Understand how to Link CTR to Umbrella

Contents

Introduction

This document describes how to connect the Cisco Threat Response (CTR) portal with Cisco Umbrella and all prerequisites required.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

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.

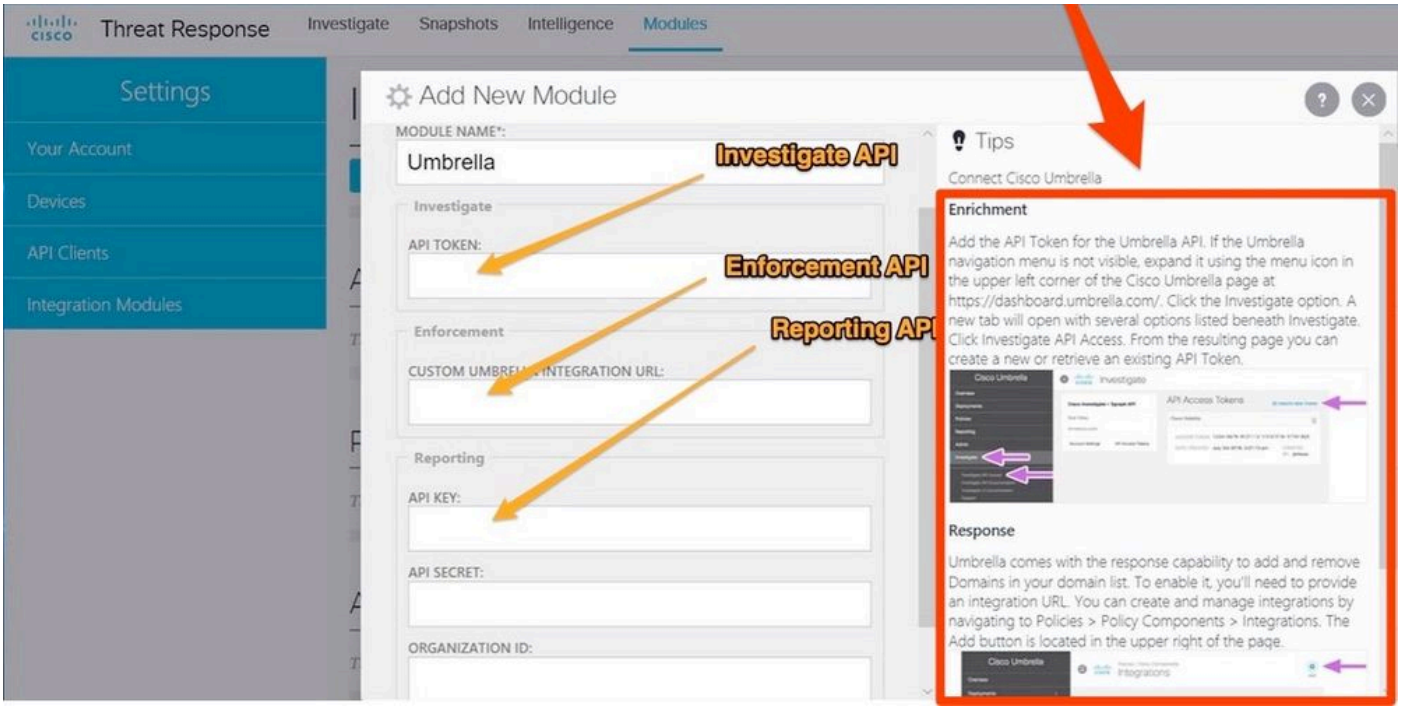
Overview

This article discusses how to connect the CTR portal with Umbrella and all prerequisites required to make this connection. The CTR links in three Umbrella components:

- Investigate (Requires Cisco Umbrella subscription)
- Enforcement (Requires elevated Cisco Umbrella subscription with access to Enforcement API)
- Reporting

Configure the CTR Link to Umbrella

Linking CTR to Umbrella is comprised of up to three steps, depending on your level of Umbrella subscription. The linking page looks like this screenshot:



360034168072

Linking Umbrella Reporting to CTR

All Umbrella users have access to the reporting API. To get started, you need an API key and secret. See the Umbrella API documentation for how to find your API authentication details. Finally, enter the organization ID of the Umbrella organization to link to the CTR.

