Upload IDS rules to the ExtraHop system through the REST API

Published: 2024-03-26

You can download a set of curated IDS rules from the ExtraHop Customer Portal and manually upload the rules to IDS sensors. If your ExtraHop system is connected to ExtraHop Cloud Services, the latest ruleset is automatically downloaded to the system whenever an updated version becomes available. In this guide, we show methods for uploading IDS rules through both the cURL command and a Python script.

> **Important:** The ExtraHop Customer Portal provides downloads for both IDS Ruleset files and IDS Resource files. If you upload an IDS Ruleset file to a sensor, you must also upload the corresponding IDS Resource file to the console that the sensor is connected to.

Upload IDS rules with the cURL command

1. Download the latest IDS rules from the Extrahop website.
2. Go to the ExtraHop Customer Portal ⤤, and click **IDS Rules**.
3. Open a terminal and run the following command, replacing the variables with information from your environment:

   • **HOST:** The IP address or hostname of the IDS sensor or console.

   • **API_KEY:** The API key.

   • **IDS_FILE:** The filepath of the IDS file. If the host is a sensor, specify the path of the IDS Ruleset file. If the host is a console, specify the path of the IDS Resources file.

   ```
   curl -X POST "https://<HOST>/api/v1/extrahop/cloudresources" -H "accept:
    application/json" -H "Authorization: ExtraHop apikey=<API_KEY>" --data-
   binary @IDS_FILE -w "%{http_code}\n"
   ```

   The command returns the HTTP status code of the response. If the command is successful, the status code is 202.

   > **Note:** If the command returns no results, make sure that a trusted certificate has been added to your ExtraHop system ⤤. Alternatively, you can add the `--insecure` option to retrieve the device list from an ExtraHop system without a trusted certificate; however, this method is not secure and not recommended.

4. Repeat the previous step for each IDS sensor and console that you want to update.

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that reads a list of ExtraHop sensors and consoles from a CSV file and uploads IDS rules to each one programmatically.

1. Go to the ExtraHop code-examples GitHub repository ⤤ and download the contents of the `upload_ids_rules` directory to your local machine.
2. Download the latest IDS rules from the Extrahop website.
   a) Go to the ExtraHop Customer Portal ⤤, and click **IDS Rules**.
   b) Click **Download** next to both IDS Ruleset and IDS Resources.
   c) Copy the files to the `upload_ids_rules` directory on your local machine.
3. In a text editor, open the `ids.csv` file and replace the example values with the hostnames, API keys, and IDS file path for each sensor or console. Specify the path of IDS Ruleset files for sensors and IDS Resource files for consoles.

> **Important:** Do not delete or modify the header row.

4. Run the following command:

```
python3 upload_ids_rules.py
```

> **Note:** If the script returns an error message that the SSL certificate verification failed, make sure that a trusted certificate has been added to your sensor or console ☑. Alternatively, you can add the `verify=False` option to bypass certificate verification. However, this method is not secure and not recommended. The following code sends an HTTP GET request without certificate verification:
>
> ```
> requests.get(url, headers=headers, verify=False)
> ```