Cisco Secure Malware Analytics Appliance Administrator Guide Version 2.18

First Published: 2022-09-01

Last Modified: 2023-03-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

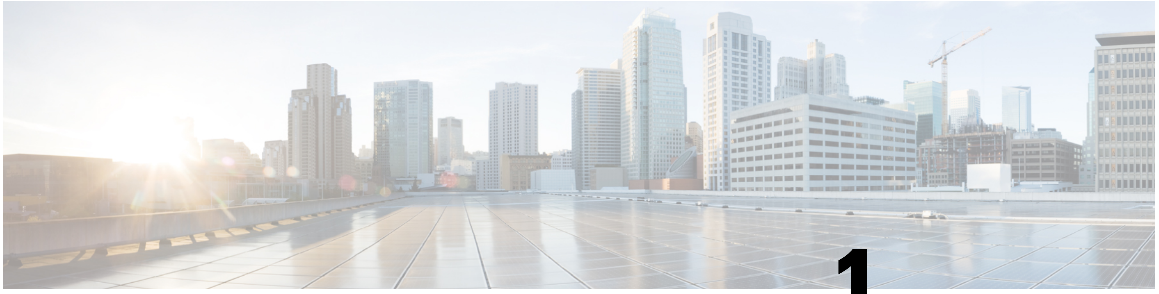
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS



CHAPTER 1

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

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 M5 Appliance server (v2.7.2 and later). It empowers organizations operating under various compliance andSecure 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 2.18:

Table 1: Changes in Version 2.18

Feature or Update	Section
Added info on the how to enable the new Content update.	Content Update, on page 57
Added more info on RADIUS Authentication section along with a note about the NAS-Identifier	RADIUS Authentication, on page 37

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 Admin TUI	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.

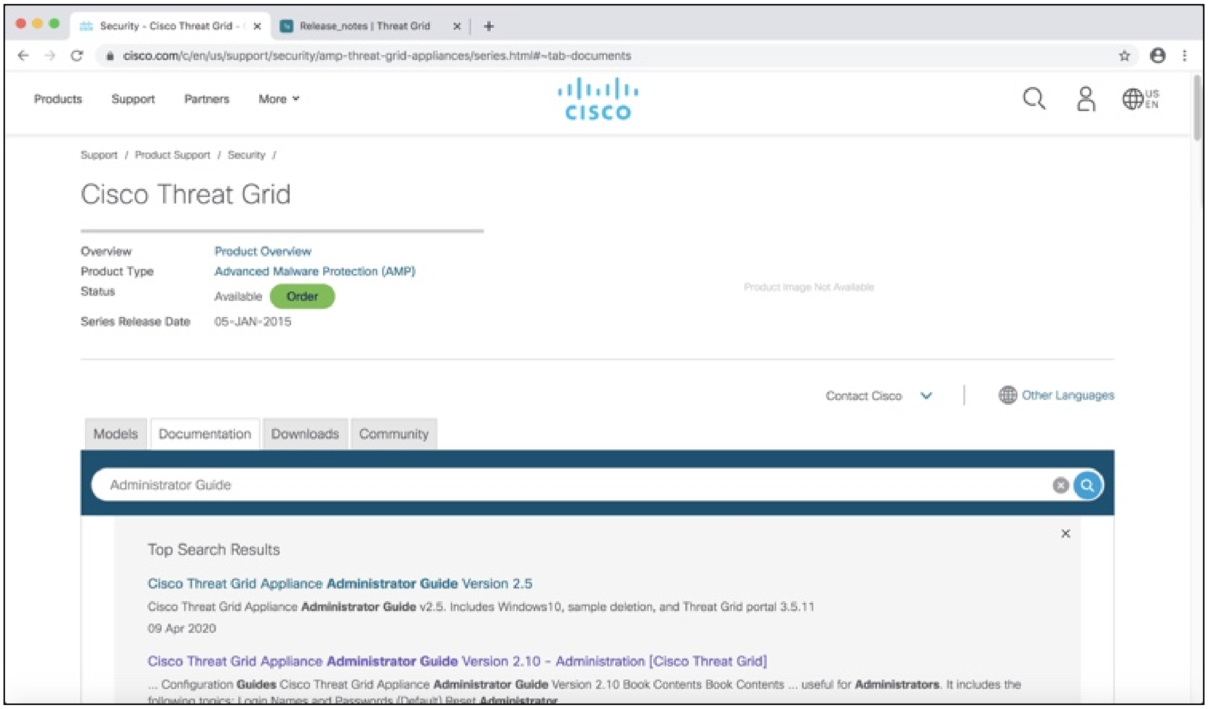
Chapter	Description
Configuration Using the Admin UI	Provides information about using the Admin UI to make configuration changes to your appliance. See About the Admin UI for a complete list of tasks that can be performed.
Status	Provides information about viewing system information in the Admin UI, 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 Operation	Describes how to use the Wipe Appliance boot option to remove all data from the Secure Malware Analytics Appliance, including clusters.
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


Security - Cisco Threat Grid
Release_notes | Threat Grid
cisco.com/c/en/us/support/security/amp-threat-grid-appliances/series.html#~tab-documents
Products
Support
Partners
More
cisco
US EN
Support / Product Support / Security /
Contact Cisco
Other Languages
Models
Documentation
Downloads
Community
Order
Product Image Not Available

Cisco Threat Grid

Overview	Product Overview
Product Type	Advanced Malware Protection (AMP)
Status	Available
Series Release Date	05-JAN-2015

Administrator Guide

Top Search Results

Cisco Threat Grid Appliance **Administrator Guide** Version 2.5

Cisco Threat Grid Appliance **Administrator Guide** v2.5. Includes Windows10, sample deletion, and Threat Grid portal 3.5.11

09 Apr 2020

Cisco Threat Grid Appliance **Administrator Guide** Version 2.10 - Administration [Cisco Threat Grid]

... Configuration **Guides** Cisco Threat Grid Appliance **Administrator Guide** Version 2.10 Book Contents Book Contents ... useful for **Administrators**. It includes the following topics: Login Names and Passwords (Default) Reset **Administrator**

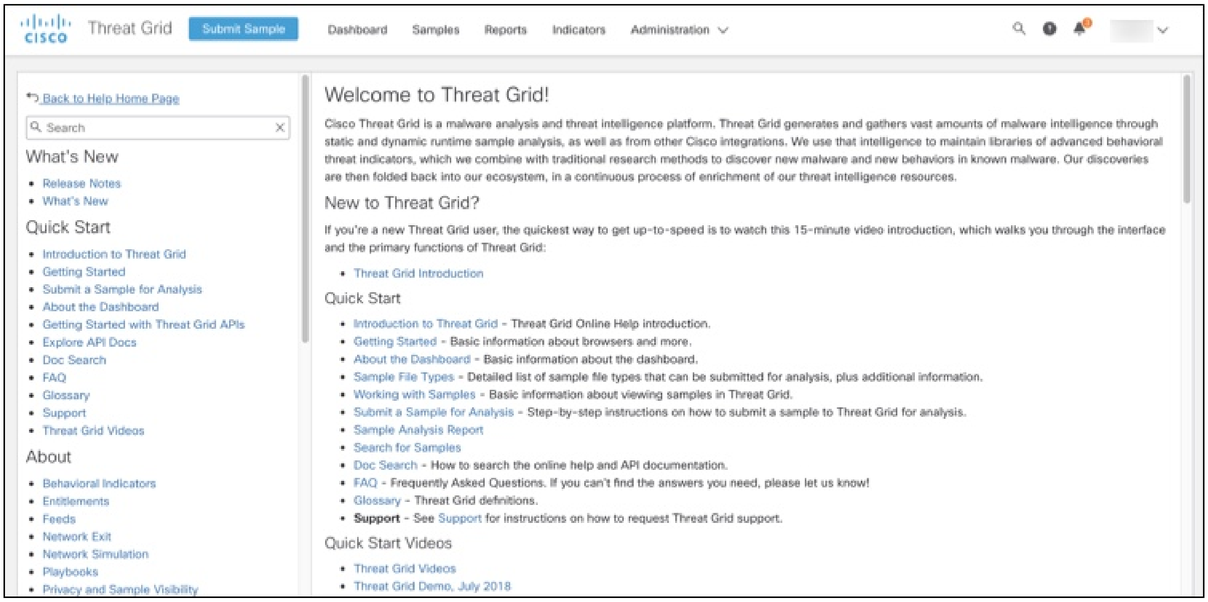
- *Cisco Secure Malware Analytics Appliance Release Notes*
- *Cisco Secure Malware Analytics Appliance Getting Started Guide*
- *Cisco Secure Malware Analytics Version Lookup Table*
- *Cisco Secure Malware Analytics M5 Hardware Installation Guide*

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



Welcome to Threat Grid!

Cisco Threat Grid is a malware analysis and threat intelligence platform. Threat Grid 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 Threat Grid?

If you're a new Threat Grid user, the quickest way to get up-to-speed is to watch this 15-minute video introduction, which walks you through the interface and the primary functions of Threat Grid:

- Threat Grid Introduction

Quick Start

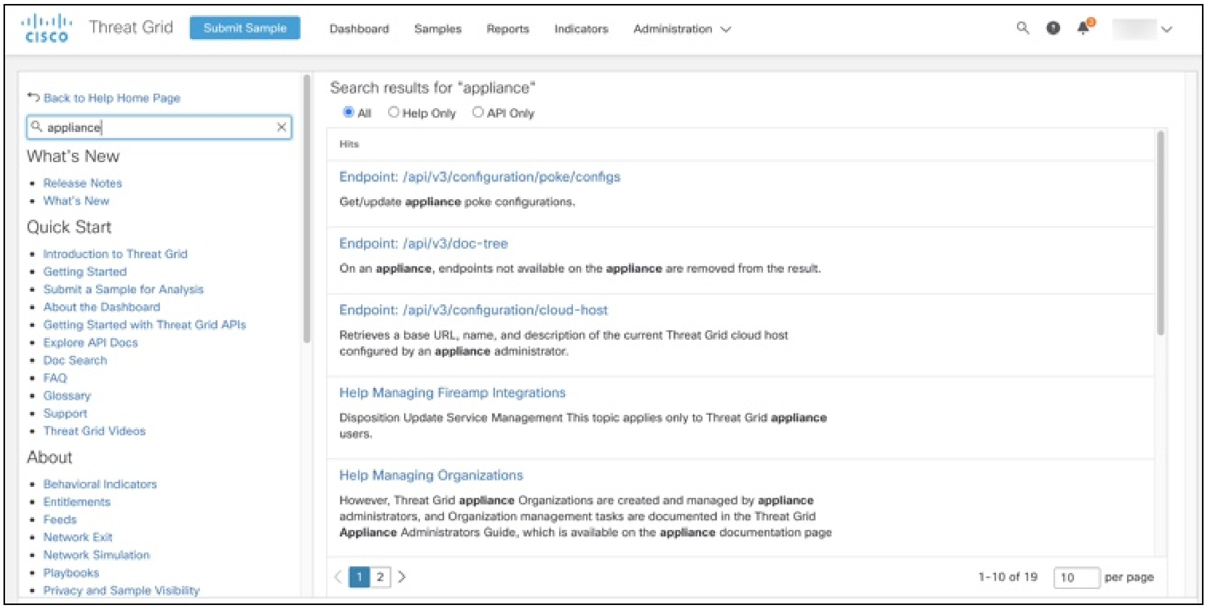
- Introduction to Threat Grid - Threat Grid Online Help introduction.
- Getting Started - Basic information about browsers and more.
- About the Dashboard - Basic information about the dashboard.
- Sample File Types - Detailed list of sample file types that can be submitted for analysis, plus additional information.
- Working with Samples - Basic information about viewing samples in Threat Grid.
- Submit a Sample for Analysis - Step-by-step instructions on how to submit a sample to Threat Grid 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 - Threat Grid definitions.
- **Support** - See Support for instructions on how to request Threat Grid support.

