How to configure log storage settings in a Windows profile

Click 'Configuration Templates' > 'Profiles' > open a Windows profile > Click 'Add Profile Section' > 'Logging Settings'

- Xcitium Client Security (CCS) event logs are generated by its various security components. These include antivirus, firewall, containment, HIPS and more.
- The communication client (CC) can creates event logs for various management events like alerts generated, monitoring events, application/ patch installations, remote control events. It also creates a dump file when it crashes. The dump file is automatically forwarded to Xcitium for our technicians to investigate.
- You can configure where and how to save these logs in the 'Logging Settings' section of a profile.
- The logs can be :
    - Locally stored on the endpoint
    - Forwarded to a remote Syslog server, for example, to a SIEM tool
    - Stored on a remote server in JSON format
- This section explains how to configure storage locations for CCS and CC logs.

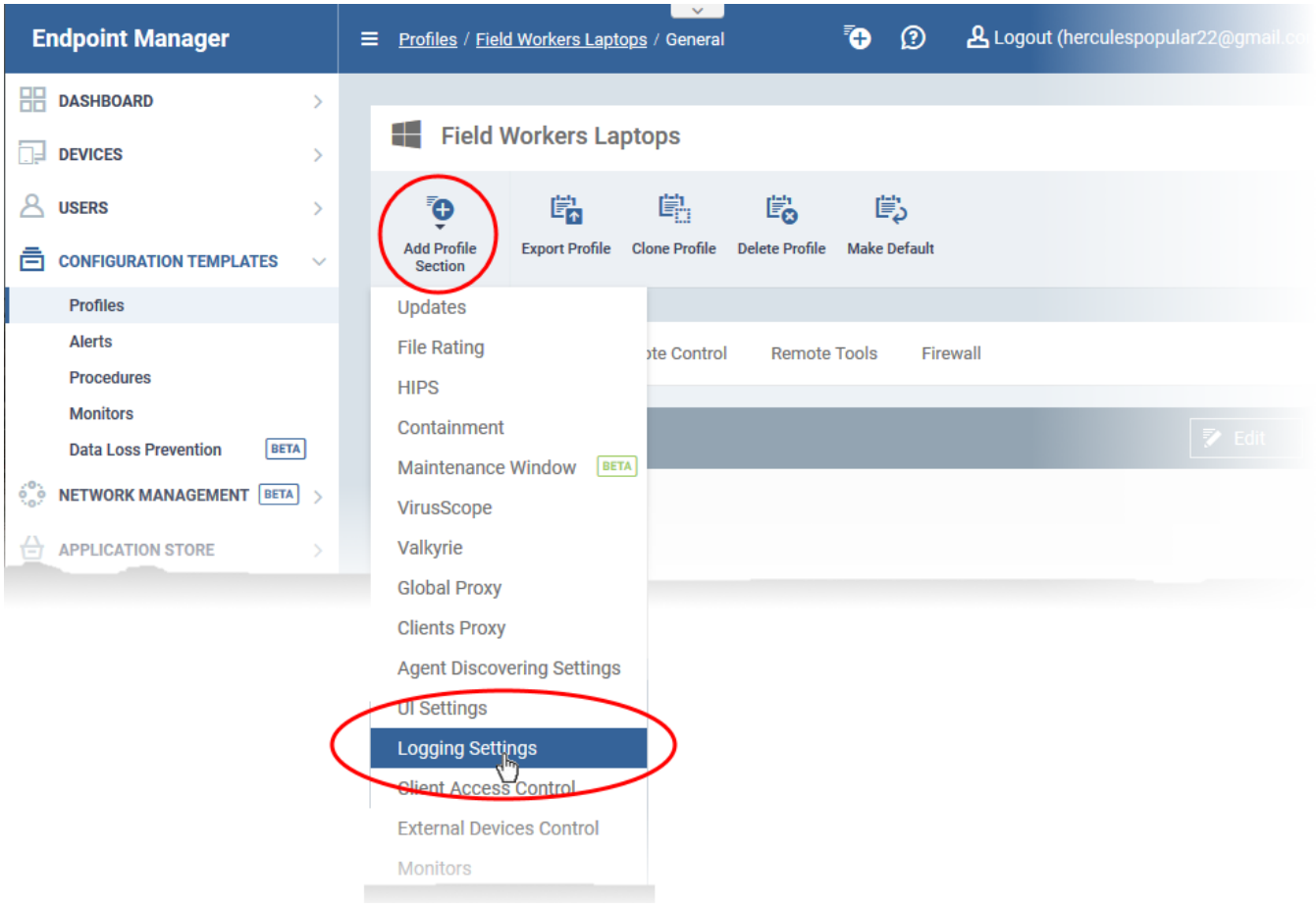
Add logging settings section to a profile