Requirements

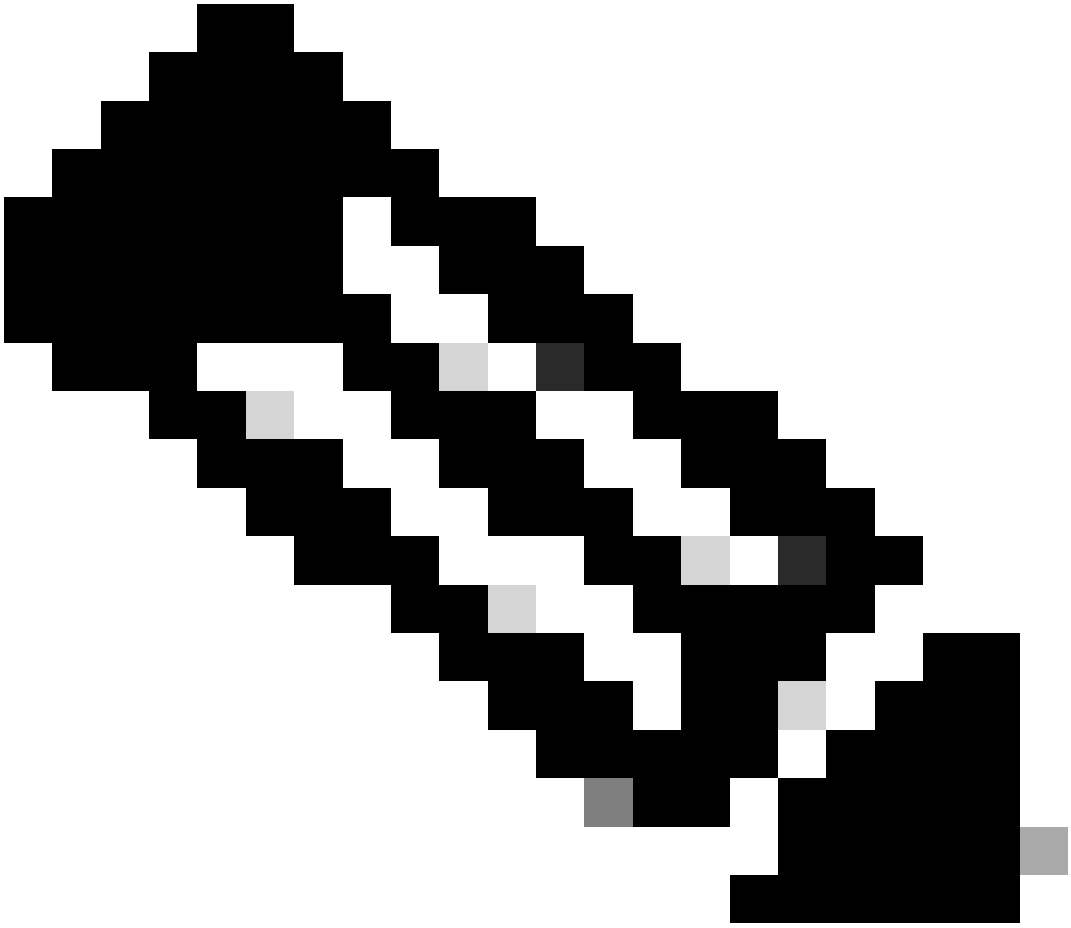
- Subscribe to Umbrella services.

Linking Umbrella Enforcement to CTR

The Umbrella Enforcement API is a feature that allows for automated addition of new domains to a security enforcement list. For more information, review the Umbrella documentation.

Requirements

- Subscribe to Umbrella Services with access to the Enforcement API in the dashboard.



