



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 Appliance 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 TGSN, you can now ping via a clean and dirty 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 TGSN 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.

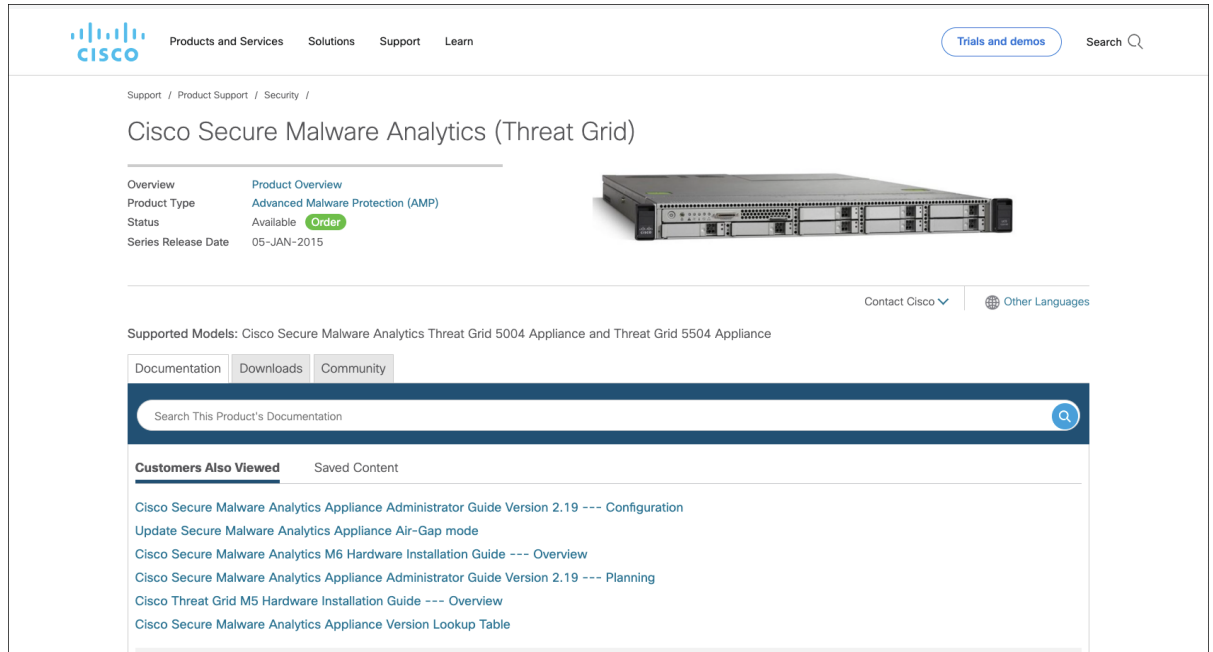
Chapter	Description
Home	Provides information about using the Home screen of the Admin UI.
Configuration	Provides information about using the Admin UI to make configuration changes to your appliance.
Status	Provides information about viewing system information in the Admin UI, such as installed system 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](https://www.cisco.com).

Figure 1: User Guides on Cisco.com



- [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.

Figure 2: Secure Malware Analytics Portal Online Help

Malware Analytics Help
↔ Back to Help Home Page

🔍 Search

- > What's New
- > Quick Start
- > Submit Sample
- > Dashboard
- > Samples
- > Search
- > Reports
- > Indicators
- > API Documentation
- > Integrations
- > My Account
- > Administration
- > Resources
- > Support

Welcome to Secure Malware Analytics!

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 of our threat intelligence resources.

New to Secure Malware Analytics?

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:

- [Secure Malware Analytics Introduction](#)

Quick Start

- [Introduction to Secure Malware Analytics - Secure Malware Analytics Online Help introduction.](#)
- [Getting Started - Basic information about browsers and more.](#)
- [About the Dashboard - Basic information about the dashboard.](#)
- [Sample File Types - Detailed list of sample file types that can be submitted for analysis, plus additional information.](#)
- [Working with Samples - Basic information about viewing samples in Secure Malware Analytics.](#)
- [Submit a Sample for Analysis - Step-by-step instructions on how to submit a sample to Secure Malware Analytics for analysis.](#)
- [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

The screenshot displays the Malware Analytics Help interface. On the left is a blue navigation sidebar with the following menu items: Malware Analytics Help, Back to Help Home Page, a search bar containing 'appliance', and a list of categories: What's New, Quick Start, Submit Sample, Dashboard, Samples, Search, Reports, Indicators, API Documentation, Integrations, My Account, Administration, Resources, and Support. The main content area shows search results for 'appliance' with filters for All (selected), Help Only, and API Only. The results list includes:

- Help Appliance**: When you search the **appliance** you are only searching the data from the files analyzed on the **appliance**.
- Help Managing Organizations Admin Orgs Appliance**: Secure Malware Analytics **appliance** organizations are created and managed by **appliance** administrators.
- Help Managing Fireamp Integrations**: This topic applies only to Secure Malware Analytics **Appliance** users.
- Help Activating New Esa Wsa Appliance User**: The initial status of the new CSA integration user (ESA/WSA **appliance** etc.) is Inactive.
- Help Managing Organizations Admin Orgs**: Secure Malware Analytics **Appliance** - Organizations are created by **appliance** Admins.
- Help Managing Organizations Admin**: Managing Entitlements Managing Organizations Secure Malware Analytics **Appliance** Organizations Managing Users Managing Devices Managing Service Notifications
- Help Managing Organizations Admin Users**: More Info Managing Organizations Secure Malware Analytics **Appliance** Organizations Managing Devices Managing Service Notifications Rate Limits
- Help Virtual Machine**: Secure Malware Analytics **Appliance** Note: The Japanese VM is NOT available on the Secure Malware Analytics **Appliance**.

 At the bottom of the results area, there is a pagination control showing '1-10 of 26' items, with '10' items per page selected.

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**.

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

Malware Analytics Help
 → Back to Help Home Page
 Search: appliance

- What's New
- Quick Start
- Submit Sample
- Dashboard
- Samples
- Search
- Reports
- Indicators
- API Documentation
- Integrations
- My Account
- Administration
 - Managing Organizations
 - Devices
 - Managing Service Notifications
 - Managing Users
 - Managing Groups
 - Managing Entitlements
 - Resources
 - Support

Administrator's Guide - Managing Organizations

Note: You must be logged in as an **Admin** user to create an Organization.

Creating New Secure Malware Analytics Organizations

- Secure Malware Analytics Cloud Organizations** - These are created by the Secure Malware Analytics Provisioning team and customer 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.
- Secure Malware Analytics Appliance** - Organizations are created by appliance Admins. See [Secure Malware Analytics Appliance Organizations](#) for information about appliance organizations.

Updating an Organization

Admins and OrgAdmins can both update an organization once it's been created.

- To update an organization, click the **Administration** tab and choose **Organizations** to open the **Organizations** page.
- Locate the organization you need to update, and click on its name to open the **Details** page.
- Edit the organization information as needed.
 - Details** - Including the organization Name, Industry type, and ATS (Advanced Threat Services) Id
 - 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 set at the user level. See [Rate Limits](#) for more information.
 - Options:**
 - Default UI Submission Privacy** - Specify whether samples are submitted as Private or Public by default.
 - Extended Runtimes** - Enable extended runtimes.
 - Can Flag Entities** - Specify whether org users can use flags. When Unset, org users can view entity flags but are unable to edit flags or add new ones.
 - Enable ES Pass Through For Submissions** - Enable access to the following Elastic Search endpoints: `/api/es/*` and `/api/submission-es/*`.
 - API Default VM** - Specify the organization's default VM for API sample submissions. Other options may be selected during 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: 1.1.1.0/24, 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

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 Email Security Appliance User Guide](#)
- [Cisco Web Security 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.

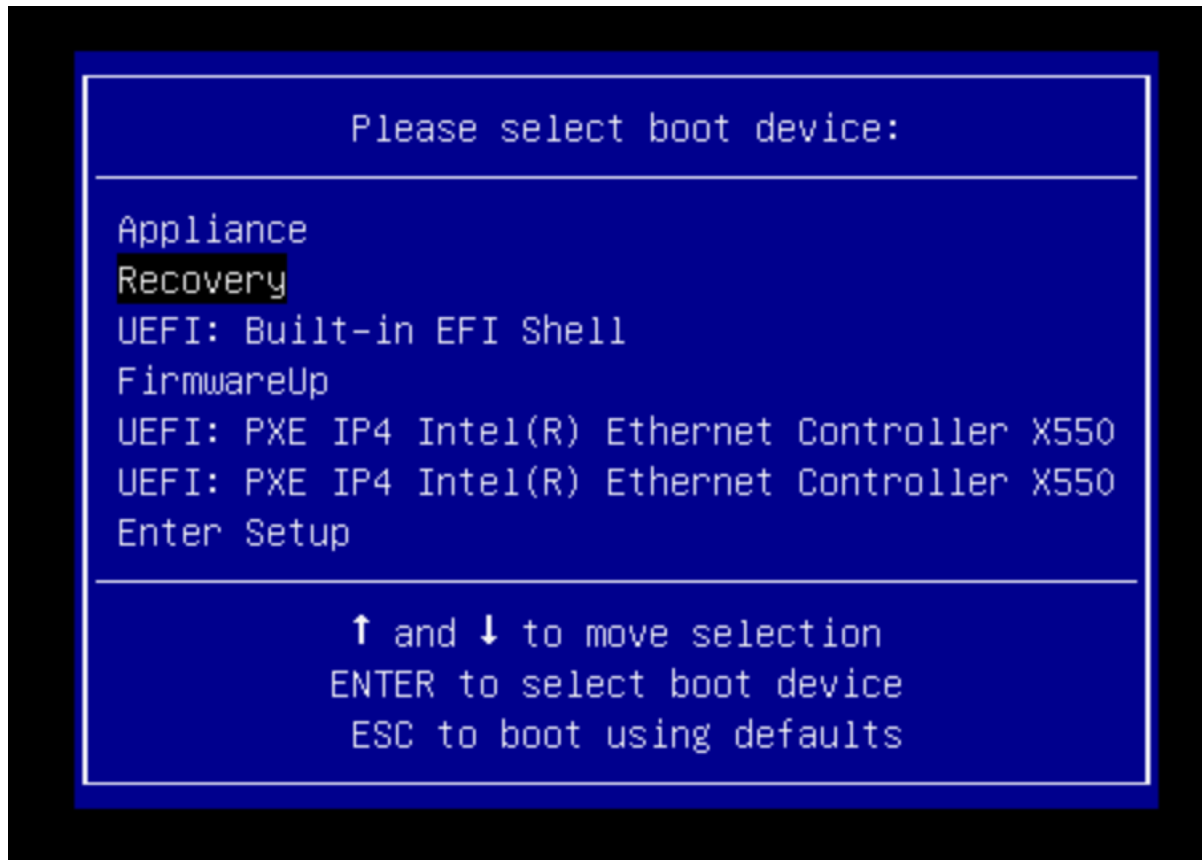
Figure 5: BIOS Window - Choose Boot Menu <F6> for Recovery Mode