Quick Start Videos

- Threat Grid Videos
- Threat Grid Demo, July 2018

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



Search results for "appliance"

● All ○ Help Only ○ API Only

Hits

Endpoint: /api/v3/configuration/poke/configs

Get/update **appliance** poke configurations.

Endpoint: /api/v3/doc-tree

On an **appliance**, endpoints not available on the **appliance** are removed from the result.

Endpoint: /api/v3/configuration/cloud-host

Retrieves a base URL, name, and description of the current Threat Grid cloud host configured by an **appliance** administrator.

Help Managing Fireamp Integrations

Disposition Update Service Management This topic applies only to Threat Grid **appliance** users.

Help Managing Organizations

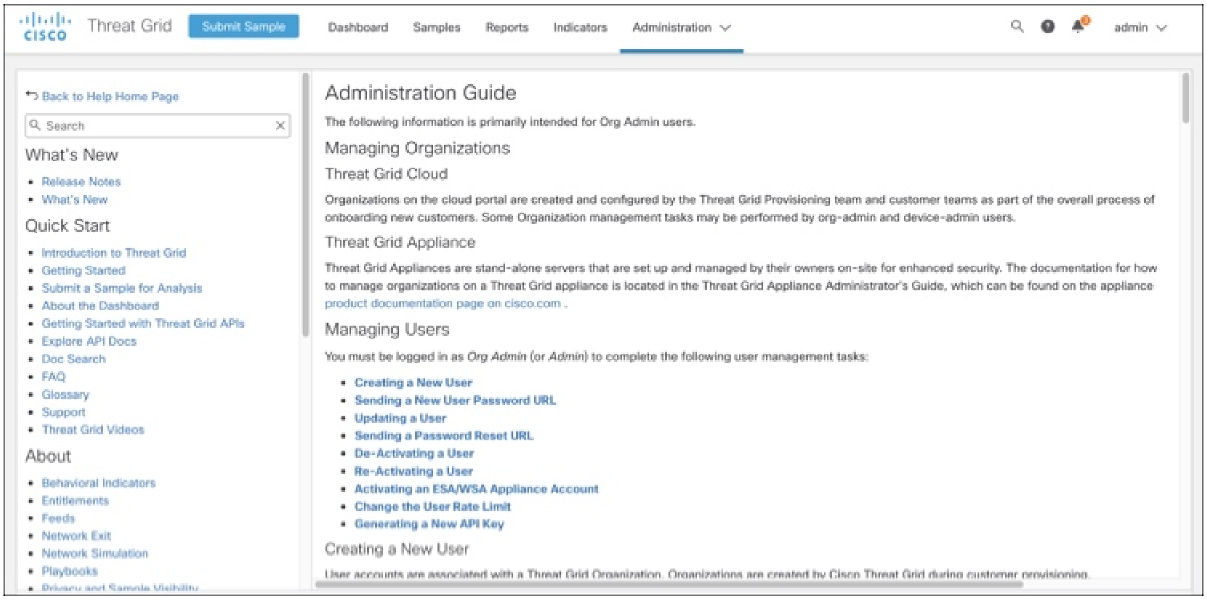
However, Threat Grid **appliance** Organizations are created and managed by **appliance** administrators, and Organization management tasks are documented in the Threat Grid **Appliance** Administrators Guide, which is available on the **appliance** documentation page

< 1 2 > 1-10 of 19 10 per page

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



Administration Guide

The following information is primarily intended for Org Admin users.

Managing Organizations

Threat Grid Cloud

Organizations on the cloud portal are created and configured by the Threat Grid Provisioning team and customer teams as part of the overall process of onboarding new customers. Some Organization management tasks may be performed by org-admin and device-admin users.

Threat Grid Appliance

Threat Grid Appliances are stand-alone servers that are set up and managed by their owners on-site for enhanced security. The documentation for how to manage organizations on a Threat Grid appliance is located in the Threat Grid Appliance Administrator's Guide, which can be found on the appliance product documentation page on cisco.com .

Managing Users

You must be logged in as *Org Admin* (or *Admin*) to complete the following user management tasks:

- Creating a New User
- Sending a New User Password URL
- Updating a User
- Sending a Password Reset URL
- De-Activating a User
- Re-Activating a User
- Activating an ESA/WSA Appliance Account
- Change the User Rate Limit
- Generating a New API Key

Creating a New User

User accounts are associated with a Threat Grid Organization. Organizations are created by Cisco Threat Grid during customer provisioning.

Email Security Appliance and Web Security Appliance Documentation

For information on connecting an Email Security Appliance (ESA) or Web Security Appliance (WSA), see Inbound and Outbound Connections.

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.

User	Login/Password
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.

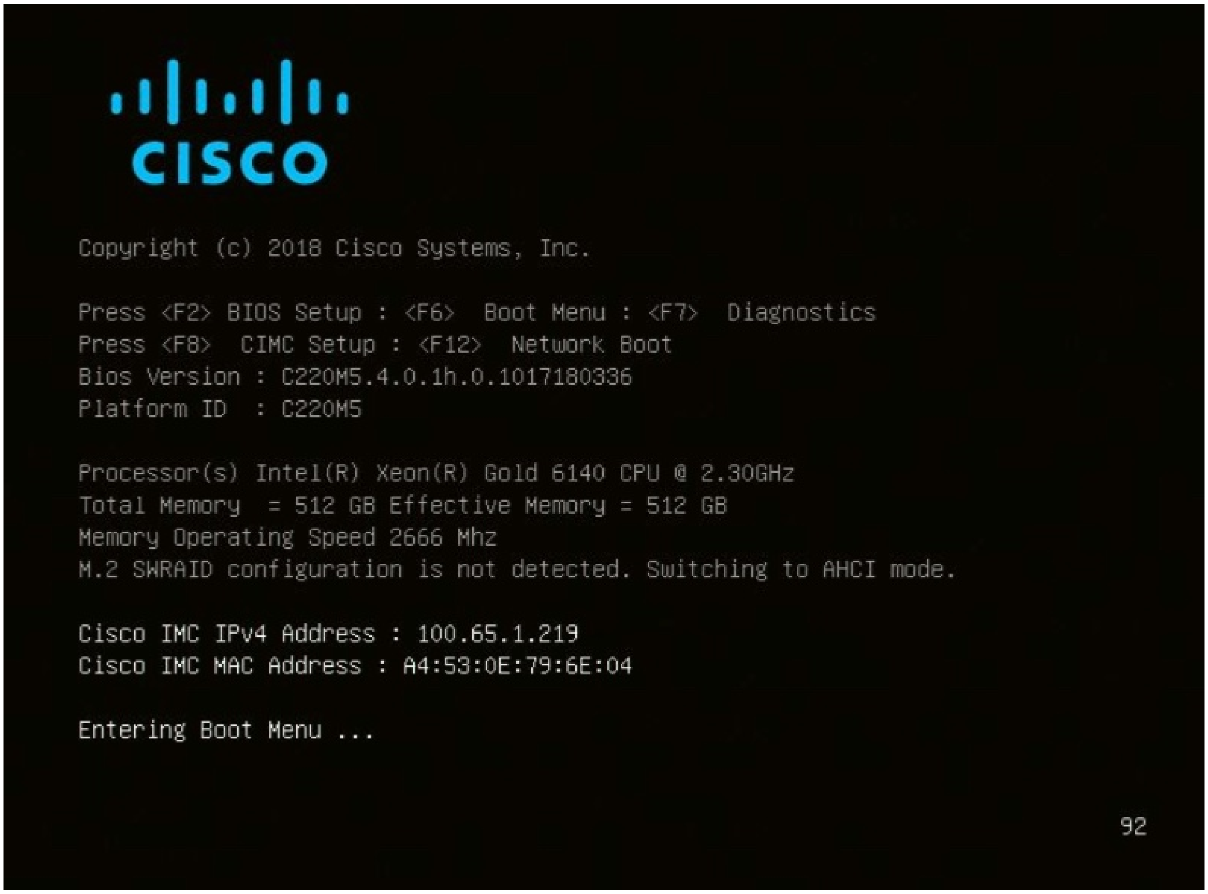
Note LDAP authentication is available for Admin TUI and Admin UI login when you have multiple administrators. If the appliance is configured for LDAP authentication only, resetting the password in recovery mode will reconfigure the authentication mode to allow login with system password as well.

