

Introduction

Welcome to the *Cisco Secure Malware Analytics Appliance Administration Guide*. This chapter provides a brief description of the appliance, the intended audience and how to access relevant product documentation.

- About the Secure Malware Analytics Appliance, on page 1
- What's New In This Release, on page 2
- Audience, on page 2
- About This Guide, on page 2
- User Documentation, on page 3
- Login Names and Passwords (Default), on page 7
- Resetting the Administrator Password, on page 8

About the Secure Malware Analytics Appliance

The 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 M6 Applicance server (v.2.19 and later) or M5 Appliance server (v2.7.2 and later). It empowers organizations operating under various compliance and Secure Malware Analytics 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.

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 are able to 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.

What's New In This Release

The following changes have been implemented in this guide in Version 2.19:

Table 1: Changes in Version 2.19

Feature or Update	Section
Update firmware	Updating Firmware with FirmwareUp
Enhanced dashboard in the Admin UI	Home
In TGSH, you can now ping via a clean and dirtly interface.	-

Audience

This guide is intended to be used by the Secure Malware Analytics 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 malware analysis tool, appliance updates, backups, and other server administration tasks.

This guide also provides information for administrators who are integrating the Secure Malware Analytics Appliance with other Cisco products and services, such as Cisco Email Security Appliance, Cisco Web Security Appliance, and Secure Endpoint Private Cloud devices.



Note

For information about Secure Malware Analytics Appliance setup and configuration, see the *Cisco Threat Grid Appliance Getting Started Guide*.

About This Guide

This guide provides planning information, configuration tasks, and general administrative tasks, and is organized as follows:

Chapter	Description
Introduction	Provides brief description of the appliance, the intended audience, how to access relevant product documentation, log in names and passwords, how to reset the administrator password, and contacting Support.
Planning	Describes the environmental, hardware, and network requirements that should be reviewed prior to setup and configuration.
Network Configuration Using the TGSH Dialog	Provides information about using the Admin TUI to make changes to your initial network configuration, reconnecting to the Admin TUI, and configuring the network in recovery mode.

Chapter	Description
Home	Provides information about using the Home screen of the Admin UI.
Configuration	Provides information about using the Admin UI to make configuration changes to your appliance.
Status	Provides information about viewing system information in the Admin UI, such as installed system packages and their version, detailed logs, and available storage.
Operations	Provides information about activating configuration changes, reloading the Admin UI, managing jobs and power settings, and installing updates.
Support	Provides instructions for starting a live support session and taking support snapshots to aid in resolving issues with the appliance.
Organizations and Users	Provides instructions for creating organizations, managing users, and activating a new device user account.
Inbound and Outbound Connections	Provides information about connecting other Cisco appliances (ESA and WSA), and Secure Endpoint Private Cloud to the Secure Malware Analytics Appliance.
Removing All Data with the Wipe Appliance Boot Option	Describes how to use the Wipe Appliance boot option to remove all data from the Secure Malware Analytics Appliance, including clusters.
Updating Firmware with FirmwareUp	Describes how to update firmware.
CIMC Configuration	Provides information about using the CIMC utility to set up remote server management.

User Documentation

Secure Malware Analytics Appliance User Guides

The latest versions of Cisco Secure Malware Analytics Appliance product documentation can be found on Cisco.com.

Figure 1: User Guides on Cisco.com

	rt / Security /			
Cisco Sec	ure Malware Analytics	(Threat Grid)		
Overview Product Type Status Series Release Date	Product Overview Advanced Malware Protection (AMP) Available Order 05-JAN-2015			
			Contact Cisco 🗸 🌐 Othe	r Languages
Supported Models:	Cisco Secure Malware Analytics Threat Grid	5004 Appliance and Threat Grid 5504 Appliance		
Documentation	Downloads Community			
Search This Prod	uct's Documentation			
Customers Also V	Saved Content			
Customers Also V	Viewed Saved Content	le Version 2.19 Configuration		
Customers Also V Cisco Secure Malv		le Version 2.19 Configuration		

- Cisco Secure Malware Analytics Appliance Release Notes
- Cisco Secure Malware Analytics Appliance Getting Started Guide
- Cisco Secure Malware Analytics Version Lookup Table
- Cisco Secure Malware Analytics M6 Hardware Installation Guide



Note

The Cisco Secure Malware Analytics M6 Appliance is supported in appliance version 2.19 and later.

• Cisco Secure Malware Analytics M5 Hardware Installation Guide



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

Secure Malware Analytics Portal UI Online Help

Secure Malware Analytics Portal user documentation, including Release Notes, Using Secure Malware Analytics Online Help, API documentation, and other information is available from the ? (**Help**) icon located in the navigation bar in the upper right corner of the Secure Malware Analytics user interface.

