Secure X with Threat Grid Cloud Integration Guide

Contents

Introduction

This document describes the steps required to integrate and configure the Threat Grid Cloud module with Secure X.

Contributed by Jesus Javier Martinez, Edited by Jorge Navarrete, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Threat Response
- Threat Grid Cloud
- Secure X

Components Used

The information in this document is based on these software versions:

- CTR console (User account with Administrator rights)
- Threat Grid console (User account with Administrator rights)
- Secure X console (User account with Administrator rights)

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.

Background Information

Cisco Threat Grid is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impact the user environment.

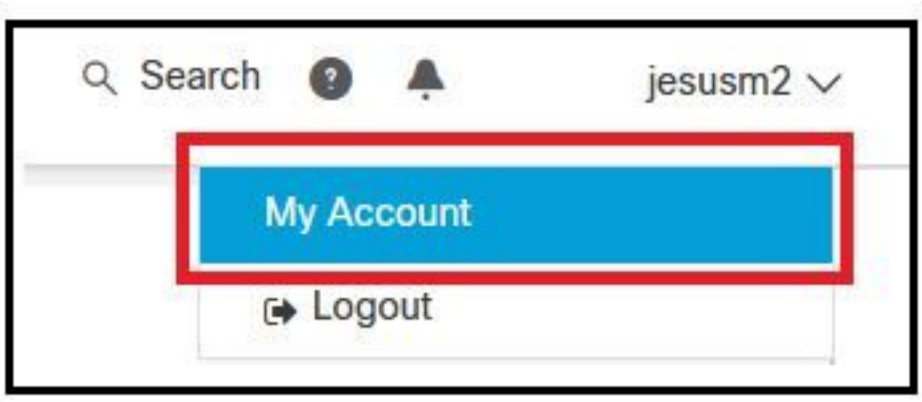
In the integration with Secure X, Threat Grid is a reference module and provides the ability to pivot into the Threat Grid Portal to gather additional intelligence about file hashes, IPs, domains, and URLs in the Threat Grid knowledge store.

Configure

Threat Grid portal - Authorize Threat Grid and get API key

Step 1. Log in to **Threat Grid**, use Administrator credentials.

Step 2. Navigate to **My Account** section, as shown in the image.



Step 3. Navigate to the **Connections** section and select **Connect Threat Response** option as shown in the image.

Sep 4. Select Authorize option in order to allow Threat Grid to access to Threat Response, as shown in the image.

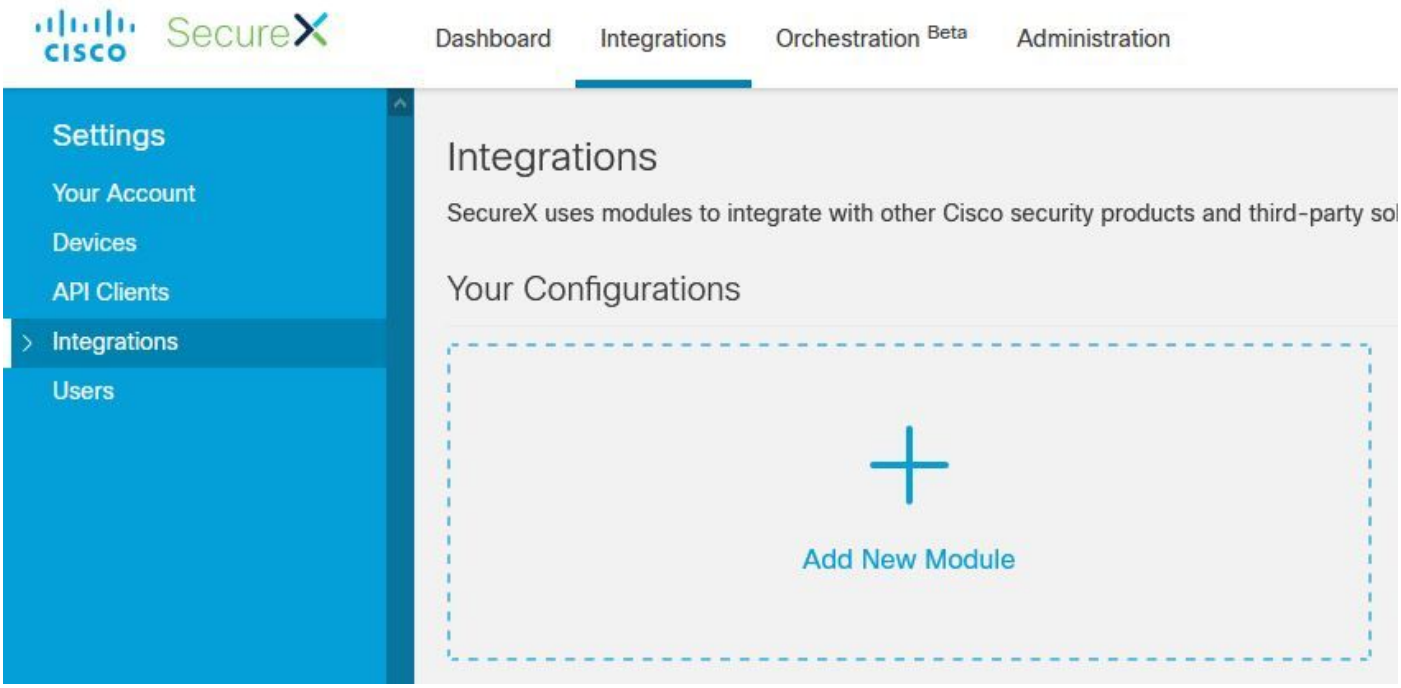
Step 5. The **Access Authorized** message appears to verify Threat Grid has access to Threat Response threat intelligence and enrichment capabilities, as shown in the image.

