



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](#)
- [Audience, on page 2](#)
- [Assumptions, on page 2](#)
- [Product Documentation, on page 2](#)
- [What's New In This Release, on page 3](#)
- [Supported Browsers, on page 3](#)
- [Updates, on page 4](#)
- [Threat Grid Support, on page 4](#)
- [Setup and Configuration Overview, on page 6](#)

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.

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.

Assumptions

It is assumed that you have gathered the necessary information and completed the planning steps as described in the *Cisco Threat Grid Appliance Administration Guide*.

It is also assumed that you have already set up the Threat Grid Appliance based on the instructions in the *Cisco Threat Grid M5 Hardware Installation Guide*.

If you have not yet completed these two tasks, please do so before you begin the steps described in this Getting Started Guide.

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 Administration 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.

What's New In This Release

The following changes have been implemented in this guide in Version 2.11:

Table 1: Changes in Version 2.11 - May 8, 2020

Feature or Update	Section
Moved the following information to the <i>Cisco Threat Grid Appliance Administration Guide</i> : <ul style="list-style-type: none"> • Enable Support Mode • Support Snapshots • Planning 	NA
Moved the following topics to the Introduction chapter in this guide: <ul style="list-style-type: none"> • Supported Browsers • Updates 	Supported Browsers Updates
OpAdmin is replaced with a completely modernized Admin user interface.	NA
Updated Admin UI configuration and screenshots.	Admin UI Configuration

Supported Browsers

Threat Grid supports the following browsers:

- Google Chrome™
- Mozilla Firefox®
- Apple Safari®



Note Microsoft Internet Explorer is **not** supported.

Updates

The initial Threat Grid Appliance setup and configuration steps **must be completed** before installing any Threat Grid Appliance updates. We recommend that you check for updates immediately after completing the initial configuration (see [Install Updates](#)).

Threat Grid Appliance updates cannot be downloaded until the license is installed, and the update process requires that the initial appliance configuration is completed. Updates must be done in sequence.



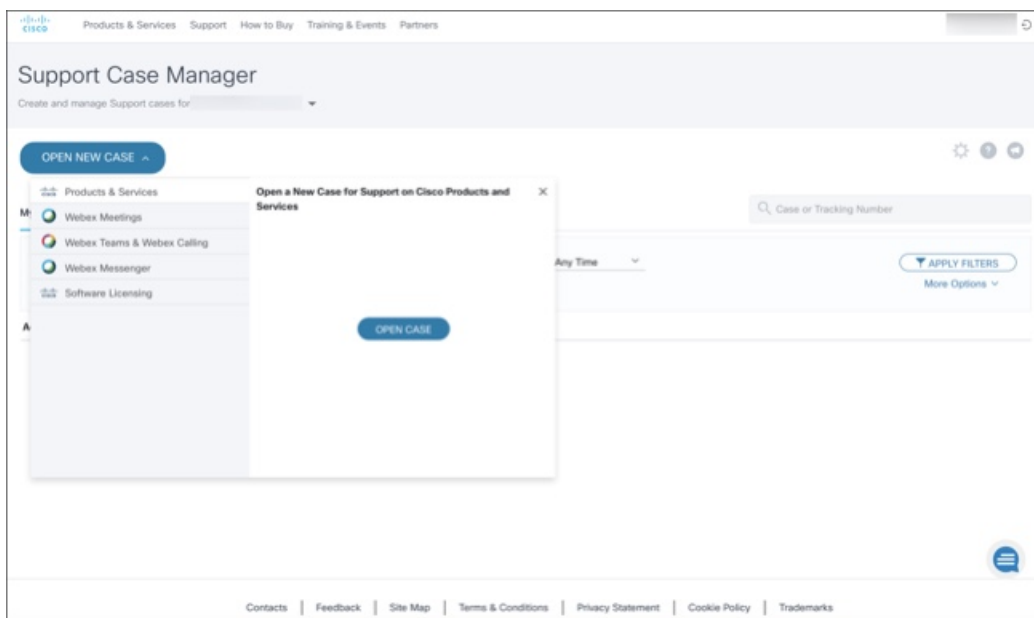
Note Verify that SSH is specified for updates.

