

Introduction

This chapter provide 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 1
- Audience, on page 2
- Product Documentation, on page 3
- 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 single UCS server: Cisco UCS C220-M3 (TG5000) or Cisco UCS C220 M4 (TG5400). It empowers organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.

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 are able to 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 2.7:

Table 1: Changes in Version 2.7.2

Feature or Update	Section
Background Elasticsearch index migration to ES6-native indexes enabled.	Database Schema Updates
Database base backups are only retained until a new base backup has been successfully created.	Backup Data Retention

Table 2: Changes in Version 2.7.1

Feature or Update	Section
Simulated Only option for Network Exit Mode	Configure Network Exit
Network Simulation option for sample analysis.	See note in Configure Network Exit

Table 3: Changes in Version 2.7

Feature or Update	Section
Network configuration in recovery mode now mirrow the full system.	Configure Networking in Recovery Mode
Threat Grid Appliance serial number is now used as hostname.	Configuration Using OpAdmin Portal
Configuring SSH public key for access to the Threat Grid Appliance disables password-based authentication via SSH.	Configure SSH Keys
TLS v1.0 and v1.1 disabled in Admin interface.	About SSL Certificates and Threat Grid Appliance
XFS is primary file system.	File System
Enhanced data reset process.	Data Reset Process
Sample deletion now includes artifacts, which matches the behavior of the cloud product.	Sample Deletion

Audience

This guide is intended to be used by the Threat Grid Appliance administrator after the appliance has been set up and configured, and an initial test malware sample has been successfully submitted and analyzed. It describes how to manage organizations and users for the Threat Grid malware analysis tool, appliance updates, backups, and other server administration tasks.

This guide also provides information for administrators who are integrating the Threat Grid Appliance with other Cisco products and services, such as Cisco Email Security Appliance, Cisco Web Security Appliance, and AMP for Endpoints Private Cloud devices.

Note For information about Secure Malware Analytics Appliance setup and configuration, see the *Cisco Threat Grid Appliance 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*

Prior version of Cisco Threat Grid Appliance product documentation can be found on the Threat Grid Install and Upgrade page.

Threat Grid Portal UI Online Help

Threat Grid Portal user documentation, including *Release Notes*, *Using 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.

Email Security Appliance and Web Security Appliance Documentation

For information on connecting an Email Security Appliance or Web Security Appliance, see Connecting ESA/WSA Appliances to a Threat Grid Appliance in this guide.

See the instructions for *Enabling and Configuring File Reputation and Analysis Services* in the online help or user guide for your ESA/WSA:

- *Cisco Secure Email Gateway User Guide*
- *Cisco Secure Web Appliance User Guide*