Step 6. Navigate to **My Account > API > API Key**, copy the **API key**, as shown in the image.

Secure X portal - Configure Threat Grid Module

Step 1. Log in to **Secure X**, use Administrator credentials.

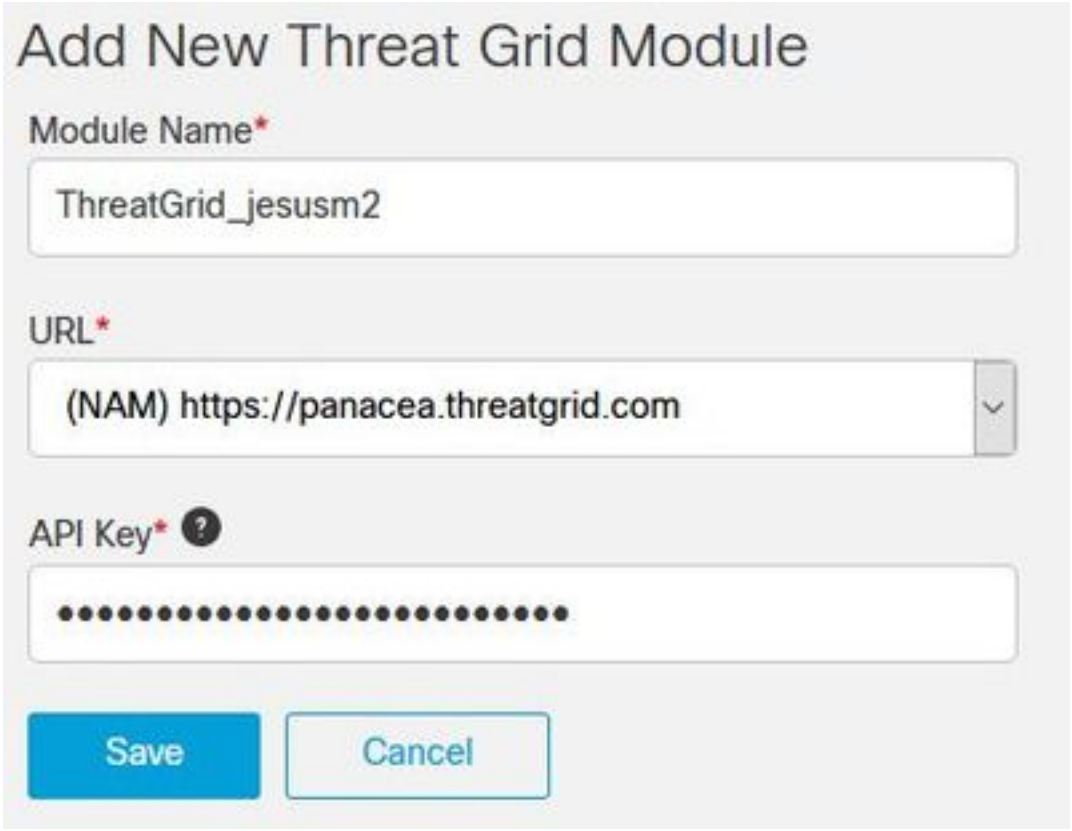
Step 2. Navigate to the **Integrations** tab, select **Integrations > Add New Module**, as shown in the image.



Step 3. On the **Integrations** page, select **Add New Module** in the Threat Grid module pane, as shown in the image.

