Integrate Cisco SecureX with VirusTotal

Contents

Introduction

This document describes the steps to integrate Cisco SecureX with VirusTotal.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- API Keys
- SecureX console

Components Used

This document is not restricted to specific software and hardware versions.

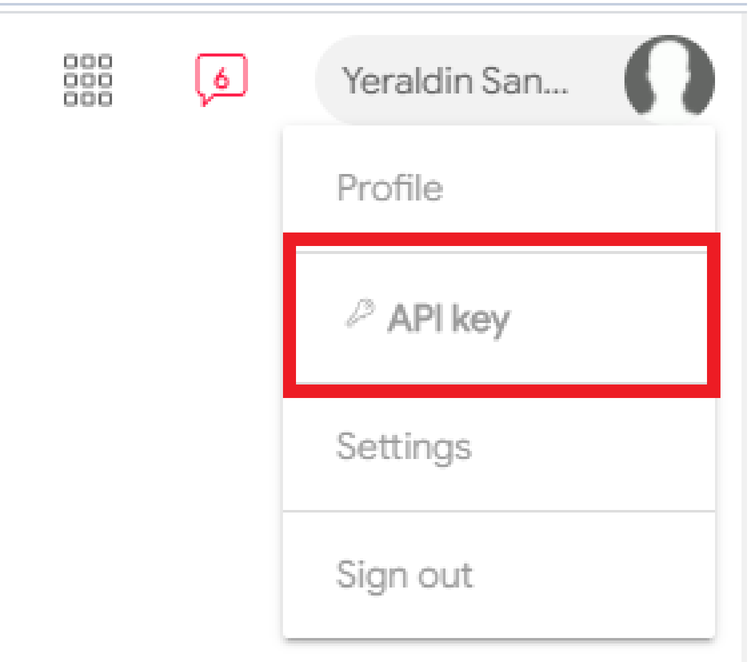
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

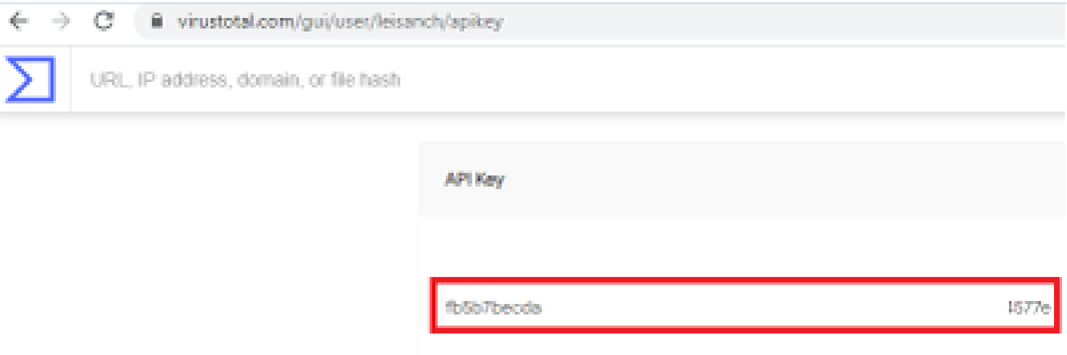
Configure

In order to configure a new VirusTotal enrichment module, you must first generate an API Key in VirusTotal and then add the VirusTotal module.

Step 1. InVirusTotal, click the VirusTotal user icon and choose**Settings**.

