

# Symantec Threat Intelligence

Ulf Spangenberg, niwis consulting gmbh



# About Symantec Threat Intelligence

Symantec is offering a set of services to core customers with no additional costs to allow access to Broadcom Global Intelligence Network (GIN) and all telemetry collected.



One of the largest civilian security threat intelligence networks in the world.

# About Symantec APIs

Symantec Endpoint Security and other Symantec solutions offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.

 <b>Symantec™ Endpoint Security (SES)</b>  SES Complete offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.  <a href="#">VIEW MORE ▶</a>	 <b>Symantec™ Endpoint Protection (SEP)</b>  SEP offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.  <a href="#">VIEW MORE ▶</a>	 <b>Symantec™ Endpoint Detection and Response (EDR)</b>  EDR offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.  <a href="#">VIEW MORE ▶</a>
 <b>Symantec™ Cloud Workload Protection</b>  CWP offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.  <a href="#">VIEW MORE ▶</a>	 <b>Symantec™ Cloud Workload Protection Storage</b>  CWP offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.  <a href="#">VIEW MORE ▶</a>	 <b>Symantec™ Data Loss Prevention (DLP)</b>  DLP offers a set of REST APIs that are useful for integration with various third-party applications to perform operations.  <a href="#">VIEW MORE ▶</a>

# About Symantec Endpoint Security (SES)

SES delivers comprehensive protection for all your traditional and mobile devices across the entire attack chain. This single-agent solution supports on-premises, hybrid, and cloud-based deployments.



Best Protection

Industry-leading solution that addresses threats across the entire attack chain.

# How to use the Symantec Threat API with Postman



# About Postman

Postman is an API platform for building and using APIs. Postman simplifies each step of the API lifecycle and streamlines collaboration so you can create better APIs—faster.

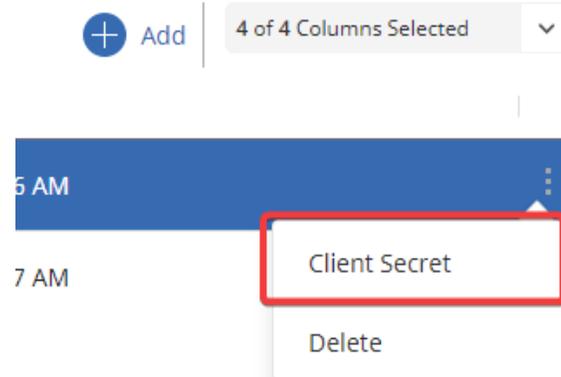


# Create an application in Symantec Endpoint Security (SES)

The screenshot displays the Symantec Endpoint Security (SES) Client Application Management interface. The left sidebar contains navigation options, with 'Client Applications' highlighted (1) and a plus icon (2). The main area shows 'Client Application Management' with a summary of 2 client applications added. A table lists the applications: 'Postman' and 'Threat Intel Browser Plug in'. A modal window titled 'Add client application' is open, showing a text input field for 'CLIENT APPLICATION NAME\*' with 'Postman' entered (4) and an 'Add' button (5). A '+ Add' button in the top right of the table is also highlighted (3).

APPLICATION NAME ↑	CLIENT ID	CREATED BY	CREATED
Postman	021D M5101 55F0C4621M7Zvax1MA D5EQ2ubh0t4... Ulf Czupponberger		Jan 2, 2023, 11:22:16 AM
Threat Intel Browser Plug in			Jan 2, 2023, 11:17:17 AM

# Go to Client Secret



# Copy OAUTH

Client application secret ✕

 CLIENT ID 

CLIENT SECRET 

OAUTH CREDENTIALS

Basic 



# Install Postman and import collection

**Download and install Postman:**

<https://www.postman.com/downloads/>

**Download and import JSON:**

<https://www.niwis.com/download/threat-intelligence-json/>

# Fill ...

... variable “AUTH” under Main Section “SES Copy” with the clipboard value of your OAUTH credentials.

The screenshot shows the Postman interface with the 'Variables' tab selected for the 'SES Copy' collection. The table below lists the variables:

	VARIABLE	INITIAL VALUE ⓘ
<input checked="" type="checkbox"/>	TOKEN	
<input checked="" type="checkbox"/>	AUTH	TzJJRC...
	Add a new variable	

Make sure to not paste in any text in front of the value!

# Make sure ...

... you fill in the “Initial value” and the “Current value”.

Do not forget to  
save!