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

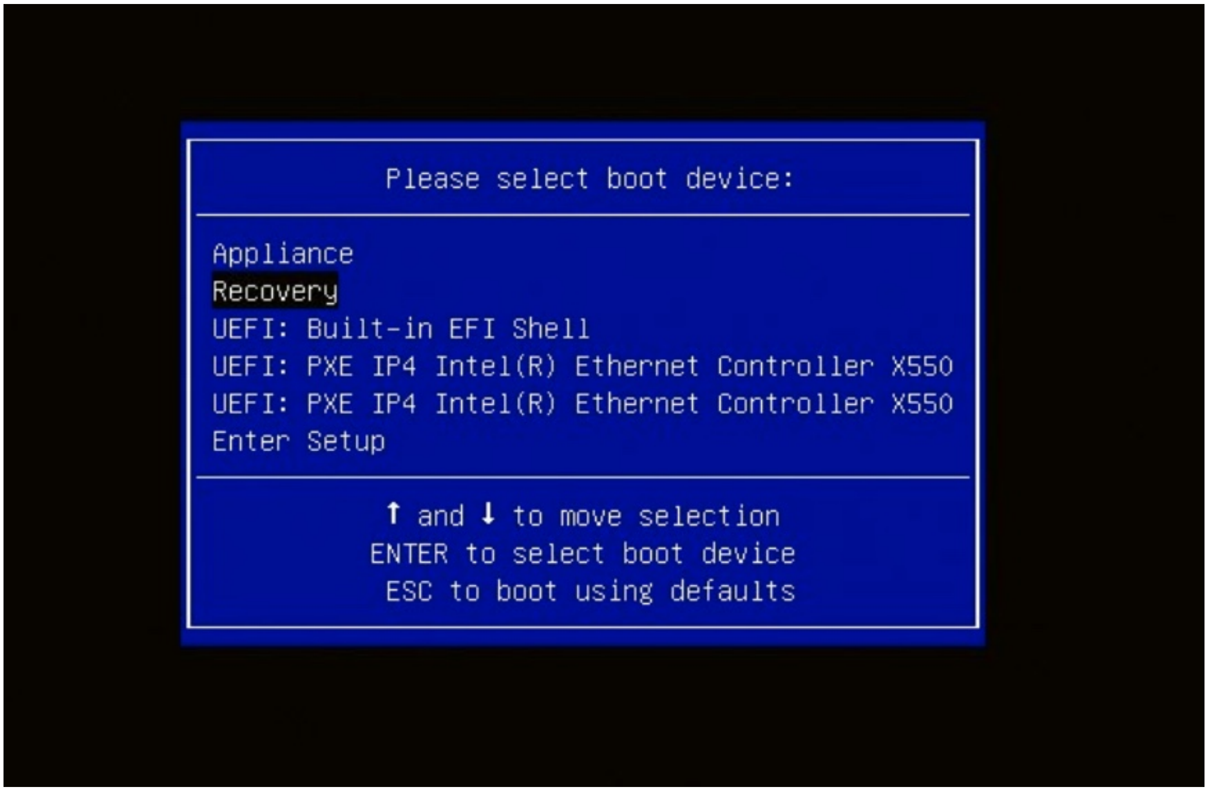


```
Copyright (c) 2018 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6>  Boot Menu : <F7>  Diagnostics
Press <F8>  CIMC Setup : <F12>  Network Boot
Bios Version : C220M5.4.0.1h.0.1017180336
Platform ID  : C220M5

Processor(s) Intel(R) Xeon(R) Gold 6140 CPU @ 2.30GHz
Total Memory  = 512 GB Effective Memory = 512 GB
Memory Operating Speed 2666 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 100.65.1.219
Cisco IMC MAC Address : A4:53:0E:79:6E:04

Entering Boot Menu ...

                                                              92
```

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

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

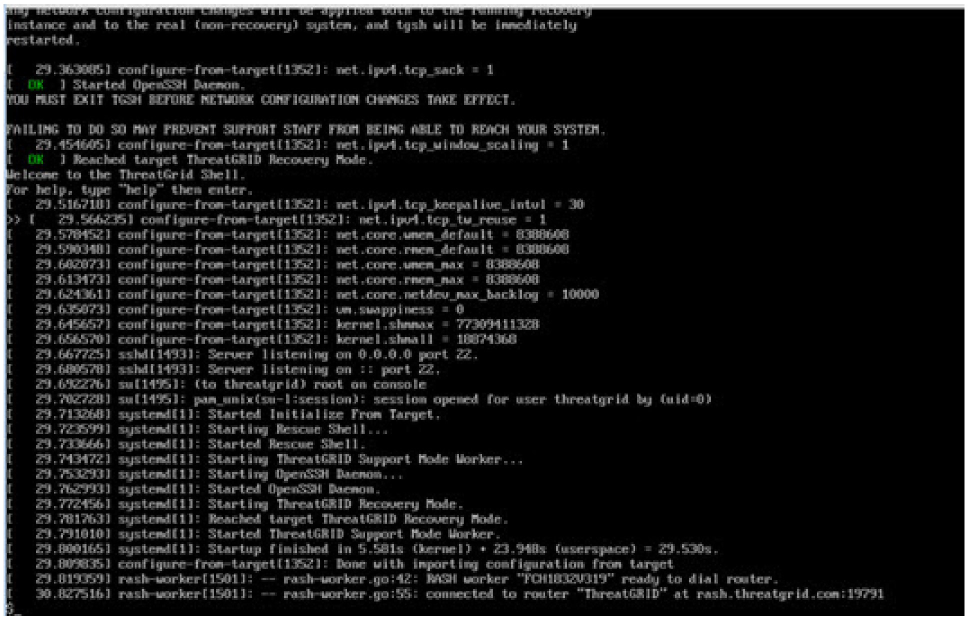
Figure 6: Boot Menu



```
Please select boot device:

Appliance
Recovery
UEFI: Built-in EFI Shell
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.

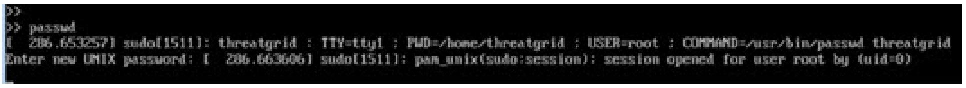
Figure 7: Secure Malware Analytics Shell (tgsh) in Recovery Mode



```
any network configuration changes will be applied both to the running recovery
instance and to the real (non-recovery) system, and tgsh will be immediately
restarted.

[   29.363085] 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.
[   29.454605] 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_intvl = 30
>> [   29.566235] configure-from-target[1352]: net.ipv4.tcp_tw_reuse = 1
[   29.578452] configure-from-target[1352]: net.core.wmem_default = 8388608
[   29.590348] configure-from-target[1352]: net.core.rmem_default = 8388608
[   29.602073] configure-from-target[1352]: net.core.wmem_max = 8388608
[   29.613473] configure-from-target[1352]: net.core.rmem_max = 8388608
[   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.
[   29.680578] 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.
[   29.723599] 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...
[   29.762993] 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: RASH worker "FCH1832V319" ready to dial router.
[   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



```
>>
>> passwd
[  286.653257] sudo[1511]: threatgrid : TTY=tty1 ; 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).

CHAPTER 2

Planning

The Cisco Secure Malware Analytics Appliance is a Linux server with Secure Malware Analytics software installed by Cisco Manufacturing prior to shipment. Once a new Secure Malware Analytics Appliance is received, it must be set up and configured for your on-premises network environment.

This chapter describes the environmental, hardware, and network requirements that should be reviewed prior to setup and configuration:

Supported Browsers

Secure Malware Analytics supports the following browsers:

- Google Chrome™
- Mozilla Firefox®
- Apple Safari®

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

Environmental Requirements

Secure Malware Analytics Appliance (v2.7.2 and later) is deployed on the Secure Malware Analytics M5 Appliance server. Before you set up and configure the Secure Malware Analytics Appliance, make sure the necessary environmental requirements for power, rack space, cooling, and other issues are met, according to the specifications in the *Cisco Threat Grid M5 Hardware Installation Guide*.

Hardware Requirements

The SFP+ form factor is used for the Admin interface. If you are clustering Secure Malware Analytics Appliances, each one will require an additional SFP+ module on the Clust interface.

Note The SFP+ modules must be connected *before* the Secure Malware Analytics Appliance is powered on for the session in which the configuration wizard is going to be run.

If there are no SFP+ ports available on the switch, or SFP+ is not desirable, then a transceiver for 1000Base-T can be used (for example, Cisco Compatible Gigabit RJ 45 Copper SFP Transceiver Module Mini -GBIC - 10/100/1000 Base-T Copper SFP Module).

Figure 9: Cisco 1000BASE-T Copper SFP (GLC-T)

You can attach a monitor to the server, or, if Cisco Integrated Management Controller (CIMC) is configured, you can use a remote KVM (on UCS C220-M3 and C220-M4 servers).

Note CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

The Cisco UCS Power Calculator is available to get a power estimate.

Network Requirements

The Secure Malware Analytics Appliance requires three networks:

- **ADMIN** - The Administrative network must be configured to perform the Secure Malware Analytics Appliance setup.
  - Admin UI Management Traffic (HTTPS)
  - SSH
  - NFSv4 (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.)
- **CLEAN** - The Clean network is used for inbound, trusted traffic to the Secure Malware Analytics Appliance (requests), and integrated appliances such as the Cisco Email Security Appliance and Web Security Appliance; integrated appliances connect to the IP address of the Clean interface.

  Note The URL for the Clean network interface will not work until the Admin UI configuration is complete.

  The following specific, restricted types of network traffic can be outbound from the Clean network:
  - Remote syslog connections
  - Email messages sent by the Secure Malware Analytics Appliance
  - Disposition Update Service connections to Secure Endpoint Private Cloud devices
  - DNS requests (related to any of the above)
  - LDAP
  - RADIUS traffic
- **DIRTY** - The Dirty network is used for outbound traffic from the Secure Malware Analytics Appliance (including malware traffic).

Note To protect your internal network assets, we recommend using a dedicated external IP address (for example, the Dirty interface) that is different from your corporate IP.

For network interface setup information, see Network Interfaces.

DNS Server Access

The DNS server needs to be accessible via the Dirty network when used for purposes other than Disposition Update Service lookups, resolving remote syslog connections, and resolving the mail server used for notifications from the Secure Malware Analytics software.

By default, DNS uses the Dirty interface. The Clean interface is used for Secure Endpoint Private Cloud integrations and other services. If the Secure Endpoint Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the Admin UI.

NTP Server Access

By default, the NTP server needs to be accessible via the Dirty network.

Starting with the 2.12 release, an appliance can be optionally configured to connect to an NTP server from the clean interface rather than the dirty interface (default). This makes it possible to use an internal NTP server.

Integrations

Additional planning is required if the Secure Malware Analytics Appliance is going to be used with other Cisco products, such as the Email Security Appliance, Web Security Appliance, or Secure Endpoint Private Cloud. See Connecting ESA or WSA to Secure Malware Analytics Appliance for more information.

DHCP Requirements

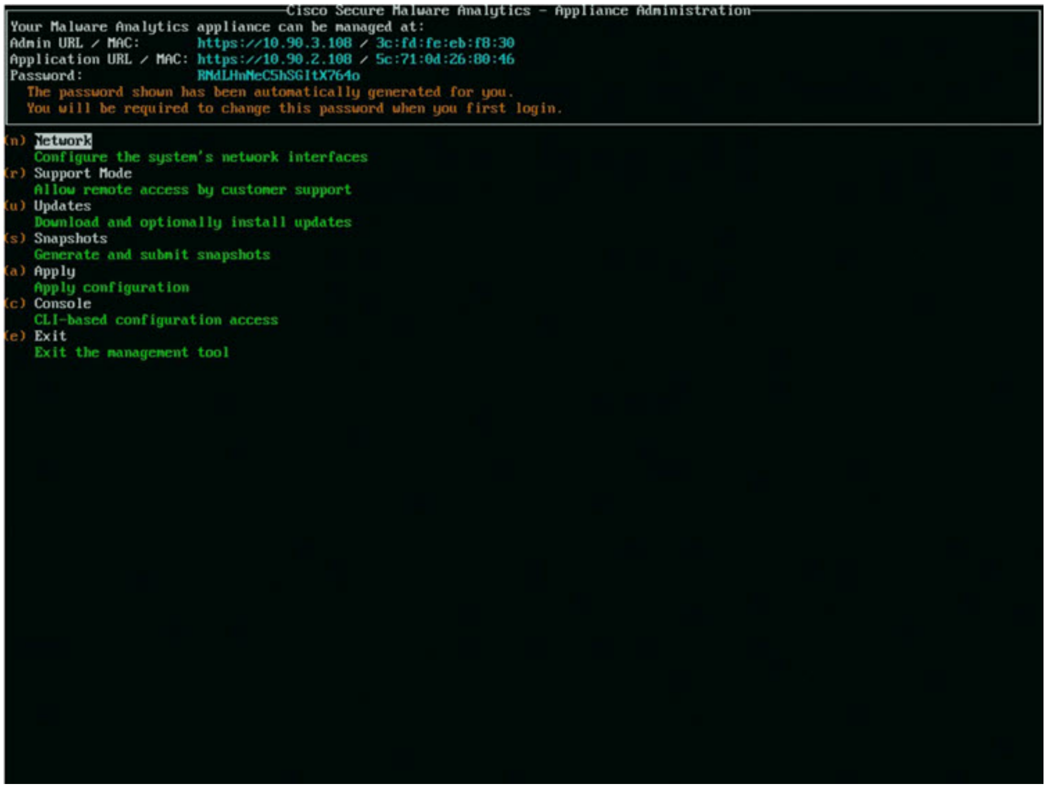
If you are connected to a network configured to use DHCP, it is important that you understand the requirements. Secure Malware Analytics Appliances that use DHCP need to explicitly specify DNS.

Warning An upgrade of a system without a DNS server explicitly specified will fail.

Note The Admin TUI displays the information you will need to access and configure the Admin UI. It may take some time for the IP addresses for DHCP to display after your appliance boots.

Open the Admin TUI (Text-mode UI) and note the following information:

Figure 10: Admin TUI (Connected to a Network Configured to Use DHCP)



