Configure file analysis

Published: 2025-01-10

File analysis enables you to specify files to be hashed with the SHA-256 hashing algorithm. File hashes that match a threat collection generate a detection, and file hash data can be queried in records.

ExtraHop recommends that you manage these settings from an ExtraHop console, which is the default configuration in RevealX 360. For RevealX Enterprise, sensors manage these settings by default. If you prefer to manage the settings on a console instead of a sensor, you can transfer management to a console.

Prerequisites

- You must have System and Access Administration or System Administration (RevealX 360 only) user privileges.

Configure a size limit for file filters

You can specify a size limit that applies globally to all file filters. Any file that exceeds this limit will not be hashed.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **File Analysis**.
3. In the Size Limit (MB) field, specify a file size, in MB.
   The range is from 1 to 1,000,000 MB. The default value is 10 MB.
4. Click **Save**.

Create a file filter

You can create custom file filters that determine which files are hashed on the ExtraHop system. The ExtraHop Default filter is automatically enabled and is configured to hash executable media type files and files observed on any protocols, localities, and file extensions supported by file analysis. You can disable the default filter but you cannot modify the filter configuration.

Note: Enabling a large number of custom file filters might affect system performance.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **File Analysis**.
3. In the File Filters section, click **Add Filter**.
4. In the Name field, enter a unique name for the filter.
5. From the **Protocol** drop-down menu, select one of the following protocol options:
   - Any protocol (default)
   - HTTP
   - SMP
   - FTP

   Selecting **Any protocol** only hashes files observed on HTTP, SMB, or FTP protocols.
6. From the **Locality** drop-down menu, select one of the following flow direction options:
   - Any locality (default)
   - Inbound
   - Internal
   - Outbound

7. In the File Format section, select the type of files to filter:
   - To filter by media type, click **Media Type**, and then select one of the following media options:
     - Archive
     - Document
     - Executable
   - To filter by file extension, click **File Extension**, and then type one or more file extensions, separated with a comma. You can enter extensions in either of the following formats: `txt` or `.txt`.
8. In the Options section, select the **Enable file filter** checkbox to enable the filter and begin hashing files that match the criteria.
9. Optional: If the file filter is enabled, you can select the **Display hashed files in Files table** checkbox to display hashed files and associated metadata in the Files table available from the Assets page.
10. Click **Save**.

Transfer management of file analysis settings

For RevealX 360, ExtraHop consoles manage file analysis settings by default. For RevealX Enterprise, ExtraHop sensors manage these settings.

You can log in to a console and transfer management of file analysis settings to a sensor, or log in to a sensor and transfer management to a console.

Note: Transferring management for these settings also transfers management for all shared settings.

1. Log in to the console or sensor that is currently managing file analysis settings through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **File Analysis**.
3. Transfer management of file analysis to a different system.

Option	Description
Transfer from sensor to console	1. Click **Transfer Management**. 2. From the **Managing Console** drop-down menu, select a console name.
Transfer from console to sensor	1. Click ***N* of *N* connected sensors**. The Management Settings window displays a list of sensors that the console manages shared settings and a list of sensors that manage their own settings. 2. Click the name of the sensor that you want to manage its own settings. 3. Log in to the sensor. 4. Click **Transfer Management**. 5. From the **Managing Console** drop-down menu, select **Sensor Appliance - Self**.