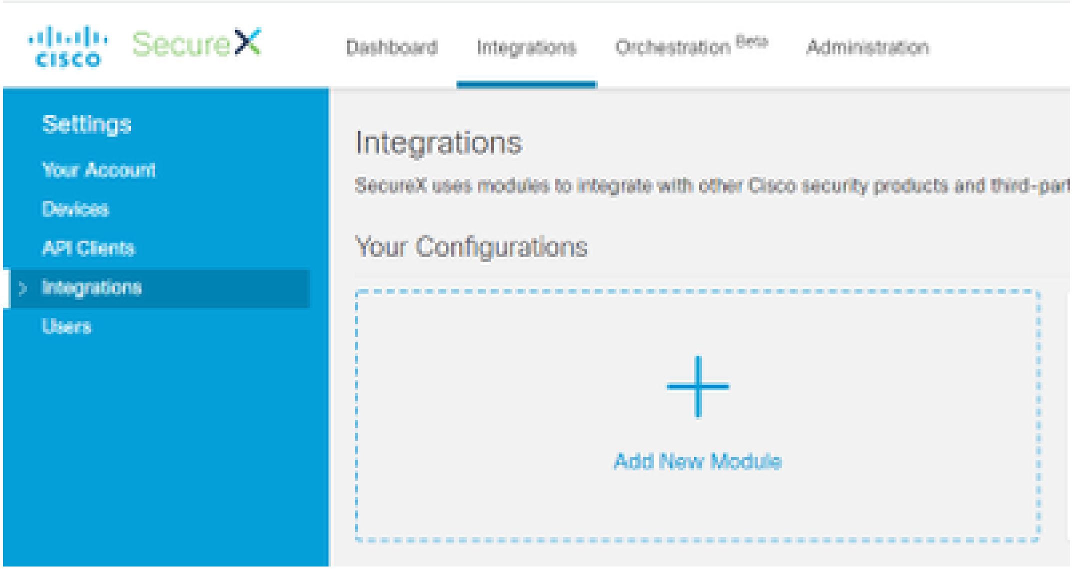
Step 2. Click**API Key**and save the key value, as shown in the image.




virustotal.com/gui/user/leisanch/apikey

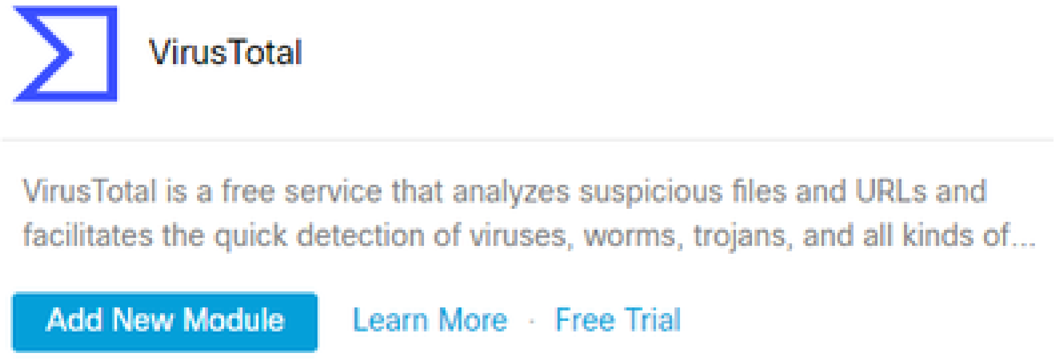
fb5b7becda l577e

Step 3. On the SecureX portal, navigate to Integrations, click on**Add New Module**, as shown in the image



SecureX uses modules to integrate with other Cisco security products and third-part

