Integrate CTR and Threat Grid Cloud

Contents

Introduction

This document describes the steps to Integrate Cisco Threat Response (CTR) with Threat Grid (TG) Cloud in order to perform CTR investigations.

Contributed by Jesus Javier Martinez, and Edited by Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Threat Response
- Threat Grid

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)

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 impacting the user environment.

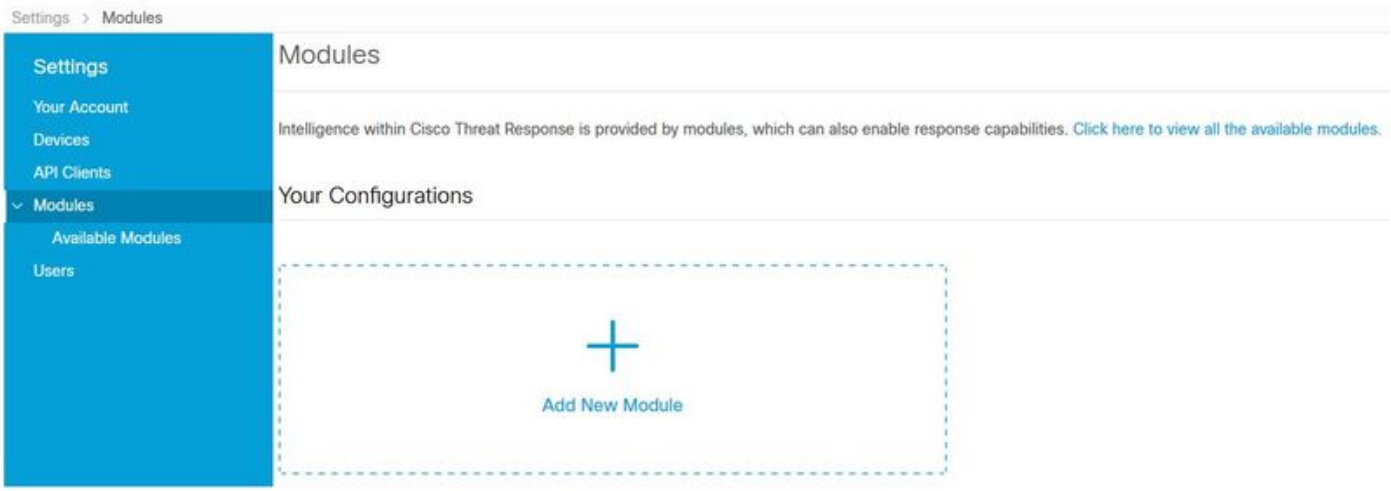
In the integration with Cisco Threat Response, Threat Grid is a reference module and provides the ability to pivot into the Threat Grid Portal to gather additional intelligence about file hashes, IPs, domains, and URLs in the Threat Grid knowledge store.

Configure

CTR Console - Configure Threat Grid Module

Step 1. Log in to Cisco Threat Response using Administrator credentials.

