Introduction

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

About Cisco Secure Malware Analytics Appliance

The Cisco Secure Malware Analytics appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. A Secure Malware Analytics Appliance provides the complete malware analysis platform, installed on a Cisco Secure Malware Analytics 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 M4 (TG5400) servers are still supported for Secure Malware Analytics Appliance but the servers are end of life. See the Server Setup chapter in the *Cisco Secure Malware Analytics 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 Secure Malware Analytics Appliance on-premises, organizations can send suspicious documents and files to it to be analyzed without leaving the network.

With a Secure Malware Analytics 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 Secure Malware Analytics Appliance.

This document describes how to complete the initial setup and configuration for a new Secure Malware Analytics 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 Secure Malware Analytics Appliance Administration Guide*.

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

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

Product Documentation

The latest versions of Cisco Secure Malware Analytics Appliance product documentation is found on Cisco.com:

- *Cisco Secure Malware Analytics Appliance Release Notes*
- *Cisco Secure Malware Analytics Version Lookup Table*
- *Cisco Secure Malware Analytics Appliance Administration Guide*
- *Cisco Secure Malware Analytics M5 Hardware Installation Guide*

Note The Cisco Secure Malware Analytics M5 Appliance is supported in Secure Malware Analytics Version 3.5.27 and later, and appliance version 2.7.2 and later.

Note Prior versions of Cisco Secure Malware Analytics Appliance product documentation is found at Secure Malware Analytics Install and Upgrade.

Secure Malware Analytics Portal UI Online Help

Secure Malware Analytics Portal user documentation, including Release Notes, Secure Malware Analytics 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 2.18:

Table 1: Changes in Version 2.18 Release - October 1, 2022

Feature or Update	Section
Updated screenshots and instructions.	Admin UI Configuration

Supported Browsers

Secure Malware Analytics supports the following browsers:

- Google Chrome™

- Mozilla Firefox®

- Apple Safari®

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

Updates

The initial Secure Malware Analytics Appliance setup and configuration steps **must be completed** before installing any Secure Malware Analytics Appliance updates. We recommend that you check for updates immediately after completing the initial configuration (see Install Updates).

Secure Malware Analytics 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.

Support

If you have questions or require assistance with Secure Malware Analytics, 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
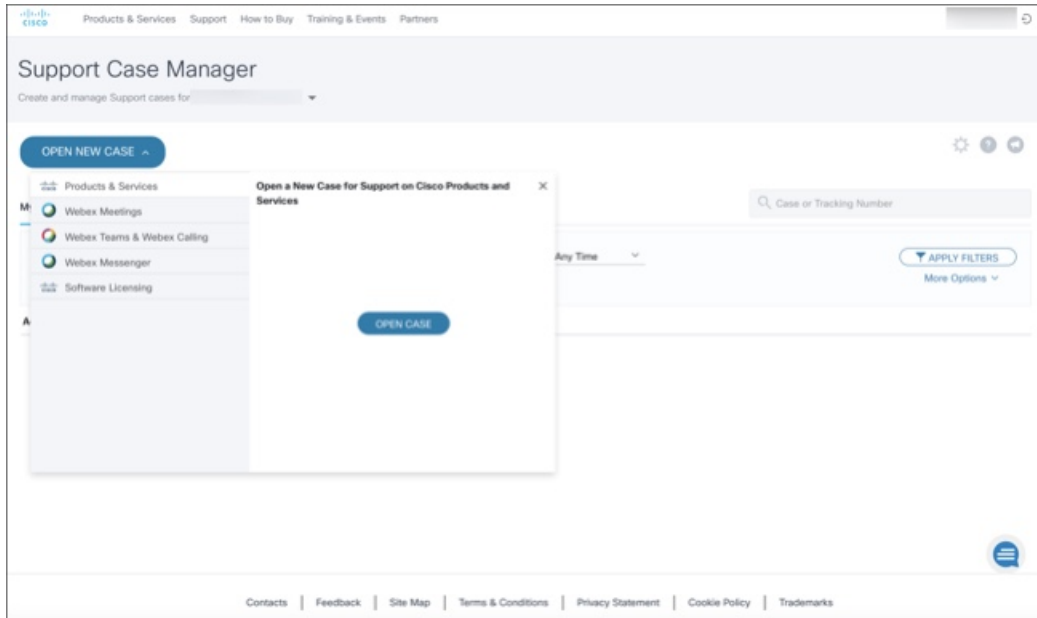
Step 2   Click the **Ask a Question** radio button and search for your Cisco Security **Product Serial Number** or **Product Service Contract**. This should be the serial number or service contract for Secure Malware Analytics.

Figure 2: Check Entitlement
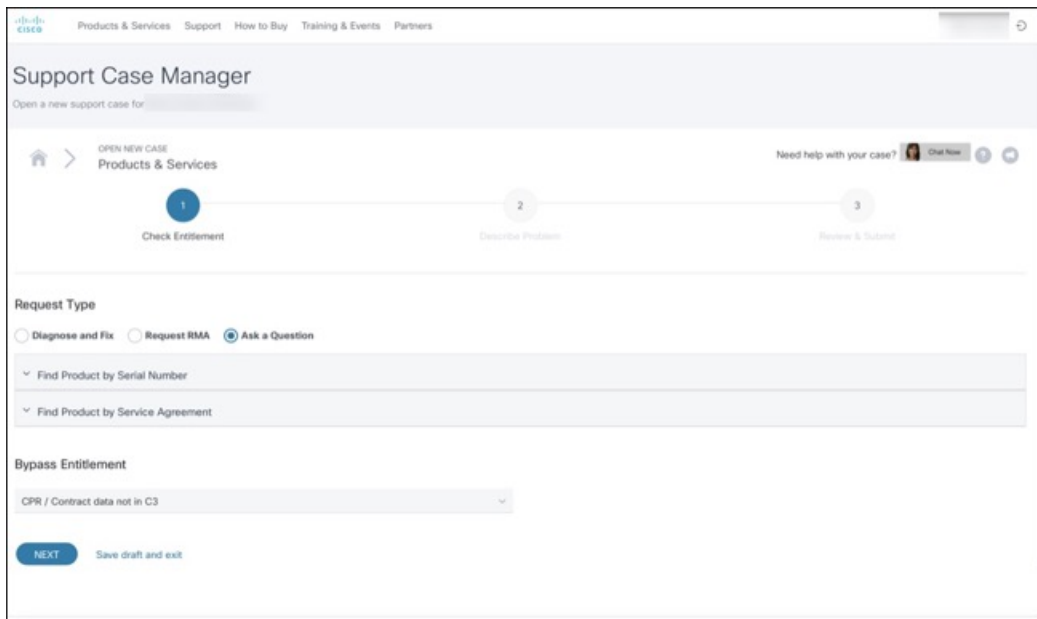
Step 3   On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Secure Malware Analytics Appliance in the title).

Step 4   Click **Manually select a Technology** and search for **Secure Malware Analytics**.

Figure 3: Select Technology

Select Technology

Q Secure Malware Analytics ✕

Security - Network Firewalls and Intrusion Prevention Systems

Cisco **Secure Malware Analytics** (Threat Grid) - SecureX Integration

Cisco **Secure Malware Analytics** Appliance (Threat Grid Appliance)

Cisco **Secure Malware Analytics** Cloud (Threat Grid Cloud)

Cancel   Select

Step 5   Choose **Cisco Secure Malware Analytics 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 *Secure Malware Analytics Appliance Administration Guide*.

- See the blog post: **Changes to the Cisco Secure Malware Analytics 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 Secure Malware Analytics Appliance Administration Guide*.