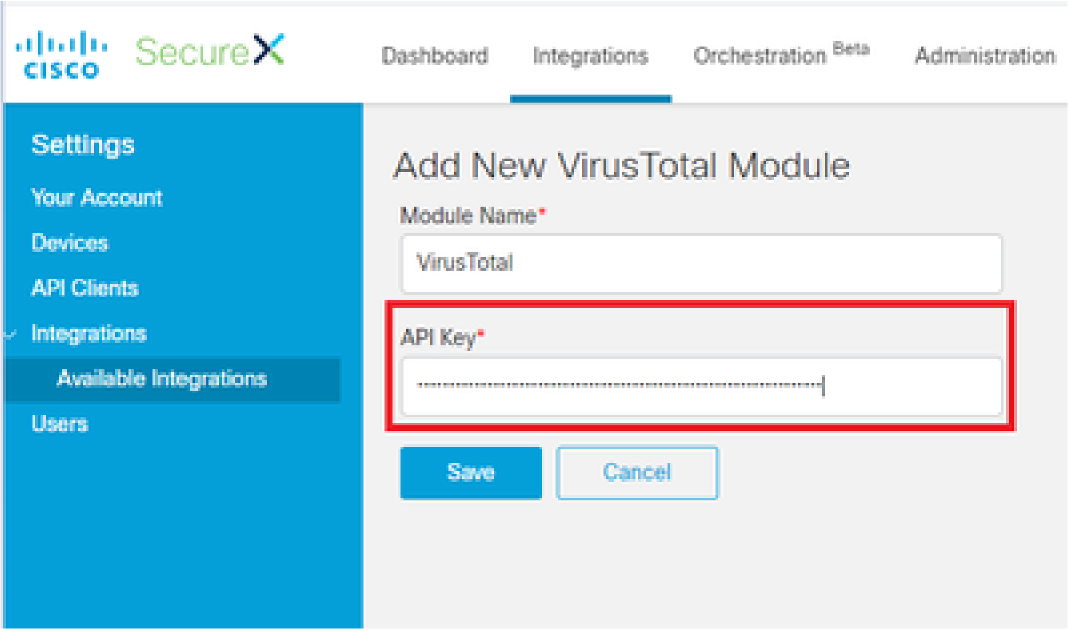
Step 4. On the VirusTotal section, click on Add New module as shown in the image.



VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of...

Step 5. Enter in this section your VirusTotal**API Key**and click**Save**, as shown in the image.



Add New VirusTotal Module

Module Name*: VirusTotal

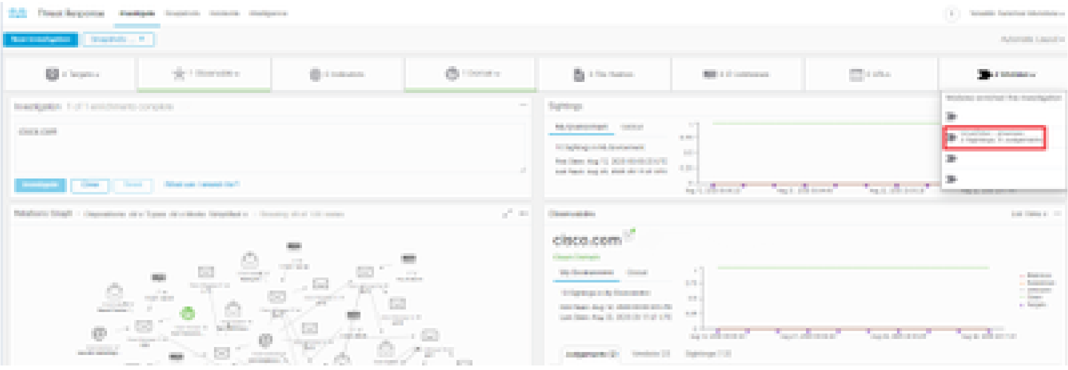
API Key*: ••

Note: The Public API is limited to a maximum of 4 requests per 1-minute time frame. The VirusTotal enrichment module makes one API request per observable. VirusTotal also offers a[Private API]which provides a higher request rate.

Verify

Use this section to confirm that your configuration works properly.

In order to verify that the module works as expected, navigate to the **Cisco Threat Response** portal and make an investigation, the results display the modules enriched, as shown in the image.



Troubleshoot

This section provides the information you can use to troubleshoot your configuration.

Step 1. Make sure the API credentials are properly copied in the module section from the SecureX portal.

Step 2. Verify that the API credentials have the right permissions and are currently available.

> **Note**: Refer to the VirusTotal API error documentation in the case of any unexpected error.

Video

You can find the configuration steps contained in this article in this video.