```
Cisco Secure Malware Analytics - Appliance Administration
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:       https://10.90.3.108 / 3c:fd:fe:eb:f8:30
Application URL / MAC: https://10.90.2.108 / 5c:71:0d:26:80:46
Password:              RNdLHnMeC5hSGItX764o
  The password shown has been automatically generated for you.
  You will be required to change this password when you first login.

(n) Network
    Configure the system's network interfaces
(r) Support Mode
    Allow remote access by customer support
(u) Updates
    Download and optionally install updates
(s) Snapshots
    Generate and submit snapshots
(a) Apply
    Apply configuration
(c) Console
    CLI-based configuration access
(e) Exit
    Exit the management tool
```

- **Admin URL** - The Admin network. You will need this address in order to continue the remaining configuration tasks in the Admin UI.
- **Application URL** - The Clean network. This is the address to use after completing the configuration in the Admin UI.

  The Dirty network is not shown.
- **Password** - The initial Admin password that is randomly generated during the Secure Malware Analytics Appliance installation. You will need to change this password later as the first step the Admin UI configuration process.

If you need to change your initial IP assignments from DHCP to static IP addresses, see Network.

License

When a new appliance is purchased, a license is generated and the **Retrieve License From Server** button on the **Configuration** > **License** page is enabled. However, if that does not work or if there is a special case (such as a license being a custom one-off), then you will be given the license directly, as an encrypted file with a password.

For additional questions about licenses, contact Opening a Support Case.

Rate Limits

The API sample submission rate limit is global for the Secure Malware Analytics Appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions.

Rate limits are based on a window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error, plus a message about how long to wait before retrying. See the portal online Help for more information.

Organizations and Users

Once you have completed the Secure Malware Analytics Appliance setup and network configuration, you must create the initial Secure Malware Analytics organizations and add user account(s), so that people can login and begin submitting malware samples for analysis. This task may require planning and coordination among multiple organizations and users, depending on your requirements.

See Creating a New Organization and the Secure Malware Analytics portal Help (click **Administration** > **Administrator's Guide** to open the Administration Guide topic) for additional information.

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 the *Cisco Threat Grid Appliance Getting Started Guide*).

Secure Malware Analytics Appliance updates cannot be downloaded until the license is installed, and except where otherwise directed by the customer support, the update process requires that the initial appliance configuration is completed. Updates must be done in sequence.

User Interfaces

After the server has been correctly attached to the network and powered up, there are several user interfaces available for configuring the Secure Malware Analytics Appliance.

Note LDAP authentication is available for Admin TUI and the Admin UI. RADIUS authentication is available for the Secure Malware Analytics Application UI (v2.10 and later).

Admin TUI

The **Admin TUI** interface is used to configure the network interfaces. The Admin TUI is displayed when the Secure Malware Analytics Appliance successfully boots up.

Reconnecting to the Admin TUI

The Admin TUI remains open on the console and is accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

Note CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

To reconnect to the Admin TUI, ssh into the Admin IP address as the user **threatgrid**.

The required password is either the initial, randomly generated password, which is visible initially in the Admin TUI, or the new Admin password you create during the first step of the Admin UI Configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*).

Threat Grid Shell (tgsh)

The Threat Grid Shell (tgsh) is an administrator's interface that is used to execute commands (including destroy-data and forced backup), and for expert, low-level debugging. To access tgsh, choose **CONSOLE** in the Admin TUI.

Note The Admin UI uses the same credentials as the Secure Malware Analytics user, so any password changes/updates made via tgsh will also impact the Admin UI.

Caution Network configuration changes made with tgsh are not supported unless specifically directed by Secure Malware Analytics support; the Admin UI or Admin TUI should be used instead. Options to modify admin email, glovebox URL, SMTP configuration, and so on have been removed with the 2.12 release. The Wipe Appliance operation is now activated within recovery mode tgsh rather than the bootloader menu.

Admin UI

This is the primary Secure Malware Analytics user interface used for configuration. Much of the Secure Malware Analytics Appliance configuration can ONLY be done via the Admin UI, including licenses, email host, and SSL certificates.

Secure Malware Analytics Portal

The Secure Malware Analytics user interface application is available as a cloud service, and is also installed on Secure Malware Analytics Appliances. There is no communication between Secure Malware Analytics Cloud service and the Secure Malware Analytics Portal that is included with a Secure Malware Analytics Appliance.

Network Interfaces

The available network interfaces are described in the following table:

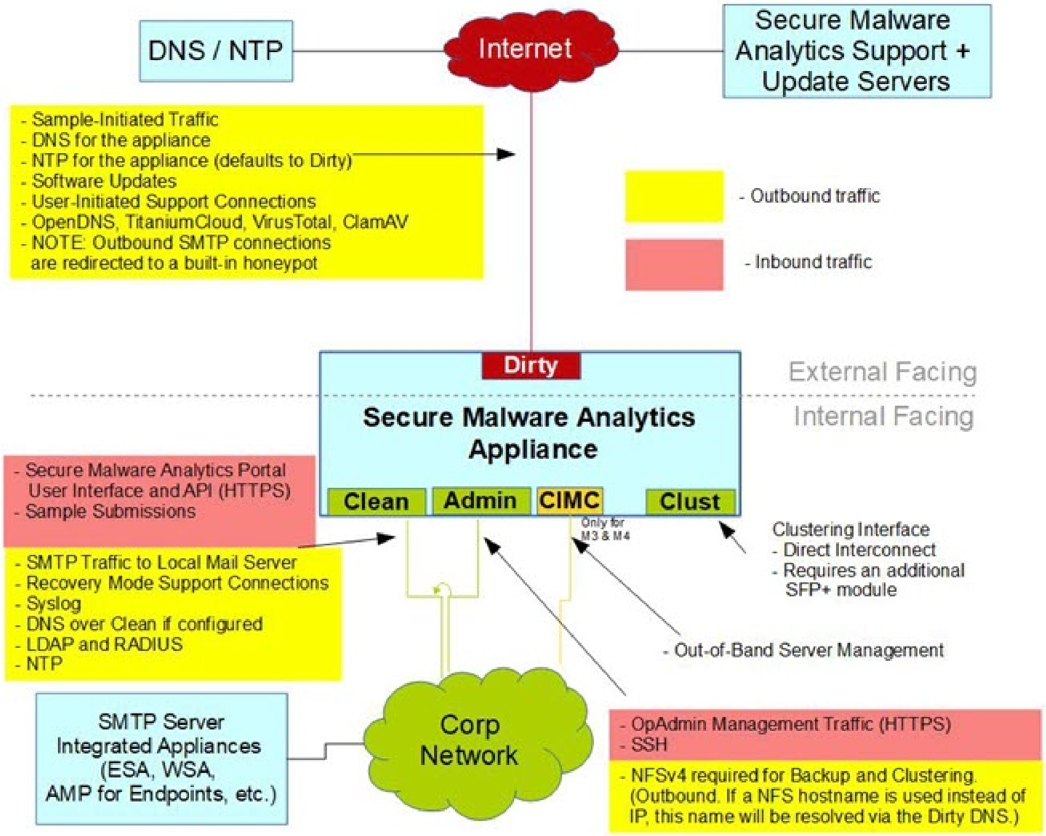
Interface	Description
Admin	- Connect to the Admin network. **Only inbound** from Admin network. - Admin UI traffic - SSH (inbound) for Admin TUI - NFSv4 for backups and clustering (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.) Must be accessible from all cluster notes. - The Admin port can be disabled (from the tgsh shell); from the Admin UI with v2.11. When disabled, non-clustered Secure Malware Analytics Appliances can operate correctly with only the clean and dirty ports connected, and the admin UI will be presented on port 8443 of the clean interface (an also port 18443 with the v2.11 release). If the port is not disabled, unplugging the admin port results in a non-functional (or at best, a partially functional) Secure Malware Analytics Appliance. **Note** The form factor for the Admin interface is SFP+. See Hardware Requirements.
Clust	The non-Admin SFP+ port is used for clustering. - Clust interface required for clustering (optional) - Requires an additional SFP+ module for direct interconnect. This interface does not require any configuration. Addresses are automatically assigned.
Clean	- Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet. - UI and API traffic (inbound) - Sample submissions - SMTP (outbound connection to the configured mail server) - SSH (inbound for Admin TUI) - Syslog (outbound to configured syslog server) - ESA/WSA and CSA Integrations - Secure Endpoint Private Cloud Integration - DNS optional - LDAP (outbound) - RADIUS (outbound) - NTP (for using an internal NTP server)

Interface	Description
Dirty	Connect to the Dirty network; requires Internet access. Outbound Only. You should not use your own DNS (private IP) for the Dirty Interface because traffic sent to a private IP is dropped at the Network Exit Localization firewall. • DNS **Note** If you are setting up an integration with a Secure Endpoint Private Cloud, and the Secure Endpoint appliance hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the Admin UI. • NTP (defaults to Dirty) • Updates • Support sessions • Support snapshots • Malware sample-initiated traffic • OpenDNS, TitaniumCloud, VirusTotal, ClamAV_signature updates • SMTP outbound connections are redirected to a built-in honeypot **Note** Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.