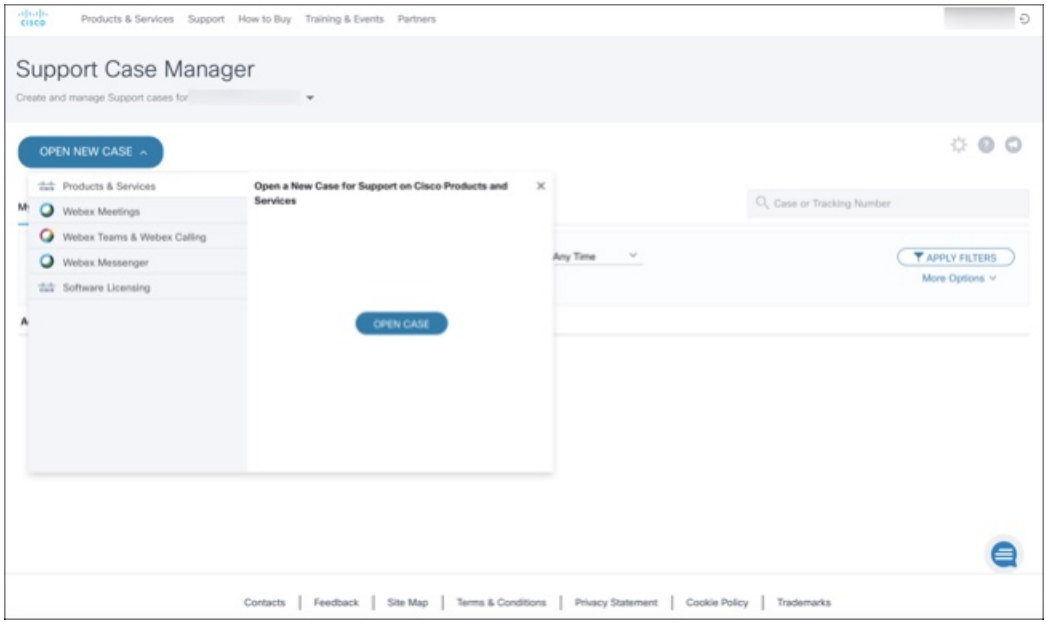
Threat Grid Support

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

Procedure

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

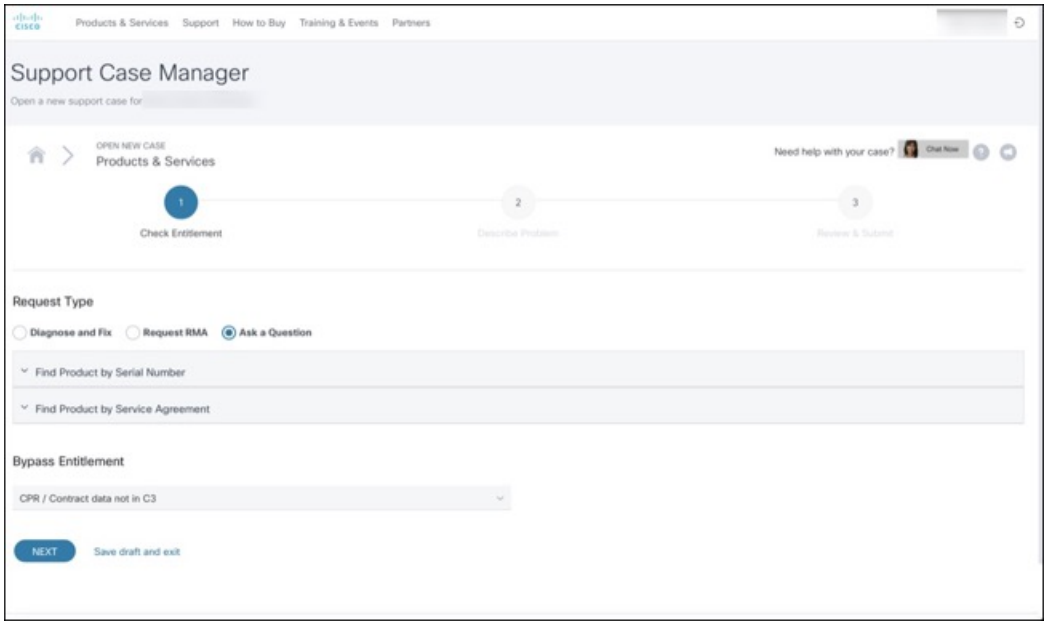
Figure 1: Open New Case



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**.