- Communication client (CC) log settings
- xcitium client – security (CCS) log settings

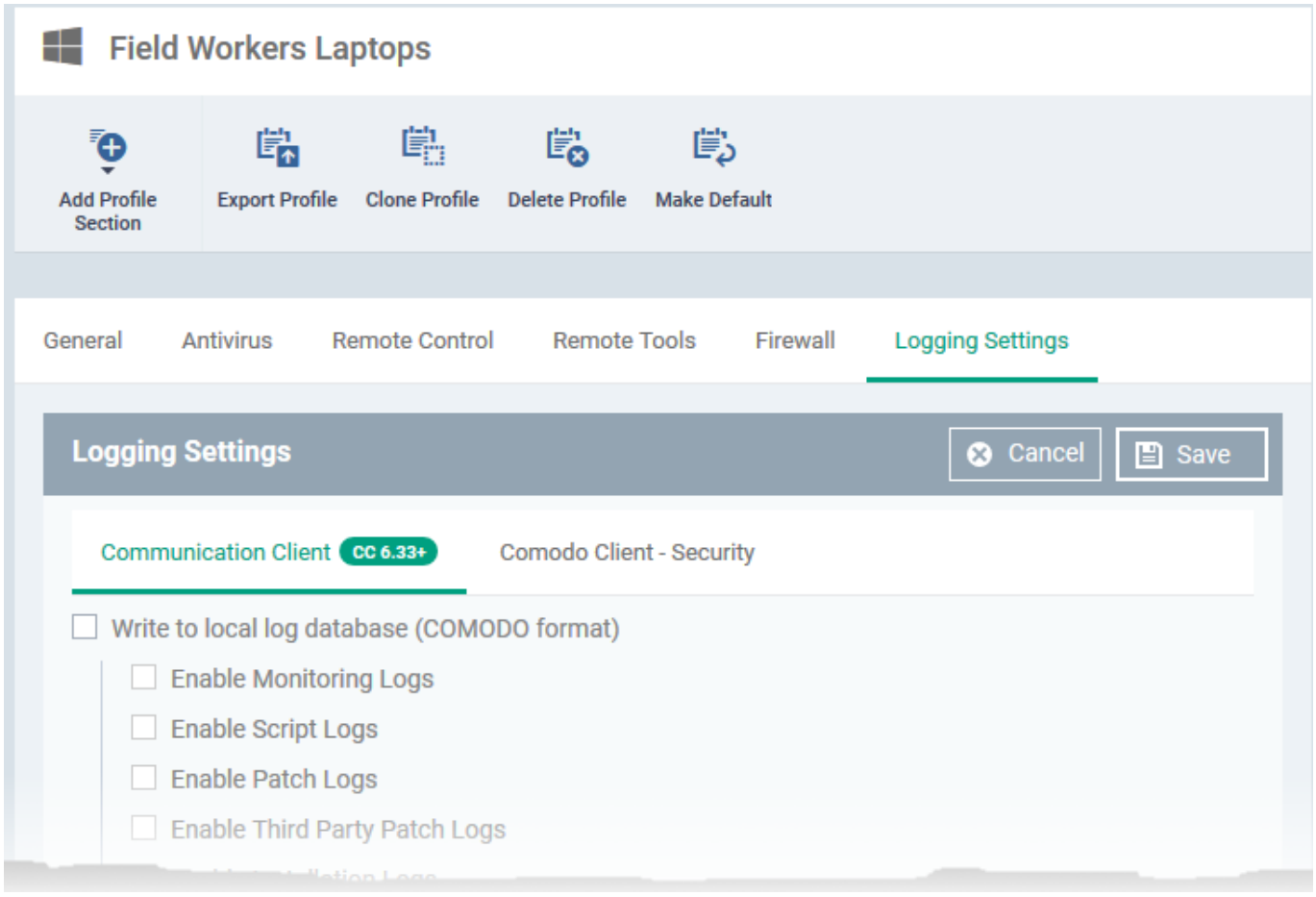
Add 'Logging Settings' section to a profile

