



Introduction

This chapter provides a brief description of the Cisco Threat Grid Appliance, the intended audience and how to access relevant product documentation. It includes the following:

- [About Cisco Threat Grid Appliance, on page 1](#)
- [What's New In This Release, on page 2](#)
- [Audience, on page 2](#)
- [Product Documentation, on page 2](#)
- [Threat Grid Support, on page 3](#)

About Cisco Threat Grid Appliance

The Cisco Threat Grid appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. A Threat Grid Appliance provides the complete Threat Grid malware analysis platform, installed on a Cisco Threat Grid M5 Appliance server (v2.7.2 and later). It empowers organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.



Note Cisco UCS C220-M3 (TG5000) and Cisco UCS C220 M4 (TG5400) servers are still supported for Threat Grid Appliance but the servers are end of life. See the Server Setup chapter in the *Cisco Threat Grid Appliance Setup and Configuration Guide* (v2.7 and earlier) for instructions.

Many organizations that handle sensitive data, such as banks and health services, must follow various regulatory rules and guidelines that do not allow certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Cisco Threat Grid Appliance on-premises, organizations can send suspicious documents and files to it to be analyzed without leaving the network.

With a Threat Grid Appliance, security teams can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. The appliance correlates the analysis results with hundreds of millions of previously analyzed malware artifacts, to provide a global view of malware attacks and campaigns, and their distributions. A single sample of observed activity and characteristics can quickly be correlated against millions of other samples to fully understand its behaviors within an historical and global context. This ability helps security teams to effectively defend the organization against threats and attacks from advanced malware.

What's New In This Release

The following changes have been implemented in this guide in Version 2.10:

Table 1: Changes in Version 2.10 - January 28, 2020

Feature or Update	Section
Added support for RADIUS authentication.	User Interfaces Network Interfaces Firewall Rules

Audience

Before a new appliance can be used for malware analysis, it must be set up and configured for the organization's network. This guide is intended for the security team IT staff tasked with setting up and configuring a new Threat Grid Appliance.

This document describes how to complete the initial setup and configuration for a new Threat Grid Appliance, up to the point where malware samples can be submitted to it for analysis.

Product Documentation

The latest versions of Cisco Threat Grid Appliance product documentation can be found on Cisco.com:

- [Cisco Threat Grid Appliance Release Notes](#)
- [Cisco Threat Grid Version Lookup Table](#)
- [Cisco Threat Grid Appliance Administrator Guide](#)
- [Cisco Threat Grid M5 Hardware Installation Guide](#)



Note The Cisco Threat Grid M5 Appliance is supported in Threat Grid Version 3.5.27 and later, and appliance version 2.7.2 and later.



Note Prior versions of Cisco Threat Grid Appliance product documentation can be found at [Threat Grid Install and Upgrade](#).

Threat Grid Portal UI Online Help

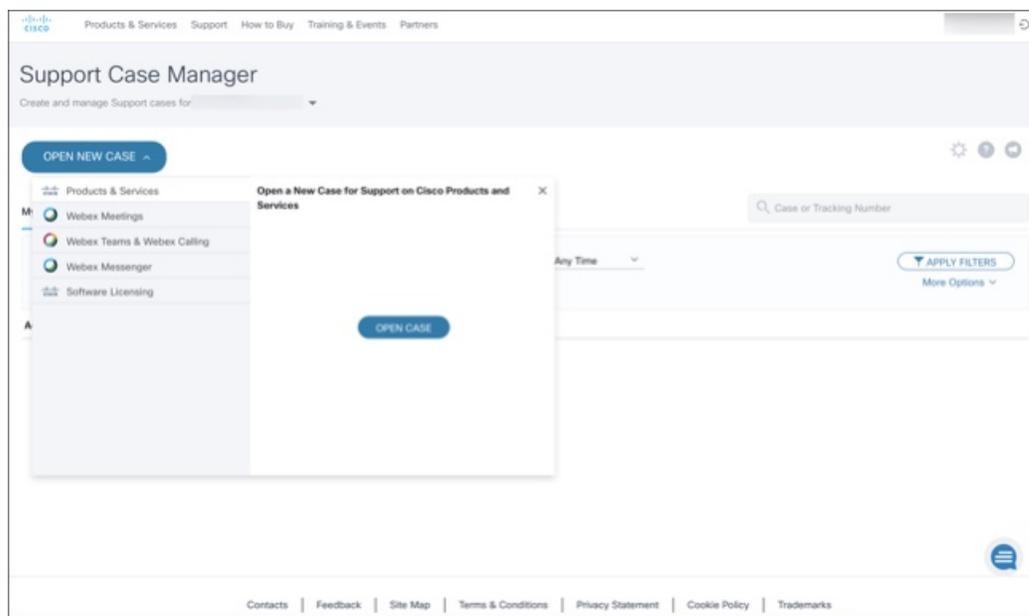
Threat Grid Portal user documentation, including Release Notes, Threat Grid Online Help, API documentation, and other information is available from the **Help** menu located in the navigation bar at the top of the user interface.