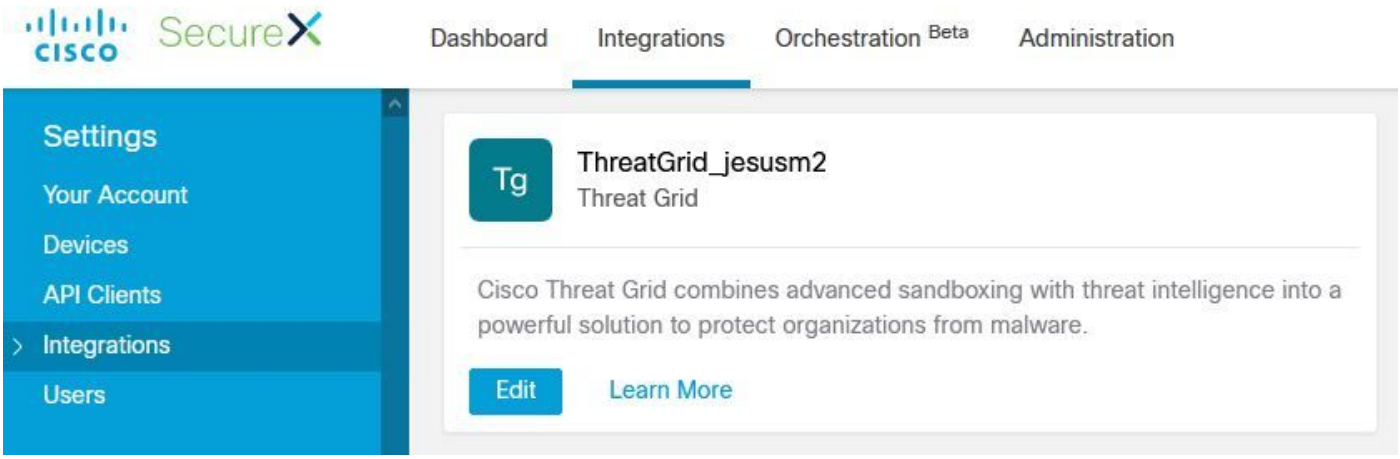
Step 4. The **Add New Module** form opens. Complete the form and select **Save** to complete the Threat Grid module configuration, as shown in the image.

- **Module Name** - Leave the default name or enter a name that is meaningful to you.
- **URL** - From the drop-down list, choose the appropriate URL for the location where your Threat Grid account is based (North America or Europe). Ignore the Other option for now.
- **API Key** - Threat Grid API Key (copy and paste the API Key from TG page).



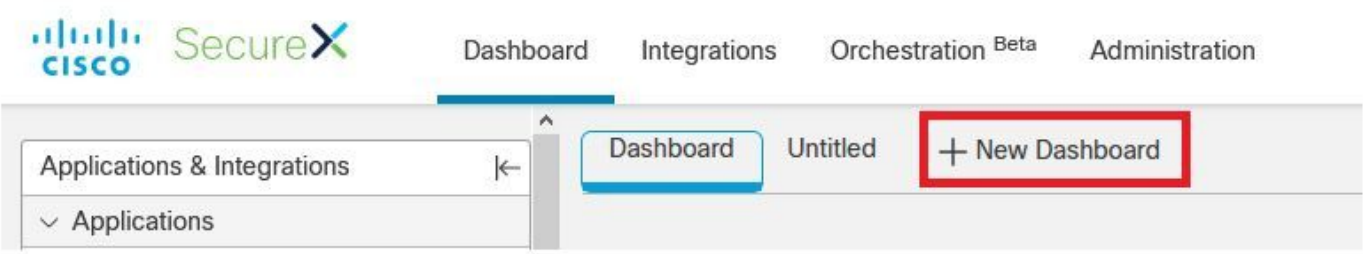
Step 5. Threat Grid is now displayed under your configurations on the **Integrations** page, as shown in the image.

(TG is available from pivot menus and in casebooks for improved threat investigation).



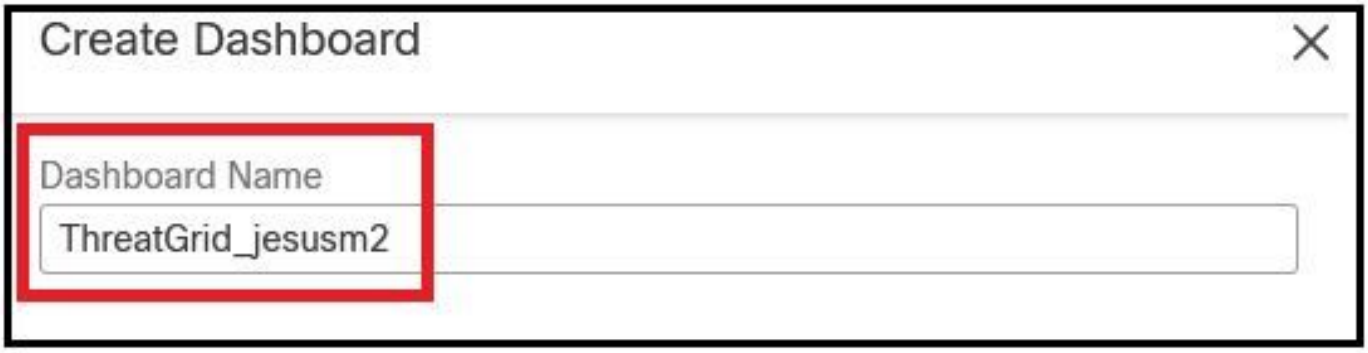
Secure X Portal - Add Threat Grid Dashboard

Step 1. On Secure X main page, select **+New Dashboard.**



Step 2. Select your Threat Grid module.

Step 3. Set a **Dashboard Name.**



Step 4. Mark the options based on your requirements and click on **Save.**