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



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

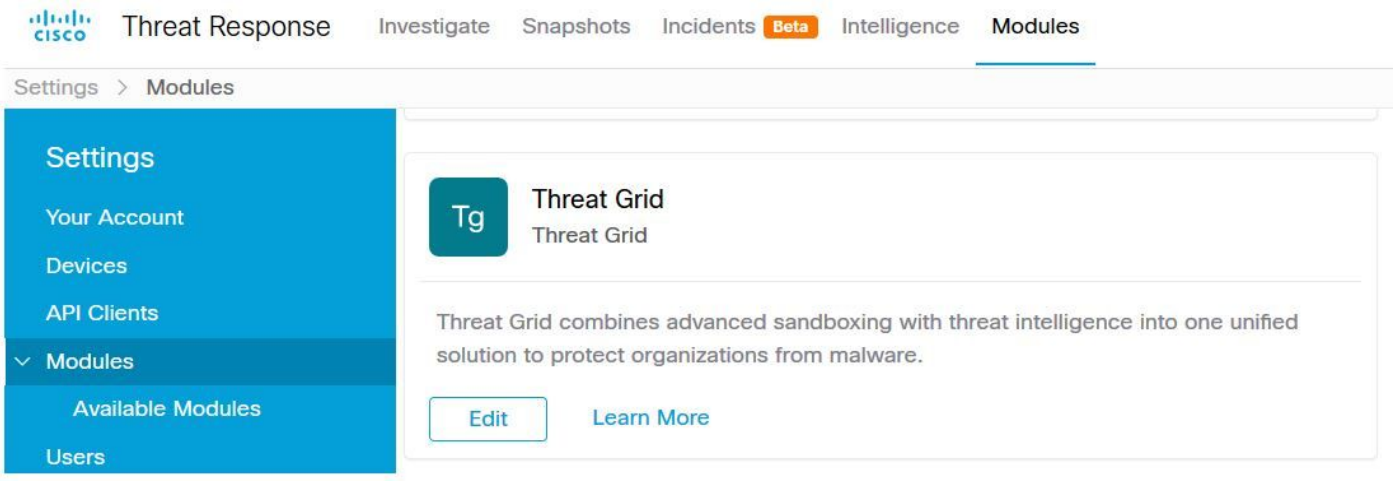
Step 4. The **Add New Module** form opens. Complete the form as shown in the image.

- **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.

Step 5. Select **Save** to complete the Threat Grid module configuration.

Step 6. Threat Grid is now displayed under your configurations on the **Modules** page as shown in the image.

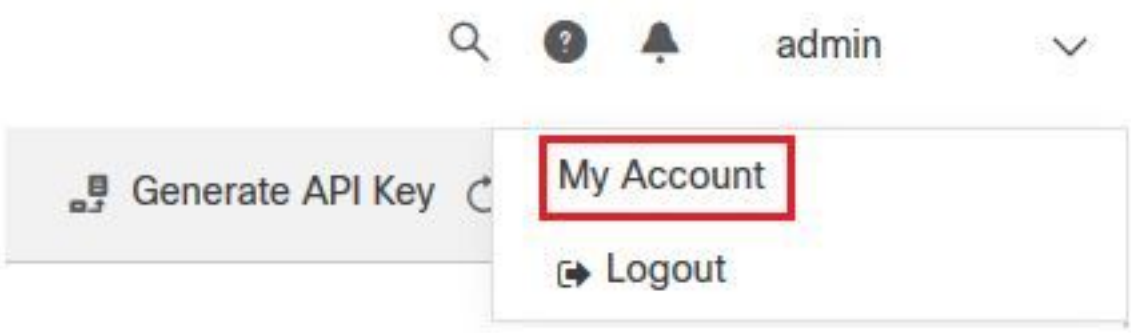
(TG is available from pivot menus and in casebooks for improved threat investigation).



Threat Grid console - Authorize Threat Grid to access Threat response

Step 1. Log in to Threat Grid using Administrator credentials.