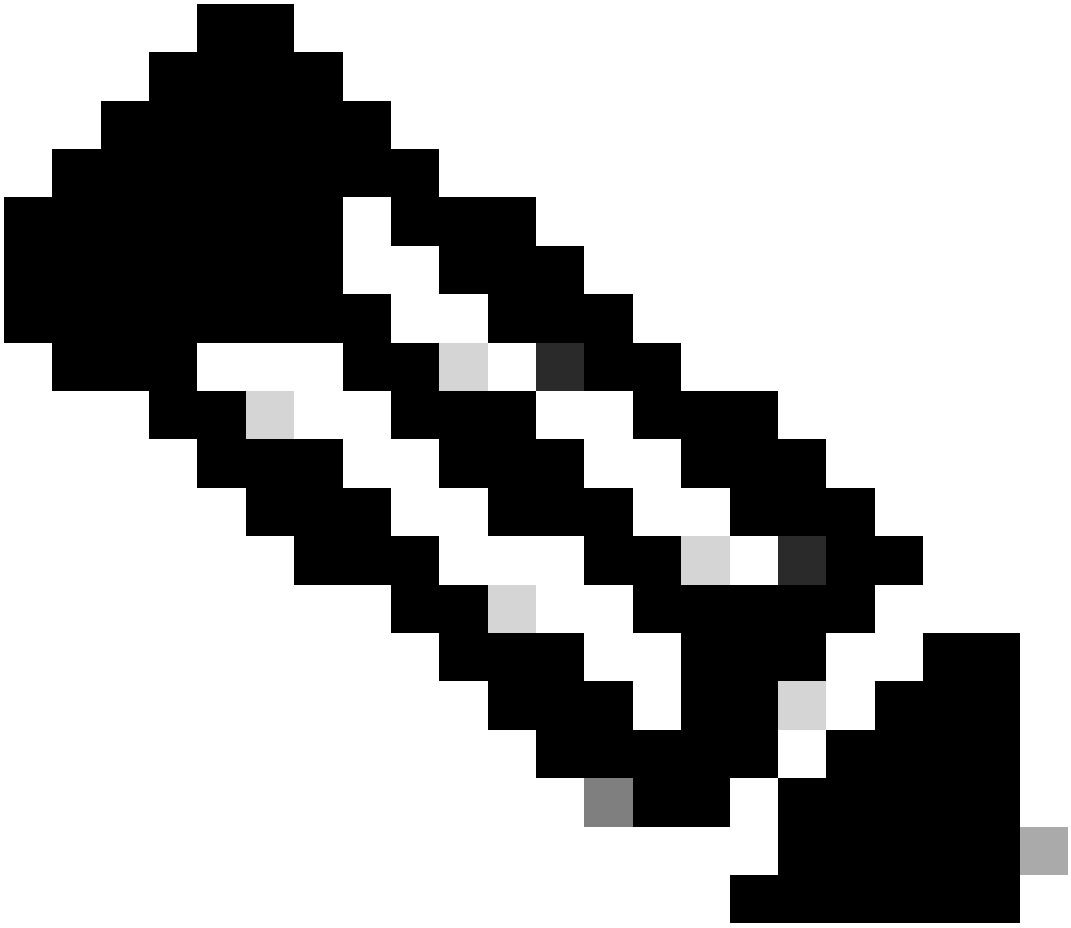
Note: If you do not have the Umbrella Enforcement API for custom integrations in your Umbrella dashboard and would like to have access, please contact your Cisco Umbrella representative.

Linking Umbrella Investigate to CTR

The Umbrella Investigate API is a feature that allows for queries against the Cisco Umbrella Investigate system outside of the Investigate web portal. API access is limited. For more information, review the Umbrella documentation.

Requirements

- Subscribe to Cisco Umbrella Investigate (https://investigate.umbrella.com).
  - The package or add-on for the Investigate API must be active.
  - Some entitlements allow for a low volume of queries. CTR can function up until the query limit is reached.



Note: If you do not have the Umbrella Enforcement API for custom integrations in your Umbrella dashboard and would like to have access, please contact your Cisco Umbrella representative.