# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td><strong>PART I: MODULE OVERVIEW</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>PREREQUISITES</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>PART II: CONFIGURING ENDPOINT API DOCUMENTATION MODULE</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Enabling the Endpoint API Documentation Module</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Disabling the Endpoint API Documentation Module</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Configuring API User Accounts and Token Authentication</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>PART III: USING THE ENDPOINT API DOCUMENTATION MODULE</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Accessing APIs</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>TECHNICAL SUPPORT</strong></td>
<td>12</td>
</tr>
</tbody>
</table>
PART I: Module Overview

The FireEye Endpoint Security application programming interface (API) allows users to automate certain actions and integrate security information and event management (SIEM) solutions from FireEye and other companies. The API provides access to information about endpoints, acquisitions, alerts, source alerts, conditions, indicators, and containment. The Endpoint Security API uses role-based access control (RBAC) and representational state transfer (REST) architecture.

The Endpoint Security API Documentation Module enables users to find and try the various API routes that exist within the Endpoint Security Server. Using the module, you can quickly search for specific API routes, see examples of the request and possible responses as well as try the request and see the response all from the UI.

Prerequisites

This release of Endpoint API Documentation is supported on **Endpoint Security 5.0.2**

Note: Endpoint API Documentation 1.0.0 will NOT work on Endpoint Security 5.0 or lower. This is not a supported scenario.
PART II: Configuring Endpoint API Documentation Module

You can enable and disable the API Documentation module directly in the Endpoint Security Web UI.

This section covers the following topics:

- Enabling the API Documentation Module
- Disabling the API Documentation Module
- API User Accounts and Token Authentication

Enabling the Endpoint API Documentation Module

You can perform these tasks from the Modules page in the Endpoint Security Web UI.

To enable the Endpoint API Documentation Module:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the Modules menu, select HX Module Administration to access the Modules page.
3. On the Modules page, locate the Endpoint API Documentation module and click the Actions icon (the gear symbol) and select Enable to enable the module.

Disabling the Endpoint API Documentation Module

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the Modules menu, select HX Module Administration to access the Modules page.
3. On the Modules page, locate the Endpoint API Documentation module and click the Actions icon (the gear icon) and select Disable to disable the module.

Configuring API User Accounts and Token Authentication

To submit API requests to the Endpoint Security server you must have either an API user account or an API token.

To use an API user account, an Endpoint Security Administrator must create either an api_admin or api_analyst account. For more information about setting up user accounts on the Endpoint Security server, please see the Endpoint Security System Administration Guide.
There are two options to create an API token:

1. Request a token for a user using CURL:
   
      i. User must be an Administrator
   b. Response will look like:

   HTTP/1.1 204 No Content
   Date: Fri, 02 Oct 2020 09:06:58 GMT
   Server: Apache/2
   X-Content-Type-Options: nosniff
   Cache-Control: no-cache, no-store, must-revalidate
   Pragma: no-cache
   Expires: 0
   Strict-Transport-Security: max-age=631138519; includeSubDomains
   X-FeApi-Token: IP68FGsyQVIBfHLyh+/nqwbDXiEHOIm1nkoRin0gRjiqAE8=
   X-Frame-Options: SameOrigin

2. Use the API Documentation Module to generate a token:

   a. Set the BASIC_AUTH Username and Password while viewing the lighthouse doc.

   b. Navigate to Authentication GET /token
   c. Click ‘Try’
   d. View the response headers for your token: “x-feapi-token: IP5u+fg5soHhkpHLZ7aVok3pst/iE1PUbiKiVBkjReamAE4=’
The following table lists the remote access privileges on the Endpoint Security server for each role:

<table>
<thead>
<tr>
<th>Privileges</th>
<th>api_admin</th>
<th>api_analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>View acquisitions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configure policy</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Manage and View alerts</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Approve and cancel containment</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View audits</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create data acquisitions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Run enterprise searches</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create file acquisitions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create, Update, Delete host sets</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create and view indicators</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
PART III: Using the Endpoint API Documentation Module

This section describes how to use the Endpoint API Documentation Module.

To access the Endpoint API Documentation interface:

1. Log in to the Endpoint Security Web UI as an administrator.
2. From the Modules menu, select API Documentation.

The APIs are grouped into the categories described below. Additional modules that are installed on your server may also provide API documentation and will add a category to the drop-down list if APIs are available.

**Lighthouse**

This API provides access to information about endpoints, policy, acquisitions, alerts, source alerts, conditions, indicators and containment.

**Plugin_Manager**

This API can be used to manage modules on the Endpoint Security server. An api_admin user can install, uninstall, upgrade, enable and disable a module.

**Platform_Service**

This API can be used to perform CRUD actions on module configurations.

**Messagebus**

This API provides read-access to Endpoint Security’s messagebus, which is used for event communication between Endpoint Security services and modules.

**Accessing APIs**

1. To begin finding and testing API routes, start by selecting which category you want to use:
2. Enter your API user account information or your API token key:

![Authentication](image)

3. Click to expand one of the available routes (Host Information in this example):

![Host Information](image)
4. Click the specific route you want to explore (GET /hosts in this example):

![API Request and Response Example]

**NOTE:** Each route will give a description for its intended use, the required and optional parameters for the body of the request and expected response examples.

5. Enter in the required (or optional parameters) and click the “TRY” button to see the response you would get for that API. You can also click through the response section to see the expected format of possible responses.
Options

Expand/Collapse View

The API Documentation Module provides two views to choose from, Expanded View and Collapsed View. The default view is the Collapsed view. The Expanded view offers a search bar and automatically expands every route in the selected category:

To toggle between the views, click the Expand/Collapse button:

Export:

You can export a JSON file for a category. This can be imported into a tool like Postman and use it to create SDKs. If you would like to export all the information in the selected category, click the Export button:
Technical Support

For technical support, contact FireEye through the Support portal:

https://csportal.fireeye.com

Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required):

https://docs.fireeye.com/