

Support

This chapter provides instructions for starting a support session and taking support snapshots to aid in resolving issues with the Secure Malware Analytics Appliance.

- Opening a Support Case, on page 1
- Live Support Session, on page 4
- Support Snapshots, on page 5

Opening a Support Case

If you have questions or require assistance with Secure Malware Analytics, open a case in Support Case Manager, which is located at https://mycase.cloudapps.cisco.com/case.

Note

If you are receiving support from a Cisco Secure Malware Analytics engineer, they may need remote access to your appliance. See Starting a Live Support Session to learn more about how to start a live support session, and take a snapshot of your appliance.

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

Figure 1: Open New Case

ei ei	alta ICO	Products & Services Support	How to Buy Training & Events Partners		Ð
S	up	port Case Manag	ger		
Cri	ate ar	nd manage Support cases for	v		
(OPE	EN NEW CASE			000
	***	Products & Services	Open a New Case for Support on Cisco Products and Services	×	
M	0	Webex Meetings	Dervices		Q, Case or Tracking Number
	0	Webex Teams & Webex Calling			
	0	Webex Messenger		Any Time V	More Options ~
	-	Software Licensing			More Options V
•			OPEN CASE		
			Contacts Feedback Site Map Terms & Cond	Itions Privacy Statement Cook	e Policy Trademarks

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.

clocder Products & Services Support How to Buy Training & E	vents Partners	Ð
Support Case Manager Open a new support case for		
PPEN NEW CASE Products & Services		Need help with your case? 🚺 Chait Name 💿 🔘
0	2	3
Check Entitiement		
Request Type Diagnose and Fix Request RMA		
Bypass Entitlement		
CPR / Contract data not in C3	~	
NEXT Save draft and exit		

Figure 2: Check Entitlement

- **Step 3** On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Secure Malware Analytics in the title).
- Step 4 Click Manually select a Technology and search for Secure Malware Analytics.

Figure 3: Select Technology

Q Secure Malware Analytics		×
Security - Network Firewalls and Intr	usion Prevention Systems	
Cisco Secure Malware Analytics (T	hreat Grid) - SecureX Integratio	on
Cisco Secure Malware Analytics A	opliance (Threat Grid Appliance)
Cisco Secure Malware Analytics C	oud (Threat Grid Cloud)	

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 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

Live Support Session

If you require support from a Secure Malware Analytics engineer, they may ask you to start a live support session that gives Secure Malware Analytics support engineers remote access to the appliance. Normal operations of the appliance will not be affected. You can start a live support session from the **Live Support Session** page.



Note

You can also enable support mode from the Admin TUI, and when booting up in Recovery Mode (see Resetting the Administrator Password for instructions).

Support Servers

Establishing a live support session requires that the appliance be able to reach the following servers:

- support-snapshots.threatgrid.com This allows you to directly upload a support snapshot for support, without the need to give Cisco support staff direct access to your appliance or to download the files and then upload/attach it to the support ticket.
- rash.threatgrid.com This support mode allows Cisco support staff to log in and inspect the appliance directly.

Both servers should be allowed by the firewall during an active support session.

Starting a Live Support Session

You can start a live support session from the Live Support Session page.

Step 1 Click the **Support** tab and choose **Live Support Session**.

4

Figure 4: Live Support Session

Malware Analytics	Appliance Home Configuration Documentation Status Operations Support 🛛 🕹 the SECURE
Support Ession Live Support Session Support Snapshots Execute Command	Live Support Session A support session can be created to facilitate secure remote access to your appliance from a support engineer. Support mode is not running. Start Support Session No previous support logs found
© 2021 Cisco Syst	ems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

- **Step 2** Click **Start Support Session** and follow the prompts.
- Step 3 To end the session, click Terminate Support Session.

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.



Snapshots taken before the v2.11 update may no longer have their content available to view or submit.

Step 1 To take a snapshot, click the **Support** tab and choose **Support Snapshots**.

Figure 5: Support Snapshots

Support	Snapsho	ts									
upport Snapshots											
xecute Command	be download	and the second second	rded to a support engin	neer.							
	Actio	n	ID			Time		Size	State	ıs	Actions
		e Snapshot	6BA41A8E-23ED-49	A7-8BEA-8CAB2026	8427	2022-02-02 1	7:21:11	13.7 MB	Suco	ess	
	Creat										

- **Step 2** Click **Create Snapshot**. The snapshot is taken and added to the page.
- **Step 3** Once you take the snapshot, you can view job details, download it as a **.tar** file, or click **Submit**, to automatically upload the snapshot to the Secure Malware Analytics snapshot server.

To remove a snapshot, click Delete.

Use Snapshots to Verify Backups

You can also use snapshots to test and verify that your backups are good. Take a snapshot of the backup store in your Production appliance or cluster, creating a new writable volume off of it, and then try to restore a non-production appliance or cluster from that snapshot.