CIMC Interface	If the Cisco Integrated Management Controller (CIMC) interface is configured, it can be used for server management and maintenance. See CIMC Configuration. **Note** CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

Network Interface Setup Diagram

This section describes the most logical and recommended setup for a Secure Malware Analytics Appliance. However, each customer's interface setup is different. Depending on your network requirements, you may decide to connect the Dirty interface to the inside, or the Clean interface to the outside with appropriate network security measures in place.

Figure 11: Network Interfaces Setup Diagram


DNS / NTP
Internet
Secure Malware Analytics Support + Update Servers
- Sample-Initiated Traffic
- DNS for the appliance
- NTP for the appliance (defaults to Dirty)
- Software Updates
- User-Initiated Support Connections
- OpenDNS, TitaniumCloud, VirusTotal, ClamAV
- NOTE: Outbound SMTP connections are redirected to a built-in honeypot
- Outbound traffic
- Inbound traffic
Dirty
External Facing
Internal Facing
Secure Malware Analytics Appliance
Clean
Admin
CIMC
Clust
Only for M3 & M4
- Secure Malware Analytics Portal User Interface and API (HTTPS)
- Sample Submissions
- SMTP Traffic to Local Mail Server
- Recovery Mode Support Connections
- Syslog
- DNS over Clean if configured
- LDAP and RADIUS
- NTP
Clustering Interface
- Direct Interconnect
- Requires an additional SFP+ module
- Out-of-Band Server Management
SMTP Server
Integrated Appliances (ESA, WSA, AMP for Endpoints, etc.)
Corp Network
- OpAdmin Management Traffic (HTTPS)
- SSH
- NFSv4 required for Backup and Clustering. (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via the Dirty DNS.)

Note In Secure Malware Analytics Appliance (v2.7.2 and later), the **enable_clean_interface** option is available but is disabled by default. This option (after applying configuration and rebooting) enables access to the administrative interface on port 8443 and 18443 of the assigned clean IP. Disabling the admin ethernet interface will also enable this access on port 8843 of clean.

Firewall Rules

This section provides suggested firewall rules.

Note Implementing a restrictive outgoing policy on the Dirty interface for ports 22 and 19791 requires tracking updates over time and spending more time maintaining the firewall.

Note Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.

Dirty Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	ANY	ANY	Allow	Allow outbound traffic from samples, optionally proxied through Cisco datacenters. (To get accurate results it is required that malware be allowed to contact its command and control server using whatever port and protocol it is designed to use.)

Dirty Interface Inbound

Source	Destination	Protocol	Port	Action	Note
ANY	Dirty Internet	ANY	ANY	Deny	Deny all incoming connections.

Clean Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Clean Interface	SMTP Servers	TCP	25	Allow	The appliance uses the clean interface to initiate SMTP connections to the configured mail server.

Clean Interface Outbound (Optional)

Source	Destination	Protocol	Port	Action	Note
Clean Interface	Corporate DNS Server	TCP/UDP	53	Allow	Optional, only required if Clean DNS is configured.
Clean Interface	AMP Private Cloud	TCP	443	Allow	Optional, only required if Secure Endpoint Private Cloud integration is used.
Clean Interface	Syslog Servers	UDP	514	Allow	Allow connectivity to server designated to receive Syslog messages and Secure Malware Analytics notifications.
Clean Interface	LDAP Servers	TCP/UDP	389	Allow	Optional, only required if LDAP is configured.

Source	Destination	Protocol	Port	Action	Note
Clean Interface	LDAP Servers	TCP	636	Allow	Optional, only required if LDAP is configured.
Clean Interface	RADIUS Servers	DTLS	2083	Allow	Allow login to Secure Malware Analytics application UI (Face). Optional, only required if RADIUS is configured.
Clean Interface	Internet	UDP	123	Allow	Optional, use this off-by-default functionality to use an internal NTP server.

Clean Interface Inbound

Source	Destination	Protocol	Port	Action	Note
User Subnet	Clean Interface	TCP	22	Allow	Allow SSH connectivity to the Admin TUI.
User Subnet	Clean Interface	TCP	80	Allow	Appliance API and Secure Malware Analytics user interface. This will redirect to HTTPS TCP/443.
User Subnet	Clean Interface	TCP	443	Allow	Appliance API and Secure Malware Analytics user interface.
User Subnet	Clean Interface	TCP	9443	Allow	Allow connectivity to the Secure Malware Analytics UI Glovebox.

Admin Interface Outbound (Optional)

The following depends on what services are configured.

Source	Destination	Protocol	Port	Action	Note
Admin Interface	NFSv4 Server	TCP	2049	Allow	Optional, only required if Secure Malware Analytics Appliance is configured to send backups to an NFSv4 share.

Admin Interface Inbound

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	22	Allow	Allow SSH connectivity to the Admin TUI.

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	80	Allow	Allow access to the Admin UI. This will redirect to HTTPS TCP/443.
Admin Subnet	Admin Interface	TCP	443	Allow	Allow access to the Admin UI.

Dirty Interface for Non Cisco-Validated/Recommended Deployment

Non Cisco-Validated/Recommended - Firewalling outbound traffic can reduce efficacy by preventing malware from connecting to command and control infrastructure, limiting efforts to determine what would be downloaded from that command and control infrastructure.

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	22	Allow	Update, support snapshot, and licensing services.
Dirty Interface	Internet	TCP/UDP	53	Allow	Allow outbound DNS.
Dirty Interface	Internet	UDP	123	Allow	Allow outbound NTP.
Dirty Interface	Internet	TCP	19791	Allow	Allow connectivity to Secure Malware Analytics support.
Dirty Interface	Cisco Umbrella	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	VirusTotal	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	TitaniumCloud	TCP	443	Allow	Connect with third-party detection and enrichment services.

Privacy and Sample Visibility

When submitting samples to a Secure Malware Analytics Appliance for analysis, an important consideration is the privacy of the content. Privacy is a particularly important consideration if sensitive documents or archive types are submitted for analysis, because locating sensitive material could be relatively easy for those with access to the Secure Malware Analytics Appliance, especially with the search API.

The privacy and sample visibility model for sample submissions to Secure Malware Analytics is as follows:

- Unless samples are designated as Private, they are visible to users who are outside the submitter's organization.

- Private samples can only be seen by Secure Malware Analytics users within the same organization as the user who submitted the sample.

Samples Submitted by Integrations

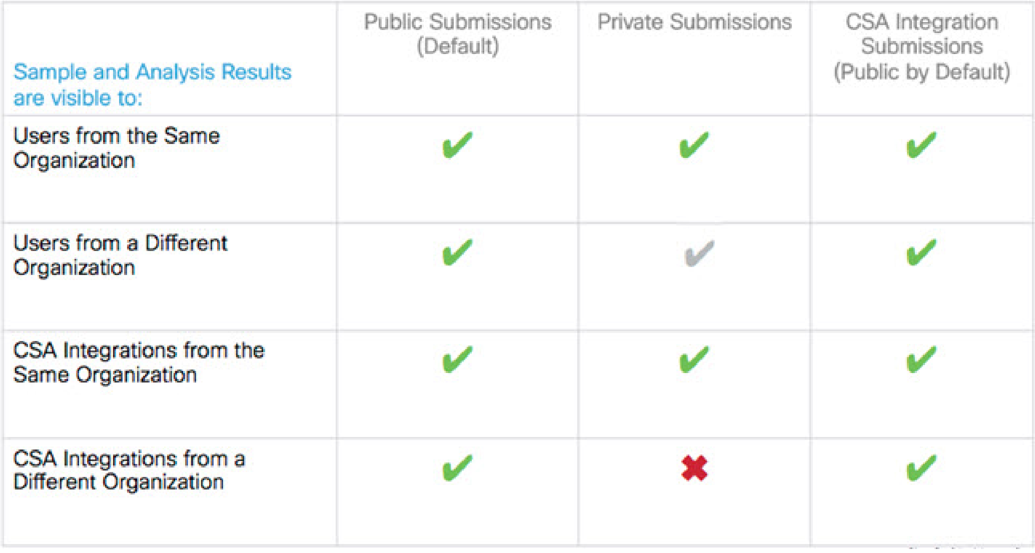
The privacy and sample visibility model is modified on Secure Malware Analytics Appliances for samples that are submitted by integrations. Integrations are Cisco products such as Email Security Appliance (ESA), Web Security Appliance (WSA), and other devices or third-party services (you may see the term CSA Integrations, which refers to ESA/WSA and other Cisco appliances, devices, and services that are integrated; for example, registered, with Secure Malware Analytics Appliance via the Cisco Sandbox API.)

