

Configure file analysis

Published: 2024-10-03

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.


You must have [System and Access Administration privileges](#) to configure file analysis.

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.

- Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
- Click the System Settings icon  and then click **File Analysis**.
- 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.
- Click **Save**.

Create a file filter

You can create custom file filters that determine which files are hashed on the system. The ExtraHop Default filter is enabled by default. The default filter cannot be modified and applies to executable media type files, any protocol, any locality, and any file extension.

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

- Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
- Click the System Settings icon  and then click **File Analysis**.
- In the File Filters section, click **Add Filter**.
- In the Create File Filter window, in the Name field, enter a unique name.
- From the **Protocol** drop-down list, select from these options:
 - Any protocol (default)
 - HTTP
 - CIFS
 - FTP
- From the **Locality** drop-down list, select from these flow direction options:
 - Any locality (default)
 - Inbound
 - Internal
 - Outbound

7. For File Format, select the type of files to filter:
 - To filter by media type, click **Media Type**, and then select from these media options:
 - Archive
 - Document
 - Executable
 - To filter by file extension, click **File Extension**, and then enter file extensions, separating multiple entries with a comma. You can enter extensions in either of these formats: `txt` or `.txt`.
8. For Options, verify that the **Enable file filter** checkbox is selected.
9. 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	<ol style="list-style-type: none"> 1. Click Transfer Management. 2. From the Managing Console drop-down list, select a console name.
Transfer from console to sensor	<ol style="list-style-type: none"> 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 list, select Sensor Appliance - Self.