Threat Grid Support

If you have questions or require assistance with Threat Grid, open a Support Case at <https://mycase.cloudapps.cisco.com/case>.

Step 1 In Support Case Manager, click **Open New Case > Open Case**.

Figure 1: Open New Case



Step 2 Click the **Ask a Question** radio button and search for your Cisco Security **Product Serial Number** or **Product Service Contract**. This should be the serial number or service contract for Threat Grid.

Step 3 If you want to bypass entitlement, choose **Contract Data not in C3** and click **Next**.

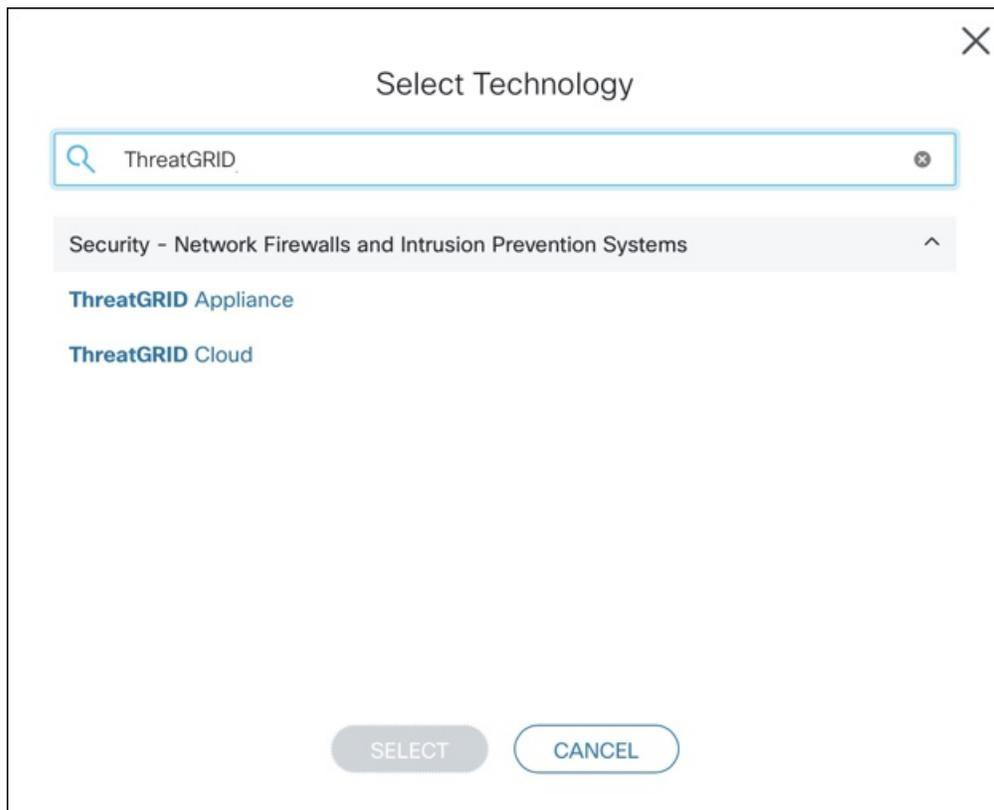
Figure 2: Check Entitlement

The screenshot shows the Cisco Support Case Manager interface. At the top, there are navigation links for Products & Services, Support, How to Buy, Training & Events, and Partners. The main heading is 'Support Case Manager' with a sub-heading 'Open a new support case for'. Below this is a progress bar with three steps: 1. Check Entitlement (highlighted with a blue circle), 2. Describe Problem, and 3. Review & Submit. Under the 'Check Entitlement' step, there are three radio button options for 'Request Type': 'Diagnose and Fix', 'Request RMA', and 'Ask a Question' (which is selected). Below these are two dropdown menus: 'Find Product by Serial Number' and 'Find Product by Service Agreement'. Under the 'Bypass Entitlement' section, there is a dropdown menu with the text 'CPR / Contract data not in C3'. At the bottom, there are two buttons: 'NEXT' and 'Save draft and exit'.

Step 4 On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Threat Grid in the title).

Step 5 Click **Manually select a Technology** and search for **ThreatGRID**.

Figure 3: Select Technology



Step 6 Choose **ThreatGRID Appliance** from the list and click **Select**.