All sample submissions on Secure Malware Analytics Appliances are Public by default, and can be viewed by any other appliance user, including integrations, regardless of the organization to which they belong. All appliance users can see all details of samples submitted by all other users.

Secure Malware Analytics users may also submit Private samples to the Secure Malware Analytics Appliance, which are only visible to other Secure Malware Analytics Appliance users, including integrations, from the same organization as the sample submitter.

Privacy and sample visibility model on Secure Malware Analytics Appliances are illustrated in the table.

Figure 12: Privacy and Visibility on a Secure Malware Analytics Appliance



Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✓	✓	✓
Users from a Different Organization	✓	✓	✓
CSA Integrations from the Same Organization	✓	✓	✓
CSA Integrations from a Different Organization	✓	✖	✓

- **Full Access** - The green check mark indicates that users have full access to the sample and the analysis results.
- **Scrubbed Reports** - The grey check mark indicates that the Private submission results are scrubbed. Users have partial access to the sample and analysis results, but all potentially sensitive information about the sample is removed. There are no filenames, process names, screenshots, or even specifics about its activity in the glovebox.

  We omit details from the Metadata section, such as the sample submitter's login information. If you encounter a hash from a private sample in the course of doing business, this will let alert you to known threats, and if you need more details, submit your own copy of the sample for full analysis.

Private samples may not be downloaded. Scrubbed reports include Artifacts (with filename removed), Behavioral Indicators, Domains, and IPs.

- **No Access** - The red X indicates that users have no access to the sample or the analysis results.

The same basic privacy rules apply to Secure Malware Analytics Appliance integrations with Secure Endpoint Private Cloud.

Wipe Appliance Operation

The Wipe Appliance operation enables you to wipe the disks on a Secure Malware Analytics Appliance to remove all data prior to decommissioning or returning it to the Cisco Demo Loan Program.

Important After performing the wipe appliance procedure, the Secure Malware Analytics Appliance will no longer operate without being returned to Cisco for reimaging (Except for demo loan program customers, re-imaging service is not guaranteed to be available without prior agreement).

For more information, see Removing All Data with the Wipe Appliance Operation.

Customer Data

Logs, active configuration, and other customer-owned data is now stored almost exclusively on the RAID 5 data array, rather than being distributed between data and OS drives. The remaining appliance-specific content stored on OS drives is limited to information required for correct operation of recovery mode should the data drives not be mountable, and has limited privacy impact if disclosed.

Because less content is stored on the OS array with the 2.12 release, early appliances (with smaller OS drives) are less likely to need to delete VM images other than the mandatory default image during a data reset (and thus need to download updates online before those deleted VM images become available again).

CHAPTER 3

Network Configuration Using the Admin TUI

The initial Secure Malware Analytics Appliance network configuration is completed during the appliance setup using the Admin TUI, as documented in the *Cisco Threat Grid Appliance Getting Started Guide*. This chapter provides additional information about using the Admin TUI to make changes to your initial network configuration:

Modifying Network Configuration

The initial network configuration is completed using the Admin TUI. If you want to make changes to your initial network configuration, perform the following steps.

Note If you are using DHCP to obtain IPs, see the Network section.

Procedure

Step 1 Login to Admin TUI.

Note

If you are configured for **LDAP Only** authentication, you can only log into Admin TUI using LDAP. If authentication mode is set to **System Password or LDAP**, the Admin TUI login only allows the **System** login.

Step 2 In the Admin TUI interface, choose **CONFIG_NETWORK**.

The **Network Configuration** console opens and displays the current network settings.

Step 3 Make any necessary changes (you need to backspace over the old entry before you can enter the new one).

Step 4 Leave the Dirty network **DNS Name** blank.

Step 5 After you finish updating the network settings, tab down and choose **Validate** to verify your entries.

If errors occur, fix the invalid values and choose **Validate** again.

After validation, the **Network Configuration Confirmation** page displays the entered values

Step 6 Choose **Apply** to apply your configuration settings.

Detailed information about the configuration changes that have been made are displayed.

Step 7 Choose **OK**.

The **Network Configuration** console refreshes again and displays the IP addresses. Network configuration is now complete.

Reconnecting to Admin TUI

Admin TUI remains open on the console and can be accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

To reconnect to the Admin TUI, SSH into the Admin IP address as the user **threatgrid**. The required password is either the initial randomly generated password, which is visible initially in the Admin TUI, or the new Admin password you created during the first step of the Admin UI configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*).

Configuring Network in Recovery Mode

Network configuration in recovery mode mirrors the full system (v2.7 and later):

- All interfaces are brought up.
- Firewall rules and policy routing restricts which processes can communicate on which interfaces.

Note Support mode traffic on port 19791 is allow-listed across all three interfaces.

Perform the following steps to set up networking in recovery mode.

Procedure

Step 1 Reboot the Secure Malware Analytics Appliance (**Operations** > **Power** > **Reboot**) and then choose **Recovery Mode** in the boot menu.

Step 2 Once the system is up, press **Enter** several times to get a clean command prompt.

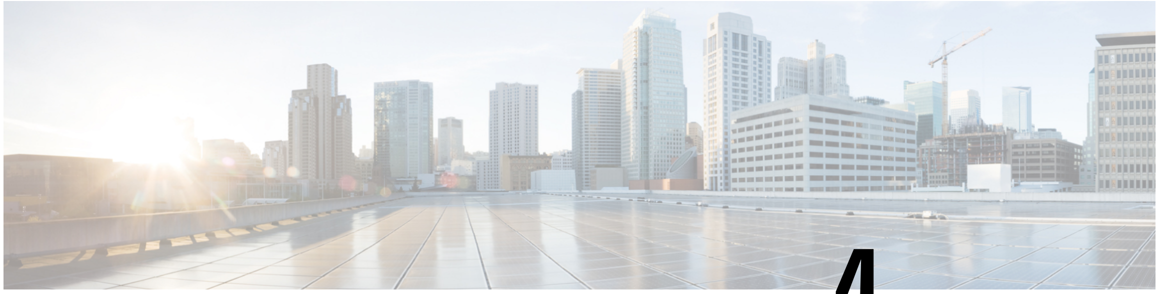
Step 3 Enter **netctl clean** and provide the following information:

- **Configuration type (dhcp|static)[Current: DHCP]**: static
- **IP Address (ipaddr)** - <Clean IP Address>
- **Netmask (ipaddr)** -<Netmask>

- **Gateway Address** - <Clean network gateway>
- **DNS name of this interface's address** - Enter DNS name of this interface's address
- **Primary DNS server for LAN addresses** - Enter primary DNS server address
- **Secondary DNS server for LAN addresses** - Enter secondary DNS server address
- **Save this profile? (Yes|No)** - Enter **Yes**

Step 4 Enter **netconfig-apply** to apply the configuration.

The appliance will attempt to open an outbound support connection on the Clean interface on port 19791/tcp.



CHAPTER 4

Configuration Using the Admin UI

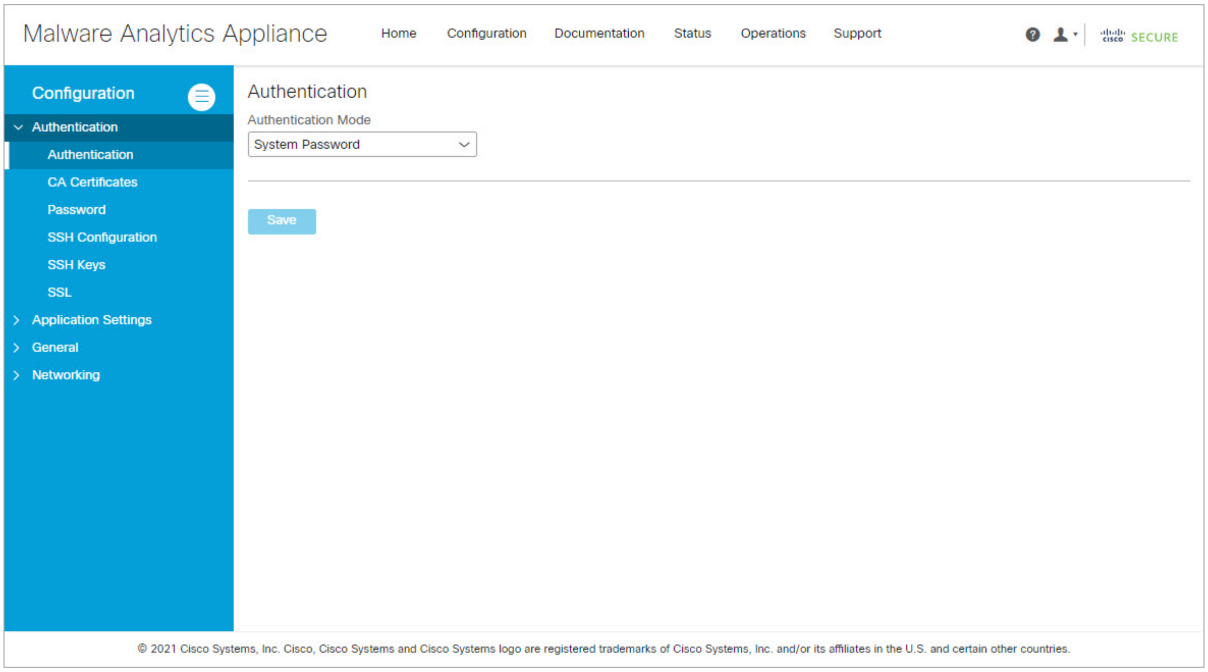
The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Getting Started Guide. New Secure Malware Analytics Appliances may require the administrator to complete additional configuration, and Admin UI settings may require updates over time. This chapter provides information about using the Admin UI to make configuration changes to your appliance.

About the Admin UI

The Admin UI is the Secure Malware Analytics Appliance administrator's main configuration interface. It is a Web portal that can be used once an IP address has been configured on the Secure Malware Analytics Appliance Admin interface.