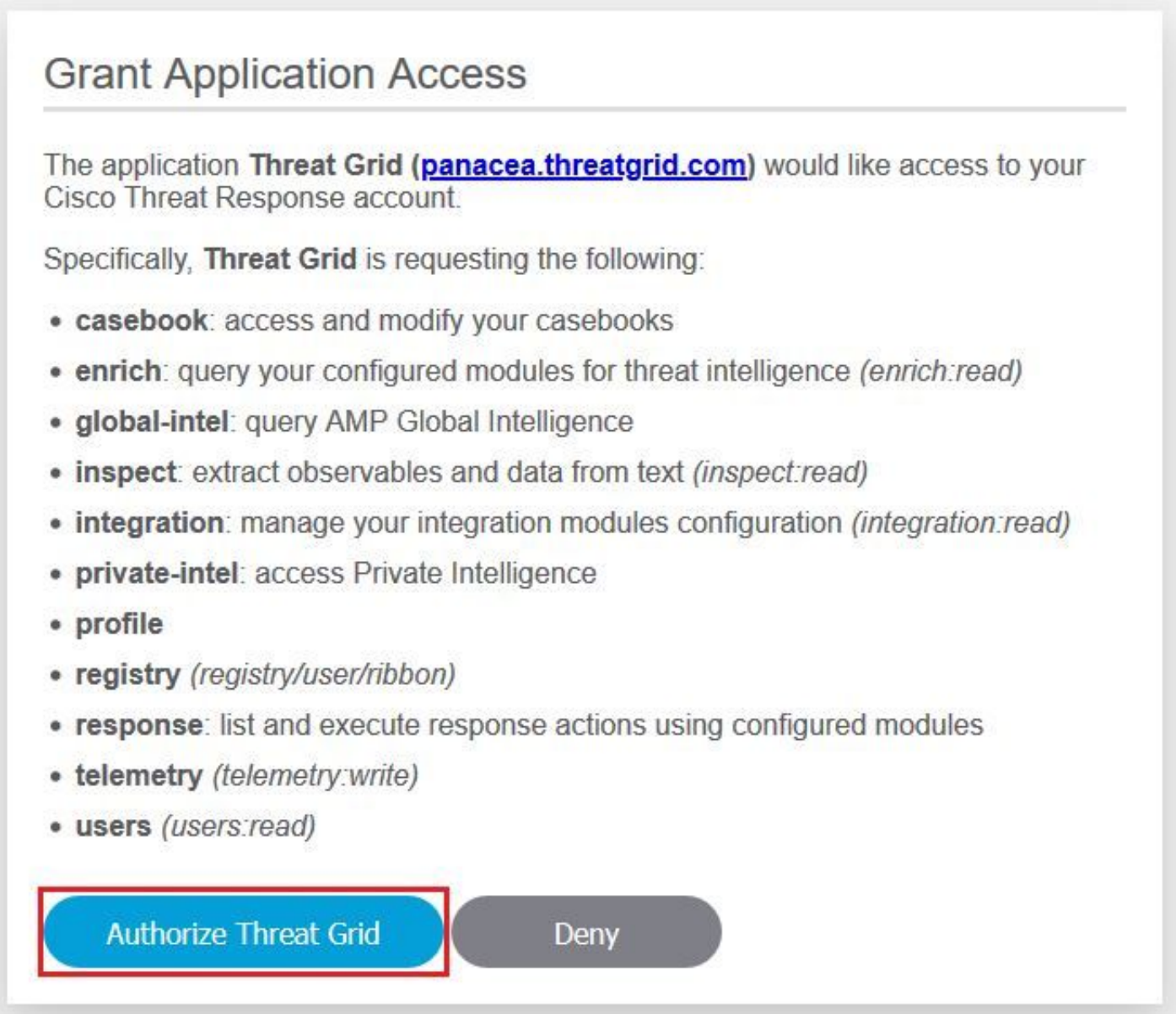
Step 2. Navigate to **My Account** section, as shown in the image.



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 Cisco Threat Response, as shown in the image.

Step 5. Select **Authorize Threat Grid** option in order to grant application access, as shown in the image.

