

Upload custom IDS rules

Published: 2024-04-02


You can upload a custom set of IDS rules to ExtraHop IDS sensors. The ExtraHop system converts the rules to detection types that generate detections that you can view and investigate.


Add rules that are formatted according to Suricata guidelines to one or more .rules files and upload them in a .zip file. Upon upload, the ExtraHop system processes each rule, which is displayed in a table that displays the signature ID, the name of each rule, and one of the following rule statuses.

- **Accepted:** The ExtraHop system successfully processed the rule.
- **Rejected:** The ExtraHop system could not process the rule. The rule might contain a formatting error or the rule might contain an action, protocol, or option that is not currently supported by the ExtraHop system. Contact [ExtraHop Support](#) to inquire about future support for the rule.
- **Upgrade required:** A **newer version of the ExtraHop firmware is required** to support the rule. The required system version is displayed.

Here are some considerations about custom IDS rules:

- Custom IDS rules must be formatted as a valid [Suricata .rules file](#).
- One or more Suricata .rules files must be added to a single .zip file for upload.
- You cannot upload more than 10,000 custom IDS rules.
- Deleting a file deletes all rules associated with the uploaded file and can take several minutes. Users might continue to see detections based on these rules until deletion is complete.
- Replacing a file deletes all rules associated with the previously uploaded file and then processes the rules from the new file.
- Built-in IDS rules are not deleted or replaced when you manage your custom IDS rules. Your ExtraHop system is connected to ExtraHop Cloud Services and the latest built-in rules are automatically downloaded to the system when updated versions become available.

 **Note:** ExtraHop might review uploaded rules to check conversion accuracy and to guide product improvement for Suricata rule conversion, correctness, and performance.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon  and then click **Custom IDS Rules**.
3. Click **Upload File**.
4. Click **Choose file**, select the .zip file you want, and then click **Upload File**.
The upload process can take several minutes. The file status and timestamps are updated after processing is complete.

Next steps

Click **Detections** from the top navigation menu page to view detections generated from custom IDS rules. These detections indicate that the rule was provided by a custom IDS file and includes the signature ID of the rule.