Note The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Getting Started Guide.

Figure 13: Configuration



Authentication

Authentication Mode: System Password

© 2021 Cisco Systems, 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.

The **Configuration** menu in the Admin UI is used to configure and manage various Secure Malware Analytics Appliance configuration settings, including:

Section	Description
Authentication	
Authentication	Describes how to configure LDAP and RADIUS authentication for logging into the Secure Malware Analytics Appliance Admin UI.
CA Certificates	Describes how to add CA certificate for outbound SSL connections for the appliance to trust the Cisco Secure Endpoint Private Cloud.
Password	Describes how to change your Admin UI password.
SSH Configuration, on page 41	Describes how to configure SSH to setup some key elements via SSH.
SSH Keys, on page 42	Describes how to set up SSH keys to provide access to the Admin TUI via SSH.
SSL	Describes how to configure SSL certificates to support Secure Malware Analytics Appliance connections with Email Security Appliance (ESA), Web Security Appliance (WSA), Secure Endpoint Private Cloud, and other integrations; replacing SSL certificates.
Application Settings	
Integrations	Describes how to configure third-party detection and enrichment services (OpenDNS, TitaniumCloud, VirusTotal); enable or disable ClamAV automatic updates.

Section	Description
License	Describes how to upload your Secure Malware Analytics Appliance license or retrieve it from the server.
Network Exit	Describes how to configure the network exit options that are available in the Secure Malware Analytics portal when submitting samples for analysis.
Updates Proxy, on page 56	Describes how to configure the SOCKS5 proxy to download the updates.
General	
Content Update, on page 57	Describes how to enable Content Update.
Date and Time	Describes how to add Network Time Protocol (NTP) server to configure date and time.
Email	Describes how to configure your email settings (SMTP) for system notifications.
Notifications	Describes how to manage notification recipients.
Syslog	Describes how to configure a system log server to receive syslog messages and notifications.
Networking	
Network	Describes how to adjust the IP assignment from DHCP to your permanent static IP addresses, and how to configure DNS.
NFS	Describes appliance backup, including NFS requirements, backup storage requirements, backup expectations, and configuring the strict retention period limits; how to perform a backup.
Clustering	Describes features, limitations, and requirements of clustering Secure Malware Analytics Appliances; network and NFS storage requirements; how to build a cluster, join appliances to the cluster, remove cluster nodes, and designate a tie-breaker node; failure tolerances and failure recovery; API and operational usage and characteristics for clusters, and sample deletion.

Note

- Configuration updates in the Admin UI should be completed in one session to reduce the chance of an interruption to the IP address during configuration.
- The Admin UI does not validate the gateway entries. If you enter the wrong gateway and save it, the Admin UI will not be accessible. You will need to use the console to fix the networking configuration if that was done on the Admin interface. If Admin is still valid, you can fix it in the Admin UI and reboot.
- Secure Malware Analytics Appliances (v2.7 or later) use the serial number as the hostname to improve interoperability with some NFS v4 servers.

Important The Admin UI uses HTTPS and you must enter this in the browser address bar; pointing to only the Admin IP is not sufficient. Enter the following address in your browser:

https://adminIP/

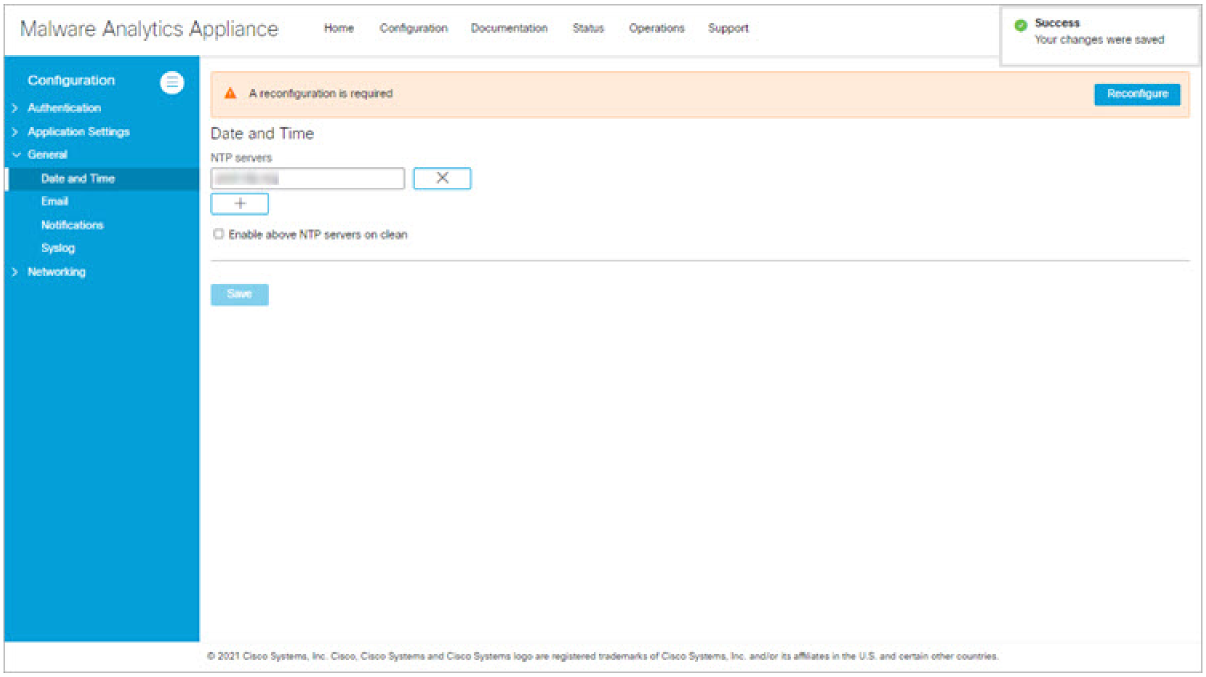
OR

https://adminHostname/

Applying Configuration Changes

Any time changes are made to configuration settings, a light orange alert message appears in a banner in the upper portion of the **Configuration** page.

Figure 14: Reconfigure Required Alert Message



Success
Your changes were saved

A reconfiguration is required

Date and Time

NTP servers: [redacted]

□ Enable above NTP servers on clean

© 2021 Cisco Systems, 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.

Changes to the Admin UI configuration settings must be saved, and several also include a step to activate the change. However, you must also finalize the changes with a reconfiguration in a separate step. Configuration changes do not take effect until reconfiguration is completed.

Note Reconfiguration may affect other users logged in to Secure Malware Analytics portal and the Admin UI.

Procedure

Step 1 Click **Reconfigure** on the alert message to launch the reconfiguration process. Otherwise to reconfigure, click **Operations** >> **Activate**.

Step 2 On the **Activate Configuration** page, click **Reconfigure** to run the reconfiguration job.

Step 3 On the confirmation dialog, click **Reconfigure** to start the reconfiguration job.

Configuration is activated, and messages on its progress are displayed in the jobs window. Details are kept in the **Jobs** page if you need to review error messages or other information.

When completed, a confirmation message is displayed indicating the reconfiguration was successful.

Step 4 Click **Continue**.

Authentication

The Secure Malware Analytics Appliance supports LDAP authentication and authorization for logging into the Admin UI and the Admin TUI. It also supports RADIUS authentication, which allows for single sign-on to the Admin UI in v2.10 and later.

LDAP Authentication

The Secure Malware Analytics Appliance supports LDAP authentication and authorization for Admin UI and Admin TUI login. You can authenticate multiple appliance administrators with different credentials that are managed on the domain controller or the LDAP server. Authentication modes include: System Password Only, System Password or LDAP, and LDAP Only.

There are three LDAP Protocol options: LDAP, LDAPS, and LDAP with STARTLS.

The following considerations should be observed:

- The dual authentication mode (**LDAP or System Password**) is required to avoid accidentally locking yourself out of the Secure Malware Analytics Appliance when setting up LDAP.

  Choosing **LDAP Only** is not allowed initially; you must first go through dual mode to make sure it works. You must log out of the Admin UI after the initial configuration, and then log back in using LDAP credentials to toggle to **LDAP Only**.

- You can only log into the Admin TUI using LDAP if you are configured for **LDAP Only** authentication. If authentication mode is set to **LDAP or System Password**, the Admin TUI login only allows the System login.

- If the Secure Malware Analytics Appliance is configured for LDAP authentication only (**LDAP Only**), you can reset the password in recovery mode to reconfigure the authentication mode to also allow login with a system password.

- Make sure that the authentication filter is set up to restrict membership.

- The Admin TUI and the Admin UI require LDAP credentials only in **LDAP Only** mode/ if **LDAP only** is configured, the Admin TUI only prompts for the LDAP user/password; not the system password.

- If authentication is configured for **System Password or LDAP**, the Admin TUI prompts for for only the system password; not both.
- To troubleshoot LDAP issues, disable it by resetting the password in Recovery Mode.
- To access the Admin TUI via SSH, a system password or a configured SSH key is required in addition to LDAP credentials when in **LDAP Only** mode.
- LDAP is outbound from the Clean interface.

Perform the following steps to configure LDAP authentication in the Admin UI.