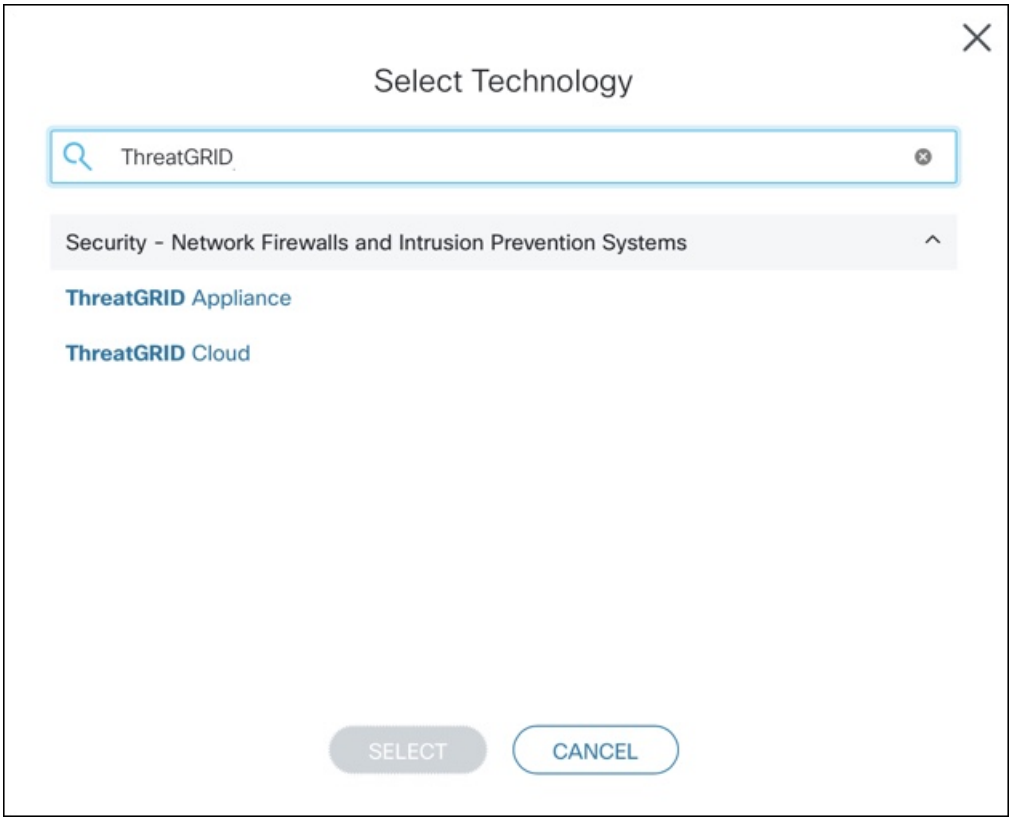
Figure 2: Check Entitlement



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

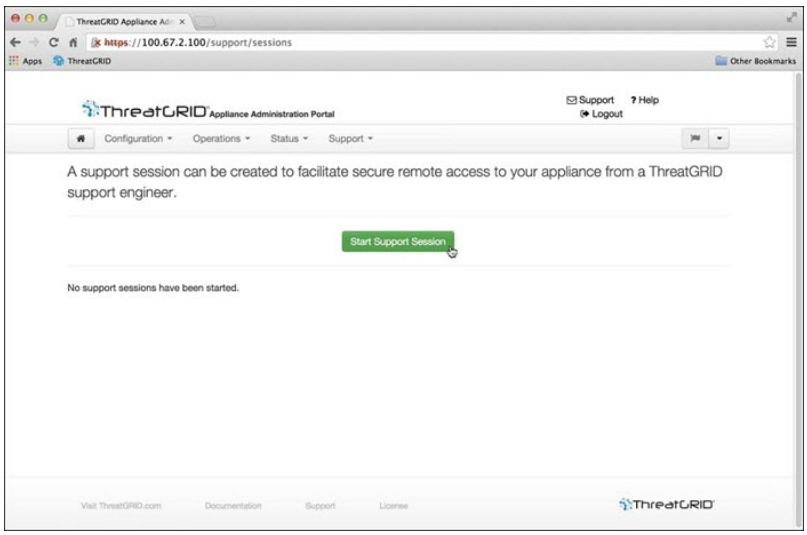
If you require support from a Threat Grid engineer, they may ask you to enable Support Mode, which is a live support session that gives Threat Grid support engineers remote access to the appliance. Normal operations of the appliance will not be affected.

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

Procedure

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.

Procedure

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.