Step 7 Complete the remainder of the form and click **Submit**.

If you are unable to open a case online, contact Cisco Support:

- **US and Canada:** 1-800-553-2447
- **Worldwide Contacts:** <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

For additional information on how to request support:

- See the blog post: **Changes to the Cisco Threat Grid Support Experience** at <https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407>
- See the main **Cisco Support & Downloads** page at: <https://www.cisco.com/c/en/us/support/index.html>

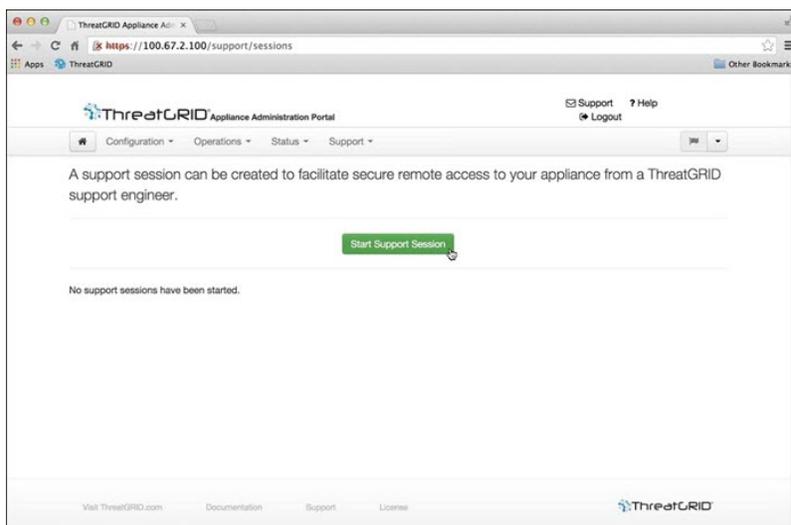
Enable Support Mode

If you require support from a Threat Grid engineer, they may ask you to enable Support Mode, which is a live support session that gives Threat Grid support engineers remote access to the appliance. Normal operations of the appliance will not be affected.

You can enable Support Mode from the OpAdmin portal **Support** menu. You can also enable it from the TGSN Dialog, the legacy Face Portal UI, and when booting up in Recovery Mode.

Step 1 In the OpAdmin portal, click the **Support** menu and choose **Live Support Session**.

Figure 4: OpAdmin Start a Live Support Session



Step 2 Click **Start Support Session**.

Note You can exit the OpAdmin configuration wizard to enable Support Mode prior to licensing.

Support Snapshots

A support snapshot is basically a snapshot of the running system, which contains logs, psoutput, etc., to help Support staff troubleshoot any issues.

Step 1 Verify that SSH is specified for Support Snapshot services.

Step 2 From the **Support** menu, choose **Support Snapshots**.

Step 3 Take the snapshot.

Step 4 Once you take the snapshot, download it as a **.tar** or **.gz** file, or click **Submit**, to automatically upload the snapshot to the Threat Grid snapshot server.