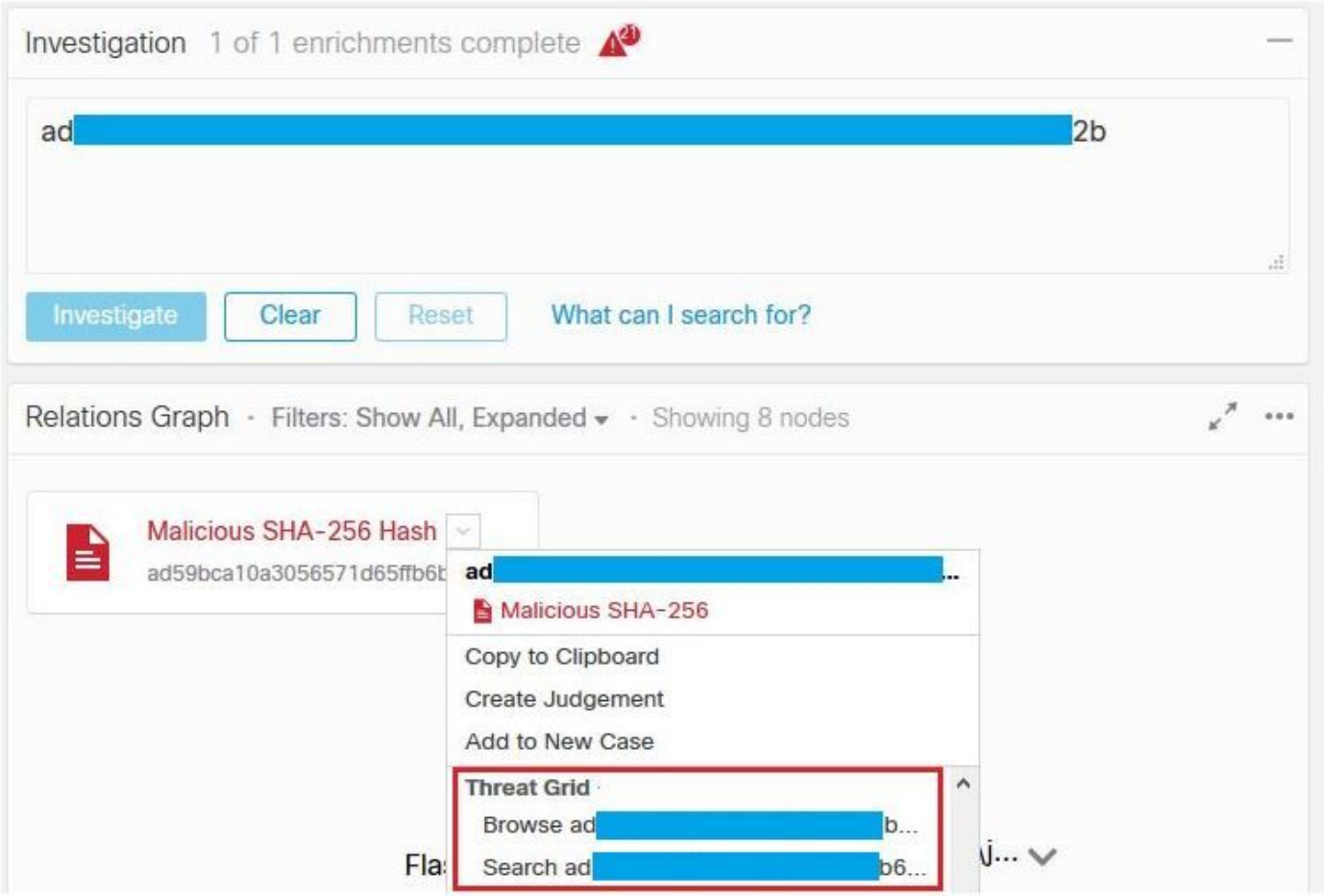


Step 6. The Access Authorized message appears to verify Threat Grid has access to Threat Response threat intelligence and enrichment capabilities, as shown in the image.

Verify

Use this section to confirm that your configuration works properly.

In order to verify the CTR and TG Integration, you can do an **Investigation** on CTR console, when all **Investigation** details appear, you are able to see Threat Grid option, as shown in the image.



You can select Browse or Search Threat Grid option and it redirects into the Threat Grid Portal to gather additional intelligence about files / hashes / IPs / domains / URLs in the Threat Grid knowledge store, as shown in the image.