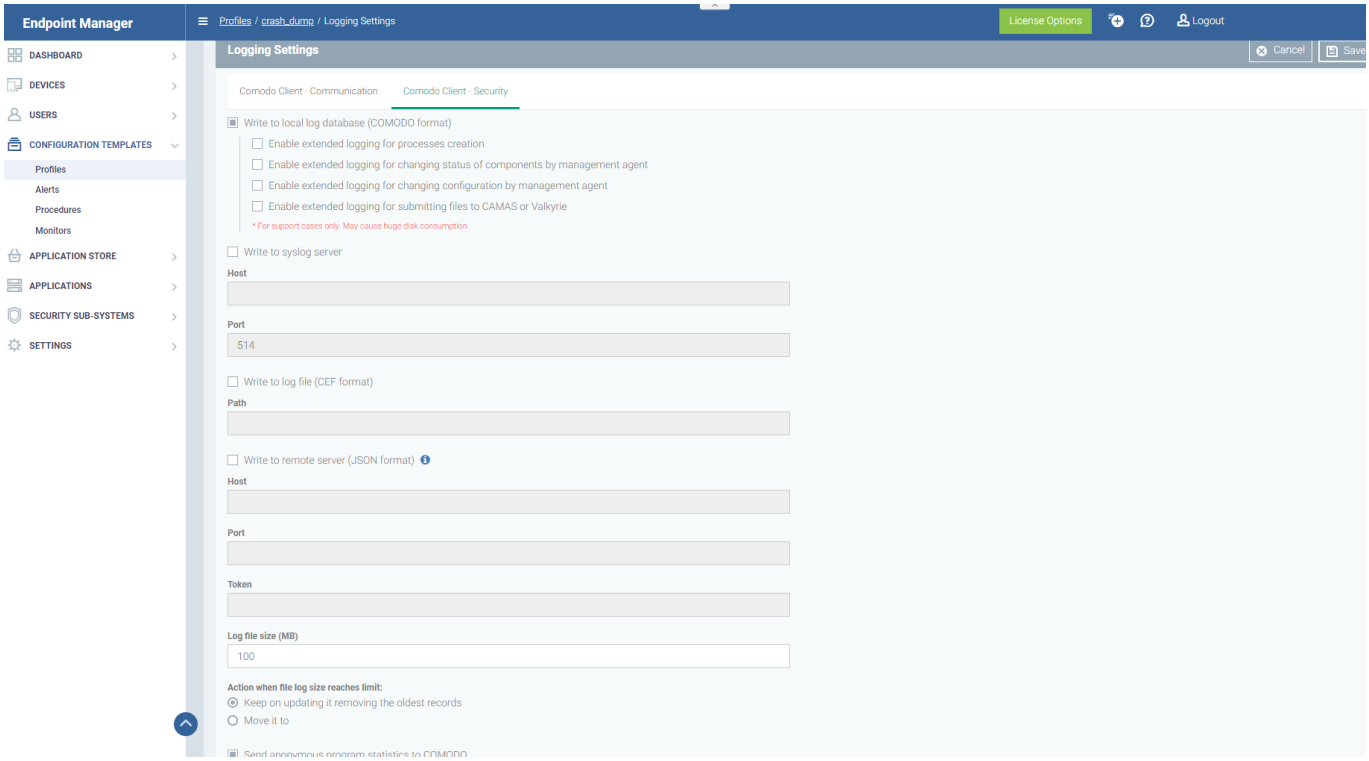
Process in more detail

- Open 'Endpoint Manager'
- Click ‘Configuration Templates’ > ‘Profiles'
- Click the 'Profiles' tab to show all available profiles
- Open the profile you wish to work on by clicking its name. This will open the profile's details page.
    - Select the '**Logging Settings**' tab if it has already been added to the profile

OR

    - Click 'Add Profile Section' > 'Logging Settings' to add the section

'Comodo Client Security' settings:



Write to Local Log Database

The log is saved in native Comodo format on the local endpoint.
You can enable extended logging for the following additional items:

- Process creation events
- CCS components are enabled/disabled by Communication Client .
- Changes to CCS configuration made by Communication Client
- Submitting files to CAMAS or Valkyrie

Extended logging means that more information is collected about each event. This is most useful if you are working with support to identify and resolve issues. Be aware that extended logging increases the size of log files so takes more disk space.

Write to Syslog Server

Log events are written to a remote syslog server. If enabled, specify the hostname/IP address and port number settings for the server.

- **Host** - The hostname or IP address of the syslog server.
- **Port** - The port number of the syslog server.

Write to Log File (CEF Format)

Logs are saved locally on the endpoint in Common Event Format (CEF) file format.

- **Path** – Enter the location where you want to store the CEF file.

Write to remote server (JSON format) - Logs are saved in JavaScript Object Notation (JSON) format on a remote server. If enabled, specify the hostname/IP address of the server, its connection port and the security token.

- **Host** - Hostname or IP address of the remote server.
- **Port** - Port number of the remote server for Endpoint Manager to connect to.
- **Token** - Security token to access the remote server.
- **Log file size (MB)** - the Maximum limit for the size of the log file *(Default = 100 MB).*

Action when file log size reaches the limit

Behaviour when the log file reaches a certain size:

- **Keep on updating it. Remove the oldest records**
  - CCS will continue to write all logs to the same file. When the size limit is reached, it will add new events to the top of the file and delete the oldest events to make room.
- **Move it to**
  - CCS will move the log file to a location of your choice when it reaches the maximum size. It will start a fresh log file to store new event records.
- **The path to the folder for old log files**
  - Specify the location to which the old/max. size log files should be moved. This is relevant if you enabled 'Move it to'.

'Communication Client ' settings:

- **Crash dump collection -** Endpoint Manager creates a dump file if Communication Client crashes on the endpoint. This is useful for analysis and troubleshooting.
- **Log type –** Determines the level of detail included in the log. 'Full' logs are larger so take more space.
  - **Mini -** The file only contains enough data to identify the conditions of the crash.
  - **Full** - A detailed log of all information related to the crash. Full logs let you analyze the crash in greater detail, but may take longer to generate than mini reports.