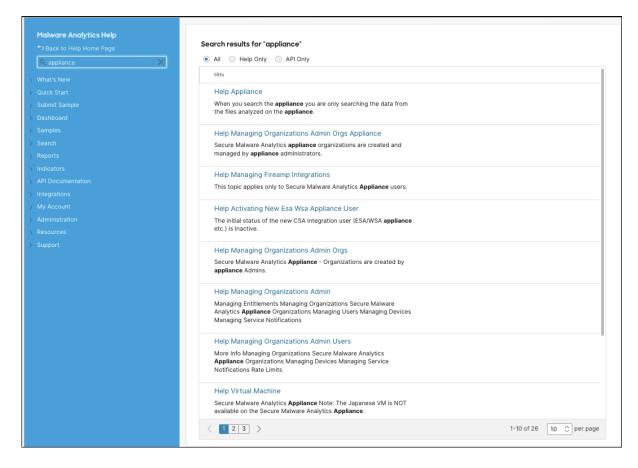
I

Figure 2: Secure Malware Analytics Portal Online Help

1alware Analytics Help	Welcome to Secure Malware Analytics!	
ウBack to Help Home Page	-	
Q Search	Cisco Secure Malware Analytics is a malware analysis and threat intelligence platform. Secure Malware Analytics generates and gathers vast amounts of malware intelligence through static and dynamic runtime sample analysis, as well as from other Cisco integrations. We use that intelligence to maintain libraries of advanced behavioral threat indicators, which we combine with traditional research methods to discover new malware and new behaviors in known malware. Our discoveries are then folded back into our ecosystem, in a continuous process of enrichment	
Quick Start	makere and the behaviors in how makere. Our discoveries are then holed back into our ecosystem, in a continuous process of emotiment of our threat intelligence resources.	
Submit Sample		
Dashboard	New to Secure Malware Analytics?	
Samples	If you're a new Secure Malware Analytics user, the quickest way to get up-to-speed is to watch this 15-minute video introduction, which walks you through the interface features and the primary functions:	
Search	Secure Malware Analytics Introduction	
Reports		
ndicators	Quick Start	
API Documentation	 Introduction to Secure Malware Analytics - Secure Malware Analytics Online Help introduction. 	
ntegrations	Getting Started - Basic information about browsers and more. About the Dashboard - Basic information about the dashboard.	
/ly Account	 Sample File Types - Detailed list of sample file types that can be submitted for analysis, plus additional information. 	
Administration	 Working with Samples - Basic information about viewing samples in Secure Malware Analytics. 	
Resources	 Submit a Sample for Analysis - Step-by-step instructions on how to submit a sample to Secure Malware Analytics for analysis. Sample Analysis Papert 	
support	Sample Analysis Report Search for Samples Doc Search - How to search the online help and API documentation. FAQ - Frequently Asked Questions. If you can't find the answers you need, please let us know! Glossary - Secure Malware Analytics definitions. Support - See Support for instructions on how to request Secure Malware Analytics support.	
	Note: The screenshots presented in the Help topics may not always reflect the latest product names or UI enhancements.	
	Quick Start Videos	
	Secure Malware Analytics Videos Secure Malware Analytics Demo, July 2018	
	What's New	
	The following documentation will help you stay current with changes to Secure Malware Analytics, as well as help you to use this powerful tool for improved threat detection, investigation, and remediation.	
	Release Notes What's New	
	About	
	Behavioral Indicators	
	Entitlements	
	Feeds	

Use the online help Search feature located at the top of the left column to find appliance-specific information.

Figure 3: Online Help Search Feature



Secure Malware Analytics Portal UI Administration Guide

A portal online help topic is available for administrators, with instructions on how to manage users and other information. Click the **Administration** tab and choose **Administration Guide**.