Step 2 In the BIOS window, press **F6** to open the **Boot** menu.

Step 3 Choose **Recovery** and press **Enter**.

Figure 6: Boot Menu



The Secure Malware Analytics Shell opens in Recovery Mode.

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

```

any network configuration changes will be applied both to the existing recovery
instance and to the real (non-recovery) system, and tgsh will be immediately
restarted.
( 29.363065) configure-from-target[1352]: net.ipv4.tcp_sack = 1
( OK ) Started OpenSSH Daemon.
YOU MUST EXIT TGSH BEFORE NETWORK CONFIGURATION CHANGES TAKE EFFECT.

FAILING TO DO SO MAY PREVENT SUPPORT STAFF FROM BEING ABLE TO REACH YOUR SYSTEM.
( 29.454665) configure-from-target[1352]: net.ipv4.tcp_window_scaling = 1
( OK ) Reached target ThreatGRID Recovery Mode.
Welcome to the ThreatGrid Shell.
For help, type "help" then enter.
( 29.516718) configure-from-target[1352]: net.ipv4.tcp_keepalive_intol = 30
o> ( 29.566235) configure-from-target[1352]: net.ipv4.tcp_tw_reuse = 1
( 29.578452) configure-from-target[1352]: net.core.umem_default = 8388668
( 29.598348) configure-from-target[1352]: net.core.rmem_default = 8388668
( 29.602073) configure-from-target[1352]: net.core.umem_max = 8388668
( 29.613473) configure-from-target[1352]: net.core.rmem_max = 8388668
( 29.624361) configure-from-target[1352]: net.core.netdev_max_backlog = 10000
( 29.635073) configure-from-target[1352]: vm.swappiness = 0
( 29.645657) configure-from-target[1352]: kernel.shmmax = 77309411328
( 29.656570) configure-from-target[1352]: kernel.shmall = 18874368
( 29.667725) sshd[1493]: Server listening on 0.0.0.0 port 22.
( 29.688578) sshd[1493]: Server listening on :: port 22.
( 29.692276) su[1495]: (to threatgrid) root on console
( 29.702728) su[1495]: pam_unix(su-l:session): session opened for user threatgrid by (uid=0)
( 29.713268) systemd[1]: Started Initialize From Target.
( 29.723591) systemd[1]: Starting Rescue Shell...
( 29.733666) systemd[1]: Started Rescue Shell.
( 29.743472) systemd[1]: Starting ThreatGRID Support Mode Worker...
( 29.753293) systemd[1]: Starting OpenSSH Daemon...
( 29.762931) systemd[1]: Started OpenSSH Daemon.
( 29.772456) systemd[1]: Starting ThreatGRID Recovery Mode.
( 29.781763) systemd[1]: Reached target ThreatGRID Recovery Mode.
( 29.791010) systemd[1]: Started ThreatGRID Support Mode Worker.
( 29.800165) systemd[1]: Startup finished in 5.581s (kernel) + 23.948s (userspace) = 29.530s.
( 29.809835) configure-from-target[1352]: Done with importing configuration from target
( 29.819359) rash-worker[1501]: -- rash-worker.go:42: BASH worker "FOH1832U319" ready to dial roster.
( 30.827516) 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

```

o> passwd
( 286.653257) sudo[1511]: threatgrid : TTY=ttty ; PWD=/home/threatgrid ; USER=root ; COMMAND=/usr/bin/passwd threatgrid
Enter new UNIX password: ( 286.663606) sudo[1511]: pam_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).