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



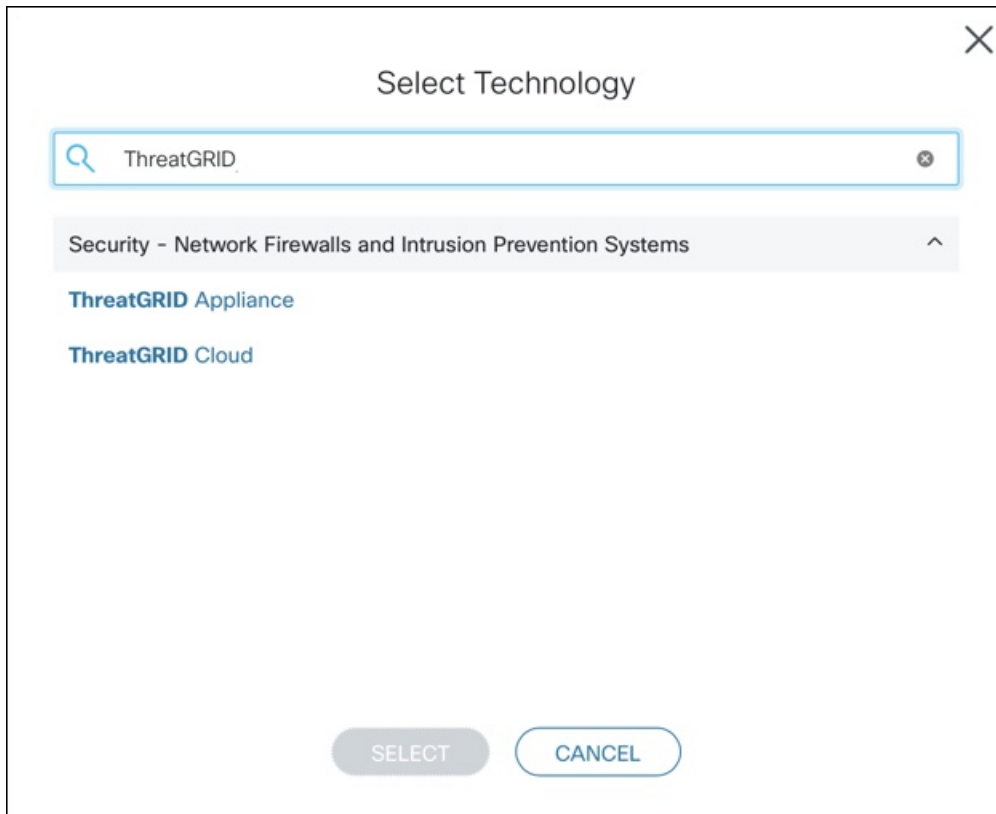
Step 2 Click the **Ask a Question** radio button and search for your Cisco Security **Product Serial Number** or **Product Service Contract**. This should be the serial number or service contract for Threat Grid.

Figure 2: Check Entitlement

The screenshot displays the 'Support Case Manager' interface. At the top, there is a navigation bar with links for 'Products & Services', 'Support', 'How to Buy', 'Training & Events', and 'Partners'. Below this, the main heading is 'Support Case Manager' with a sub-heading 'Open a new support case for'. A progress bar shows 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 expandable sections: 'Find Product by Serial Number' and 'Find Product by Service Agreement'. A 'Bypass Entitlement' section contains 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 3** On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Threat Grid Appliance in the title).
- Step 4** Click **Manually select a Technology** and search for **ThreatGRID**.

Figure 3: Select Technology



The screenshot shows a 'Select Technology' dialog box. At the top right is a close button (X). Below the title is a search input field containing 'ThreatGRID'. A dropdown menu is open, showing a category 'Security - Network Firewalls and Intrusion Prevention Systems' with an upward arrow. Underneath are two search results: 'ThreatGRID Appliance' and 'ThreatGRID Cloud'. At the bottom of the dialog are two buttons: 'SELECT' and 'CANCEL'.

Step 5 Choose **ThreatGRID Appliance** from the list and click **Select**.

Step 6 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 Enable Support Mode and Support Snapshots in the *Threat Grid Appliance Administration Guide*.
- 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>

Setup and Configuration Overview

The following setup and initial configuration steps are described in this guide:

- Initial Network Configuration
- Admin UI Configuration
- Installing Updates
- Testing Appliance Setup



Note You should allow approximately 1 hour to complete the configuration.

Additional tasks that require administrator configuration (such as license installation, email server, and SSL certificates) are documented in the [Cisco Threat Grid Appliance Administration Guide](#).