SES

Overview Authorization • Pre-request Script • Tests Variables • Runs

These variables are specific to this collection and its requests. [Learn more about collection variables](#)

Filter variables

	Variable	Initial value	Current value	...
<input checked="" type="checkbox"/>	TOKEN			
<input checked="" type="checkbox"/>	AUTH	TzJJRC5ITEx4THFZUVRr...	TzJJRC5ITEx4THFZUVRrYTIBSWhpbDBFTXV3LmFiaGJhM...	
	Add new variable			

# Turn on ...

... “Follow Authorization header”.

The screenshot shows a REST client interface with a sidebar on the left containing a list of endpoints under the 'SES' category. The main area displays the configuration for a POST request to `https://api.sep.securitycloud.symantec.com/v1/oauth2/tokens`. The 'Settings' tab is active, showing several options:

- HTTP version:** `HTTP/1.x` (Default: Settings)
- Enable SSL certificate verification:** OFF (Default: Settings)
- Automatically follow redirects:** ON (Restore Default)
- Follow original HTTP Method:** OFF (Restore Default)
- Follow Authorization header:** ON (Restore Default) - This option is highlighted with a red arrow.
- Remove referer header on redirect:** OFF

# Go to ...

... .. any listed GET command and execute and you should get a valid output.

The screenshot displays a REST client interface with a sidebar on the left containing a list of API endpoints. The endpoint 'GET Process Chain' is selected and highlighted with a red circle containing the number '1'. The main area shows the details of a GET request to the URL 'https://api.sep.securitycloud.symantec.com/v1/threat-intel/processchain/file/file'. A red callout bubble with the text 'executed API call' points to the 'Send' button, which is also marked with a red circle containing the number '2'. Below the request details, the response body is shown in a 'Pretty' JSON format. A red callout bubble with the text 'hash to look up, exchange for another' points to a specific hash value in the JSON: '8694c5732d26921ee29509a9fa4182139ef...'. Another red callout bubble with the text 'valid output' points to the overall JSON structure. The status bar at the bottom right indicates 'Status: 200 OK', 'Time: 450 ms', and 'Size: 1 KB'.

KEY	VALUE	DESCRIPTION
Key	Value	Description

KEY	VALUE	DESCRIPTION
file	5a3f0b0929bfc626012f45ce80d4316497c676e1e639bc3b241d5e9b5f113899	Description

```
1
2 {"file": "5a3f0b0929bfc626012f45ce80d4316497c676e1e639bc3b241d5e9b5f113899",
3   "chain": [
4     {
5       "parent": {
6         "parent": {
7           "parent": {
8             "parent": {
9               "parent": {
10                "parent": {
11                  "file": "8694c5732d26921ee29509a9fa4182139ef...a5defe6",
12                  "processName": "wininit.exe"
13                },
14                "file": "930f44f9a599937bdb23cfc7ea4d158991b837d2a8975c15696cdd4198880e8",
15                "processName": "services.exe"
16              },
17              "file": "438b6cccd84f4dd32d9604ed7d58fd7d1e5a75fe3f3d12ab6c78e6bb8ffad5e7",
18              "processName": "svchost.exe"
19            },
20            "file": "a0a37fde4d9cd7385e819afa967bc525231c2f166c38591532d8feab94e40da",
21            "processName": "w3wp.exe"
22          },
23          "file": "935c1861df14018d698e8b65abfa02d7e903708f68ca3c2865b6ca165d44ad2",
24          "processName": "cmd.exe"
25        },
26        "file": "935c1861df14018d698e8b65abfa02d7e903708f68ca3c2865b6ca165d44ad2",
27        "processName": "cmd.exe"
28      },
29    ]
30  }
31 }
```

# Additional



# More Symantec Threat Intelligence

- SES RestAPI documentation:

<https://apidocs.securitycloud.symantec.com/#/>

- Threat Intel Browser Plug In:

<https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Settings/Configuring-Threat-Intel-browser-plug-in.html>

- Threat Explorer (Account needed):

<https://threatexplorer.symantec.com/>

# More Symantec Threat Intelligence

- **SES Threat Reports\*<sup>1</sup> via Email**

- [Link ...](#)

\*1

- **Symantec Threat Alerts Report:** Shows information about indicators of compromise (IOCs) relating to currently active, critical threats.
- **Symantec White Papers Report:** Shows information about current threats based on in-depth research by the Symantec Threat Hunter team.
- **Threat Landscape Bulletin Report:** Provides up-to-date news and intelligence from the world of cyber security.