- Login to Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click ‘Configuration Templates’ > ‘Profiles’
- Open the Windows profile applied to your target devices
    - Open the 'Logging Settings' tab if it has already been added > 'Edit'

      OR
    - Click 'Add Profile Section' > 'Logging Settings' if it hasn't been added



The logging settings pane opens:



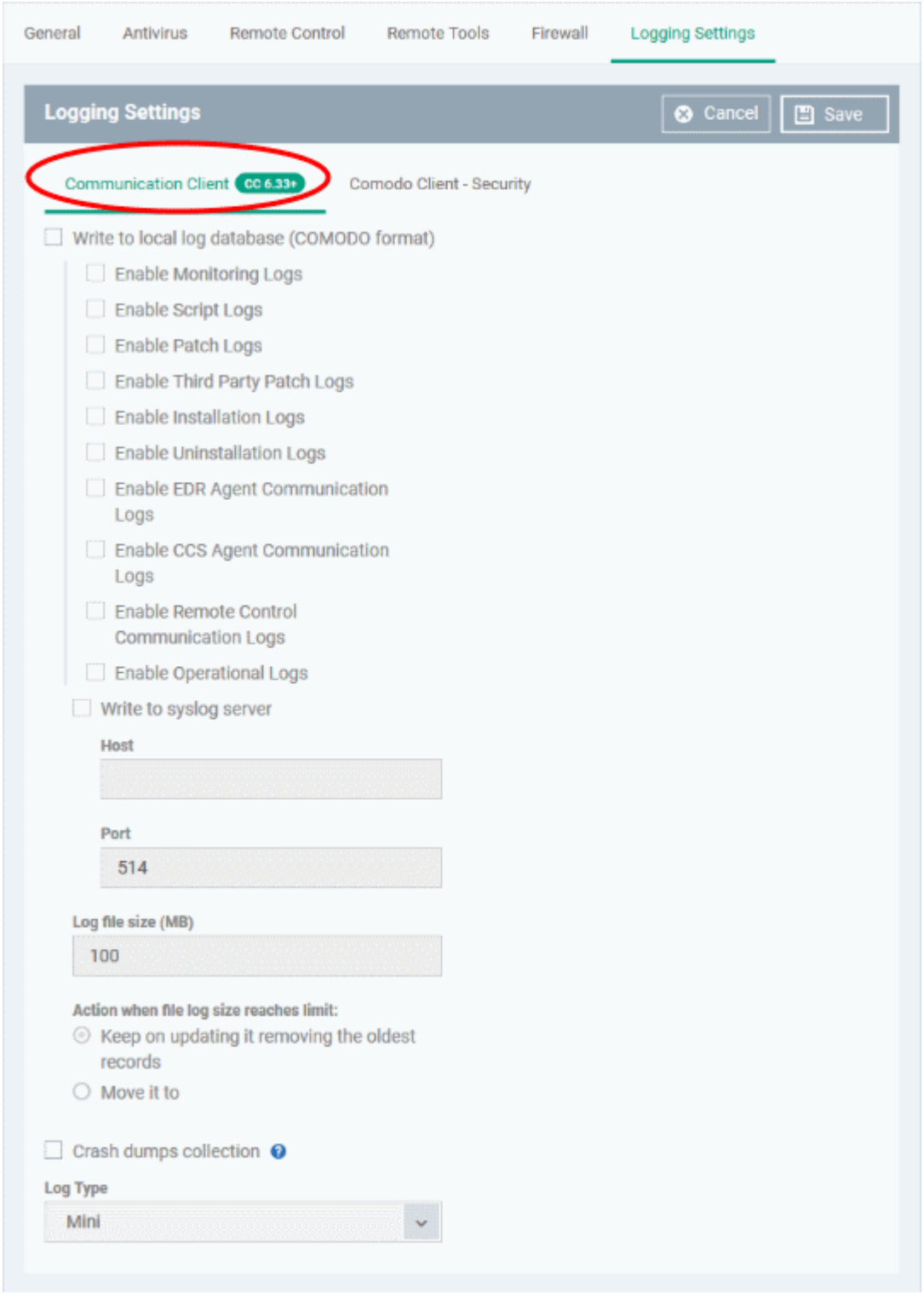
See the following sections for help to configure options under each tab.