Malware Analytics Help	Administrator's Guide - Managing Organizations
Back to Help Home Page	Note: You must be logged in as an Admin user to create an Organization.
Q appliance	Note, fou must be logged in as an Admin user to create an organization.
> What's New	Creating New Secure Malware Analytics Organizations
> Quick Start	• Secure Malware Analytics Cloud Organizations - These are created by the Secure Malware Analytics Provisioning team and customer
> Submit Sample	teams as part of the overall process of onboarding new customers. We do not provide documentation in the portal online help on how to create a new organization.
> Dashboard	Secure Malware Analytics Appliance - Organizations are created by appliance Admins. See Secure Malware Analytics Appliance
> Samples	Organizations for information about appliance organizations.
> Search	Updating an Organization
> Reports	Admins and OrgAdmins can both update an organization once it's been created.
> Indicators	1. To update an organization, click the Administration tab and choose Organizations to open the Organizations page.
> API Documentation	 Locate the organization you need to update, and click on its name to open the Details page. Edit the organization information as needed.
> Integrations	 Details - Including the organization Name, Industry type, and ATS (Advanced Threat Services) Id
> My Account	API Rate Limit - Update the API rate limit or add new rules. All org users are covered by the org limit unless different rate limits are
 Administration 	set at the user level. See Rate Limits for more information. • Options:
Managing Organizations	 Default UI Submission Privacy - Specify whether samples are submitted as Private or Public by default.
Devices	Extended Runtimes - Enable extended runtimes.
Managing Service Notifications	Can Flag Entities - Specify whether org users can use flags. When Unset, org users can view entity flags but are unable to edit
> Managing Users	flags or add new ones.
Managing Groups Managing Entitlements	 Enable ES Pass Through For Submissions - Enable access to the following Elastic Search endpoints: /api/es/* and /api/submission-es/*.
> Resources	API Default VM - Specify the organization's default VM for API sample submissions. Other options may be selected during
> Support	sample submission.
	 Organization Class - Choose an account type that is used for accounting purposes.
	 Authorized Networks - Limits access to this organization to IPs within one or more CIDR[*] networks. Click the edit button to enter the CIDR networks.
	[*] CIDR - Classless Inter-Domain Routing (CIDR) is a range of IP addresses a network uses. A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. The number after the slash represents the number of addresses in the range. For example: 11.10/24, 2.2.2.0/24
	 Max Device Entitlement Samples - The maximum number of samples that can be submitted by device entitlements. If not set the default is 200.
	 Max Entitlement Samples - The maximum number of samples that can be submitted by entitlements. If not set the default is 10,000.
	Service Notice Emails - Org admins may add emails addresses that will receive Service Notifications. (such as an outage or

Figure 4: Administration Guide for the Secure Malware Analytics Portal UI

Email Security Appliance and Web Security Appliance Documentation

For information on connecting an Email Security Appliance (ESA) or Web Security Appliance (WSA), see Integrations.

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

Login Names and Passwords (Default)

The default login names and passwords are listed in the following table:

User	Login/Password
Admin UI and Shell User	 Use the initial Secure Malware Analytics/Admin TUI randomly generated password, and then the new password entered during the first step of the Admin UI configuration workflow. If you lose the password, follow the instructions in Resetting the Administrator Password.
Secure Malware Analytics Web portal UI Administrator	Login: admin Password: Initialize with the first Admin UI password, and then it becomes independent.
CIMC	Login: admin Password: password

Password Criteria

Passwords must include the following:

- Minimum of 8 characters
- At least one number
- · At least one special character
- Uppercase and lowercase characters

Resetting the Administrator Password

The default administrator password is only visible in the Admin TUI during the initial appliance setup and configuration. Once the initial configuration is completed, the password is no longer displayed in visible text.



Note LDAP authentication is available for Admin TUI and Admin UI login when you have multiple administrators. If the appliance is configured for LDAP authentication only, resetting the password in recovery mode will reconfigure the authentication mode to allow login with system password as well.

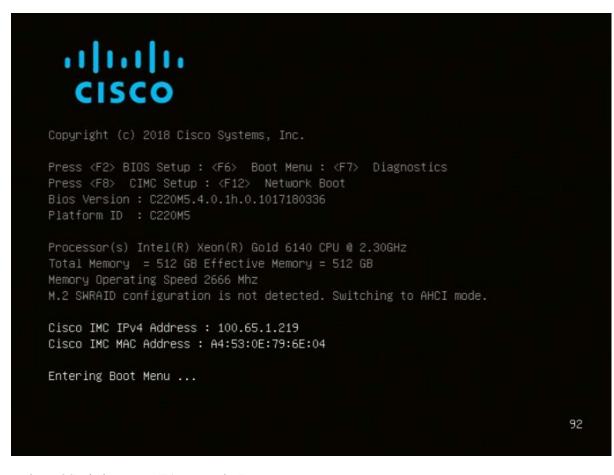
If you lose the administrator password and are unable to log in to the Admin UI, complete the following steps to reset the password.

Procedure

Step 1 Reboot the Secure Malware Analytics Appliance: click the **Operations** tab and choose **Power**, and then click the **Reboot** button. The appliance reboots, and opens the BIOS window.

L





- **Step 2** In the BIOS window, press **F6** to open the **Boot** menu.
- **Step 3** Choose **Recovery** and press **Enter**.

Figure 6: Boot Menu

Please select boot device:
Appliance Recovery UEFI: Built-in EFI Shell FirmwareUp UEFI: PXE IP4 Intel(R) Ethernet Controller X550 UEFI: PXE IP4 Intel(R) Ethernet Controller X550 Enter Setup
↑ and ↓ to move selection ENTER to select boot device ESC to boot using defaults

The Secure Malware Analytics Shell opens in Recovery Mode.

Figure 7: Secure Malware Analytics Shell (tgsh) in Recovery Mode

<pre>dmg metuberk comrigeration changes will be applied but to the remning recodery instance and to the real (non-recovery) system, and tysh will be inmediately restarted. [29.363085] configure-from-target[1352]: net.ipv4.tcp_sack = 1 [0K] Started OpenSSH Daemon.</pre>
<pre>[29.363085] configure-from-target[1352]: net.ipv4.tcp_sack = 1</pre>
[DK] Started OnenSNI Baenon
YOU MUST EXIT TGSH BEFORE NETWORK CONFIGURATION CHANGES TAKE EFFECT.
AND NO TO THE REAL DESIGNAT CHARGE FROM SELLE AND TO DEAL DRIVE CURREN
FAILING TO DO SO MAY PREVENT SUPPORT STAFF FROM BEING ABLE TO REACH YOUR SYSTEM.
[29,454605] configure=from-target[1352]: net, jpv4.tcp_window_scaling = 1 [08] Besched target Threat081B Recovery Mode.
bloom i neatha target incatoni neoberg nae.
For help, type "help" then enter.
[29] Slofill configure-from-target[1352]: net.ipv4.tcp_keepalive_intv1 = 30
> [25,56625] configure-from-target(152): net.ipu/.top.tureuse = 1
[29,570452] configure-from-target(1552): net.core.unen_default = 8388668
[29,590340] configure-from-target[1352]; met.core.rmem.default = 0300600
[29.662073] configure-from-target[1352]; net.core.umen.max = 8388608
[29.613473] configure-from-target[1352]: net.core.rmem.nax = 8388608
<pre>[29.624361] configure-from-target[1352]: net.core.netdev_max_backlog = 10000</pre>
<pre>[29.635073] configure-from-target[1352]: un.swappiness = 0</pre>
[29.645657] configure-from-target[1352]: kernel.shnmax = 77309411328
[29.656570] configure-from-target[1352]: kernel.shnall = 18874368
[29.667725] sshd[1493]; Server listening on 0.0.0.0 port 22.
[29.680578] sshd[1493]: Server listening on :: port 22.
[29.692276] su[1495]: (to threatgrid) root on console
[29.702728] su[1495]: pam_unix(su-1:session): session opened for user threatgrid by (uid=0)
[29.713268] systemd[1]: Started Initialize From Target.
[29.723599] systemd(1): Starting_Rescue_Shell
1 29.7336661 system(11: Started Rescue Shell.
1 29.743723 system(11): Starting ThreatGRID Support Mode Worker
1 29.753233 system(11): Starting OpenSNI Daenon
29.762993 system(11): Started OpenSSH Daenon.
[29,772456] system(11): Starting ThreatGRID Recovery Mode. (29,761763) system(11): Reached target ThreatGRID Recovery Mode.
22.70103 aystematii: reacrea target incatation recovery hour.
1 23.0301651 system(11): Startup finished in 5.581s (kernel) + 23.948s (userspace) = 29.530s.
1 23.0001031 agitemetri startup imismo in 3.5015 (kernel/v 23.506 (keerspace) - 23.506).
23.059559 com gare row target issues and index in a comparison from target
30.8275161 rash-worker (1501): - rash-worker.go:55: connected to router "ThreatGRID" at rash.threatgrid.com:19791

Step 4 Run passwd to change the password.

Figure 8: Enter New Password

D) passud [286.653257] sudo[1511]: threatgrid : TTY=ttyl : PWD=/home/threatgrid : USER=root : COMMAND=/usr/bin/passud threatgrid Enter new UNIX password: [206.663606] sudo[1511]: pan_unix(sudo:session): session opened for user root by (uid=0)

Note

The command prompt is not always visible in this mode and logging output may be displayed at any point on top of your input. This does not affect input; you can keep typing blindly. Ignore the two lines of logging output.

- **Step 5** Enter (blindly) the password and press **Enter**.
- **Step 6** Re-type the password and press **Enter**.

Note

The password will not be displayed.

Step 7 Type **reboot** and press **Enter** to start the appliance in normal mode.

Note

The exit command is no longer required before rebooting for a password reset to take effect (for v2.10 and later).

I