- Communication Client
- xcitium Client – Security

Click 'Save' for your settings to take effect on the devices to which the profile is applied

Communication Client log settings

- Click the 'Communication Client' tab, if it is not already open:



Write to Local Log Database (XCITIUM Format) - The log is saved in native Xcitium format on the local endpoint.

- The logs can be viewed in CCS at 'Advanced Tasks' > 'View Logs'
- You can select the events for which logs are collected and stored:
    - Monitoring logs
    - Script logs
    - OS patch logs
    - Third party application update logs
    - Application installation logs
    - Uninstall logs
    - Event Detection and Response (EDR) agent communication logs
    - Xcitium Client - Security (CCS) communication logs
    - Remote Control Communication Logs
    - Operational Logs

Write to Syslog Server - CC logs are written to a remote syslog server or a SIEM (Security Information and Event Management) tool. If enabled, specify the hostname/IP address and port of the server.

- **Host *** - The host name or IP address of the syslog server.
- **Port *** - The port number on the syslog server to which CC should forward the logs.

Log File Size - Specify the maximum size of the log file (Default = 100 MB).

Action when file log size reaches limit - Specify behavior when the log file reaches a certain size.

- **Keep on updating it removing the oldest records** - When the max. log size is reached, CC will remove the oldest entries to make way for new entries.
- **Move it to** - CC will save the log file to a specific folder when it reaches the maximum size. CC will then start a new log file.
    - **The path to the folder for old log files** - If 'Move it to' is enabled, type a storage path for the log files that reached maximum size.

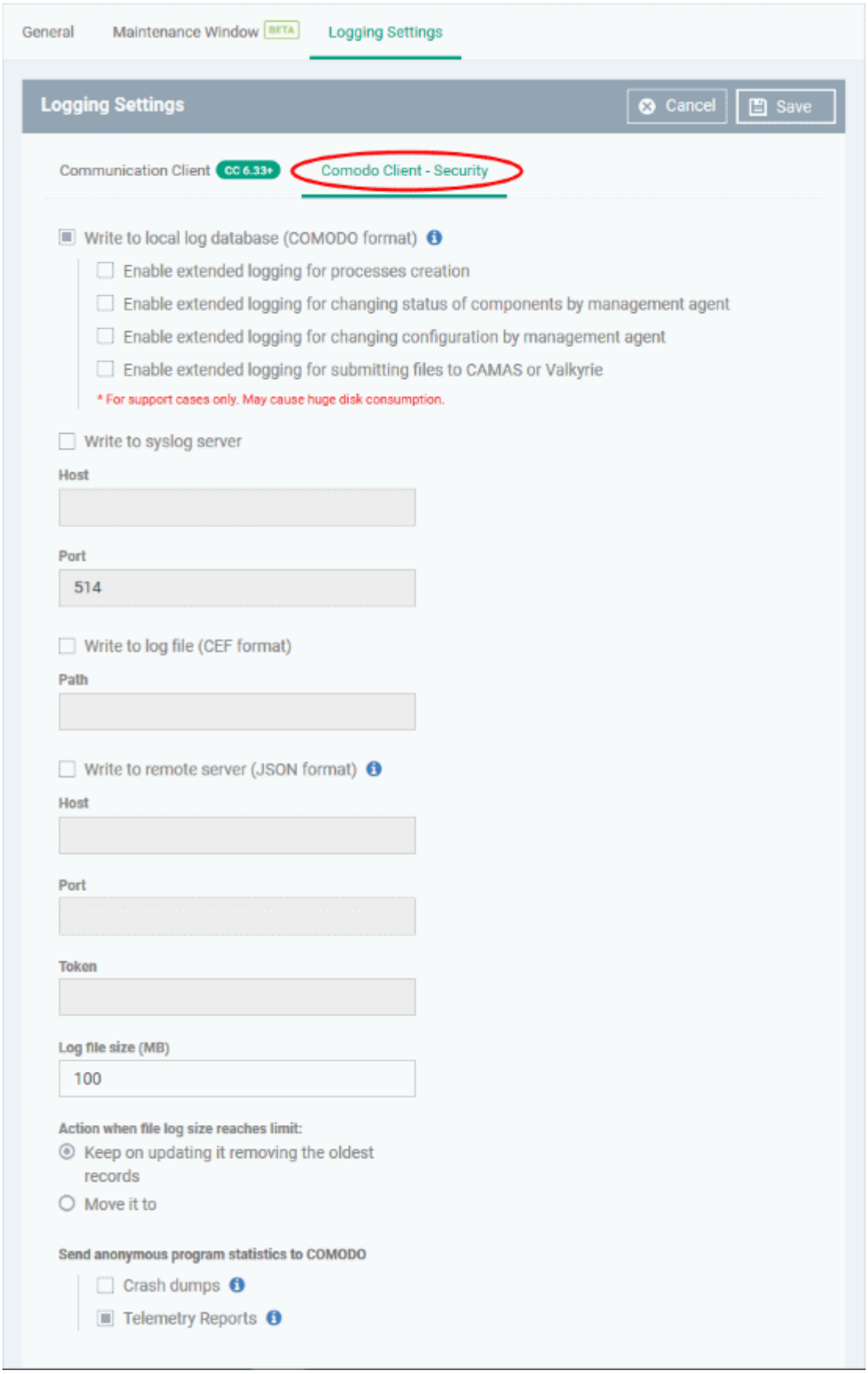
Crash dump collection - Endpoint Manager creates a dump file if the communication client crashes on an endpoint. The file contains details about the crash which can help our technicians diagnose and fix the issue. This file is automatically forwarded to Xcitium servers. If enabled, you can choose the log type:

- **Log Type** - Choose the type of dump file you want. The options are:

- **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 us analyze the crash in greater detail, but may take longer to generate than mini reports.
- No confidential or user data is included in either ‘Full’ or ‘Mini’ logs.

????Xcitium Client - Security log settings

- Click the 'Xcitium Client - Security' tab



Write to Local Log Database (XCITIUM **Format)** - The log is saved in native Xcitium format on the local endpoint.

- The logs can be viewed in CCS at 'Advanced Tasks' > 'View Logs'
- You can also enable extended logging when the following events occur:

    - A process is created on the endpoint
    - A CCS component is enabled or disabled by the communication client
    - A configuration change is made to CCS by the communication client
    - CCS submits a file CAMAS or Valkyrie for analyis.????

Extended logs contain more information than regular logs, but also take up more storage space.

Write to Syslog Server - CCS forward logs to a remote syslog server or a SIEM (Security Information and Event Management) tool. If enabled, specify the hostname/IP address and port of the server.

- **Host *** - The host name or IP address of the syslog server.
- **Port *** - The port number on the syslog server to which CCS should forward the logs.

Write to Log File (CEF Format) - Logs are saved locally on the endpoint in Common Event Format (CEF) file format. If enabled, please specify the location of the CEF file in the 'Path' field.

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

Log file size (MB) - Specify the maximum size of the log file (Default = 100 MB).

Action when file log size reaches limit - Specify what CCS should do when the log file hits the size limit:

- **Keep on updating it, removing the oldest records** - CCS will keep updating the same log file. To stay within the size limit, CCS will delete the oldest records to make room for new records.
- **Move it to** - CCS will save the log file to a specific folder when it reaches the maximum size. CCS will then start a new log file.
    - The path to the folder for old log files - If 'Move it to' is enabled, type a storage path for the log files that reached maximum size.
- **Send anonymous program statistics to Xcitium** - If enabled, select the types of statistics you want to submit to Xcitium:
    - **Crash dumps** - A file which contains diagnostics about application crashes and BSODs (blue screens of death) on the endpoint. This is useful for Xcitium to troubleshoot the issue.
    - **Telemetry Reports** - A daily log about the files you scan with CCS. We use this data to improve Endpoint Manager and CCS. The report contains the following data:
        - The hash value and path of the file
        - The hash value and path of the parent file that executed the file
        - Size, certificate information, and attributes of the file

- Click the 'Save' button to apply your changes.

Further reading:

How to forward Endpoint Manager audit logs to external server e.g. SIEM tool