Procedure

Step 1 Click the **Configuration** tab.

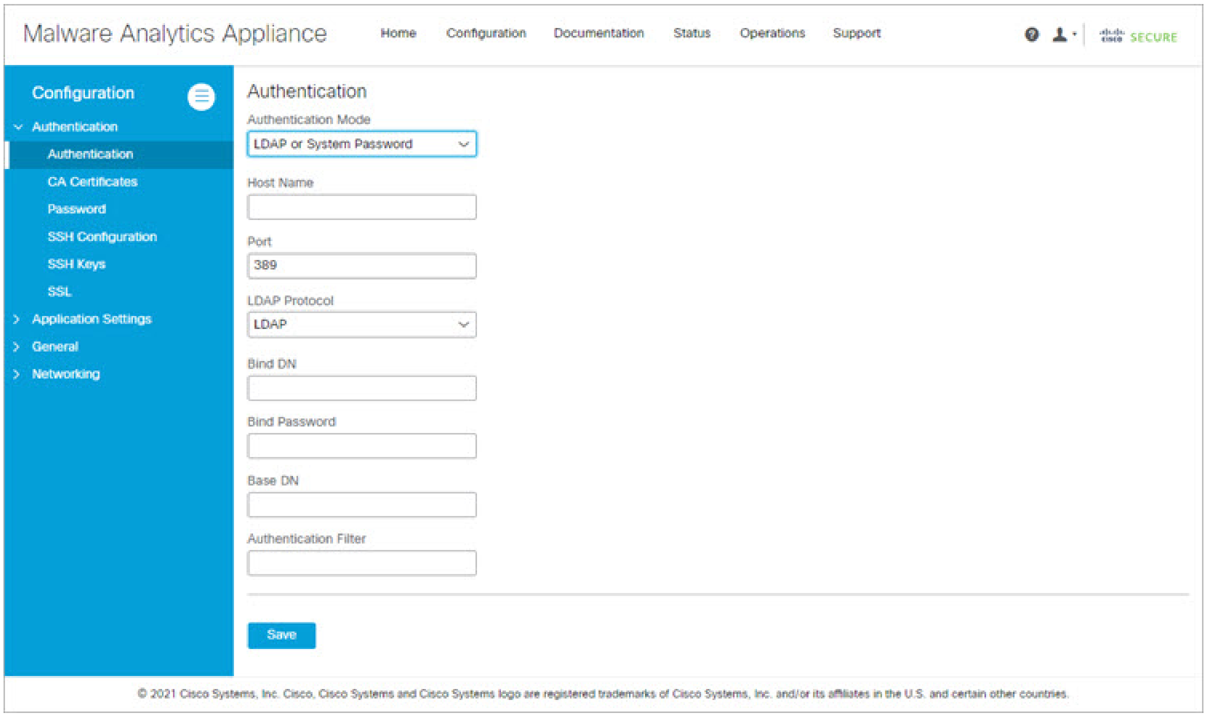
Step 2 Expand **Authentication** in the side navigation and choose **Authentication**.

Step 3 From the **Authentication Mode** drop-down, choose **LDAP or System Password** to open the LDAP configuration page.

Note

The first time you configure LDAP authentication, you must choose **LDAP or System Password**, log out of the Admin UI, and then log back in using your LDAP credentials. You can then change the setting to **LDAP**.

Figure 15: LDAP Authentication Configuration Page



Authentication

Authentication Mode: LDAP or System Password

Host Name:

Port: 389

LDAP Protocol: LDAP

Bind DN:

Bind Password:

Base DN:

Authentication Filter:

© 2021 Cisco Systems, 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 4 Complete the fields on the page as appropriate:

- **Hostname** - The host name to connect to via LDAP.
- **Port** - The port number to connect to via LDAP (default 389).

- **Authentication Mode** - The authentication mode to be used upon login.
- **LDAP Protocol** - The LDAP protocol in use.
- **Bind Password** - The password to use for binding via LDAP.
- **Bind DN** -The Distinguished Name to bind to via LDAP; for example: cn=admin,dc=foo,dc=com.
- **Base** - The base to bind to via LDAP; for example: ou=users,dc=foo,dc=com (LDAP only).
- **Authentication Filter** - The filter to be applied for authentication upon login; for example: (&(cn=%LOGIN%) (memberOf=cn=admingroup, ou=groups,dc=foo,dc=com)).

Step 5 Click **Save**.

When users log in to the Admin UI or Admin TUI, they will now be prompted for their LDAP authentication.

RADIUS Authentication

Secure Malware Analytics Appliance (v2.10 and later) supports RADIUS authentication, which uses Cisco Identity Services Engine with DTLS enabled. If RADIUS authentication is enabled, users can log in to the main Secure Malware Analytics application UI and OpAdmin with the appropriate single sign-on password.

The following considerations should be observed:

- The dual authentication mode (**RADIUS or System Password**) is required to avoid accidentally locking yourself out of the Secure Malware Analytics Appliance when setting up RADIUS.

  Choosing **RADIUS Only** is not allowed initially; you must first go through dual mode to make sure it works. You must log out of the Admin UI after the initial configuration, and then log back in using RADIUS credentials to toggle to **RADIUS Only**.

- You can only log into the Admin TUI using RADIUS if you are configured for **RADIUS Only** authentication. If authentication mode is set to **RADIUS or System Password**, the Admin TUI login only allows the System login.
- If the Secure Malware Analytics Appliance is configured for RADIUS authentication only (**RADIUS Only**), you can reset the password in recovery mode to reconfigure the authentication mode to also allow login with a system password.
- The Admin TUI and the Admin UI require RADIUS credentials only in **RADIUS Only** mode/ if **RADIUS only** is configured, the Admin TUI only prompts for the RADIUS user/password; not the system password.
- If authentication is configured for **RADIUS or System Password**, the Admin TUI prompts for for only the system password; not both.
- To troubleshoot RADIUS issues, disable it by resetting the password in Recovery Mode.
- To access the Admin TUI via SSH, a system password or a configured SSH key is required in addition to RADIUS credentials when in **RADIUS Only** mode.
- RADIUS is outbound from the Clean interface.

Perform the following steps in the Admin UI to configure RADIUS authentication:

Procedure

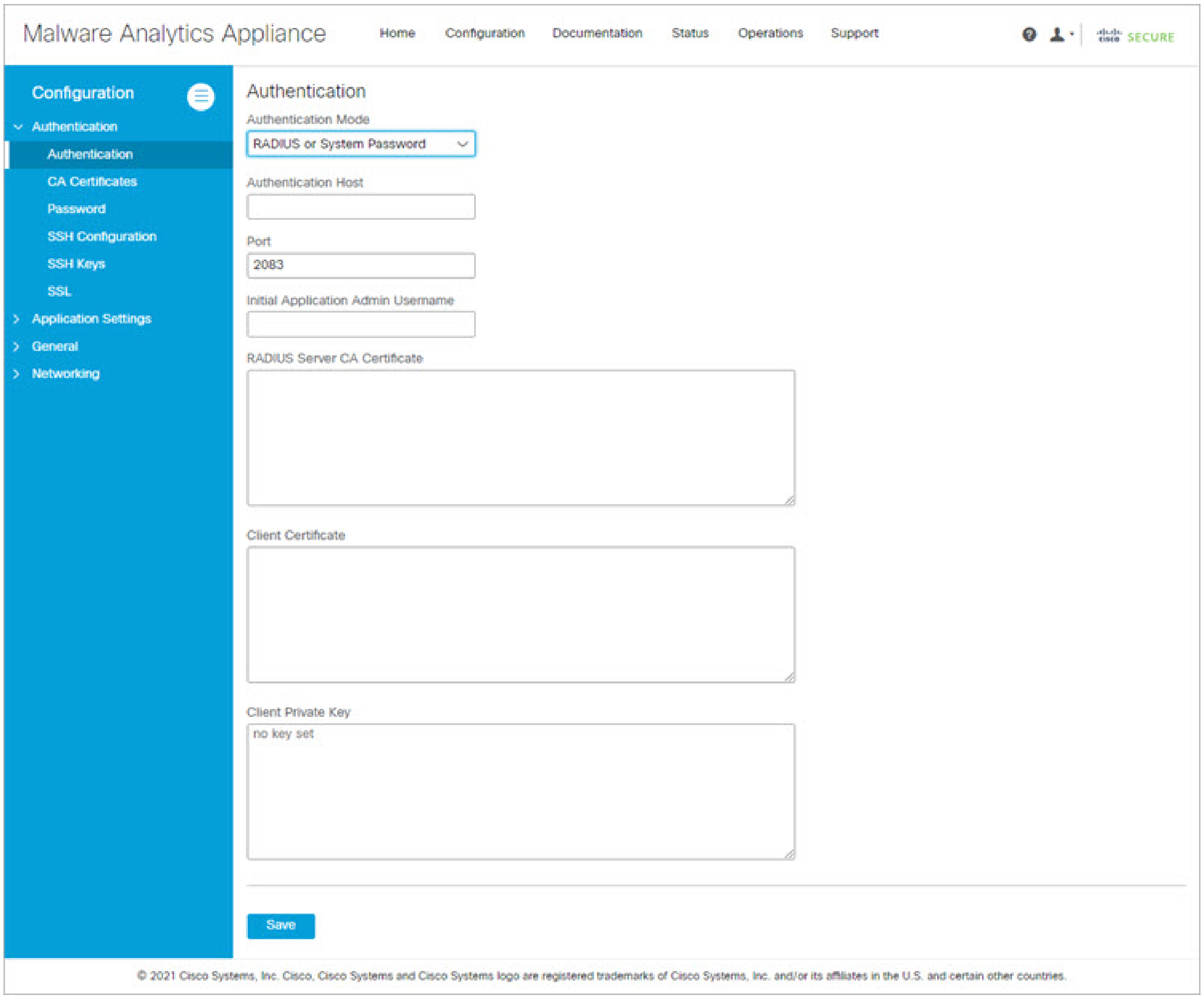
Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **Authentication**.

Step 3 From the **Authentication Mode** drop-down, choose **RADIUS or System Password** to open the RADIUS configuration page.

Note
The first time you configure RADIUS authentication, you must choose **RADIUS or System Password**, log out of the Admin UI, and then log back in using your RADIUS credentials. You can then change the setting to **RADIUS**. Logging in a second time after RADIUS and system password is configured ensures that RADIUS configuration is validated before removing system password as a fallback login method.

Figure 16: RADIUS Authentication Configuration Page



Authentication

Authentication Mode: RADIUS or System Password

Authentication Host:

Port: 2083

Initial Application Admin Username:

RADIUS Server CA Certificate:

Client Certificate:

Client Private Key: no key set

© 2021 Cisco Systems, 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 4 Complete the fields on the page as appropriate:

- **Hostname** - The host name to connect to via RADIUS.

- **Port** - The DTLS port number to connect to via RADIUS (default 2083). Unlike conventional RADIUS, DTLS uses a single port for both authentication and accounting. Only DTLS-based RADIUS authentication is supported.
- **Initial Face Admin** - The RADIUS user to whom the initial/default administration user in the primary Secure Malware Analytics UI shall be mapped. This account should be the party responsible for creating other user accounts in Secure Malware Analytics and configuring their permissions.
- **CA Certificate** - A PEM-format CA certificate to be used to authenticate the RADIUS server used for authentication. Will change to <VALID> when successfully saved. Clear this to empty the field.
- **Client Certificate** - A PEM-format client certificate to be used to authenticate this host to the RADIUS server used for authentication. This value will change to <VALID> when successfully saved; you can clear it to empty the field.
- **Client Private Key** - A PEM-format key to be used to authenticate this host to the RADIUS server used for authentication. The value must correspond with the client certificate given above. The value will change to <VALID> when successfully saved; you can clear it to empty the field. Private keys in PEM-encoded PKCS#8 format are supported by the new Admin UI.

Step 5 Click **Save**.

Note

`NAS-Identifier` is sent in the authentication requests from the Security Malware Analytics application UI and OpAdmin.

- `NAS-Identifier` sent in authentication requests from SMA portal is: `Threat Grid UI`.
- `NAS-Identifier` sent in authentication requests from OpAdmin is: `Threat Grid Admin`.

For more information on the specific values sent through the `NAS-identifier`, see https://www.rfc-editor.org/rfc/rfc2865.html#section-5.32.

CA Certificates

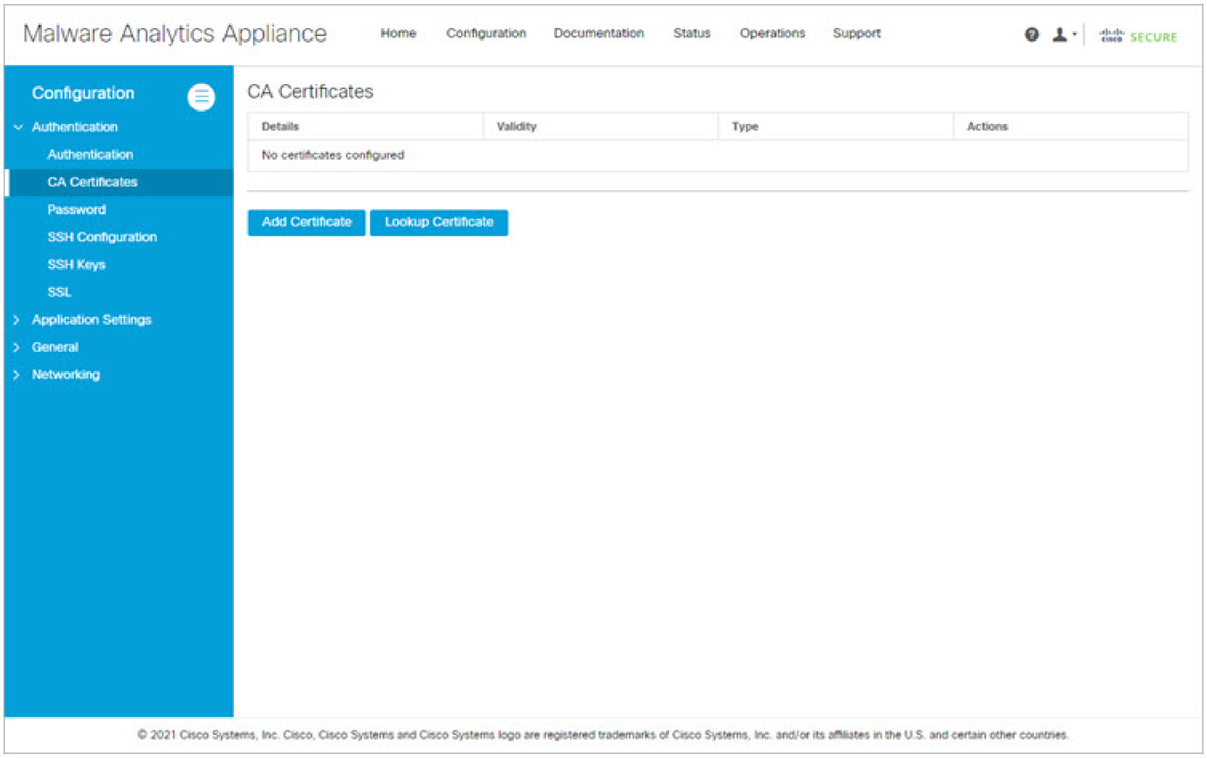
The **CA Certificates** page in the Admin UI is used to manage the Certificate Authority (CA) certificate trust store for outbound SSL connections so that the Secure Malware Analytics Appliance can trust the Cisco Secure Endpoint Private Cloud to notify it about analyzed samples that are considered malicious.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **CA Certificates** to open the **CA Certificates** page.

Figure 17: CA Certificates Page



Details	Validity	Type	Actions
No certificates configured			

© 2021 Cisco Systems, 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 3 Create a **.pem** file that contains the outbound SSL connections (CA certificates) for the Secure Endpoint Private Cloud, copy the contents, and paste it into the **Certificate** field.

Step 4 Click **Add Certificate** and confirm. Changing a CA certificate does ot require reconfiguration.

Password

Your appliance password is used to authenticate to the Secure Malware Analytics Appliance Admin UI as well as the appliance console. You can change your password from the Admin UI using the **Password** page.

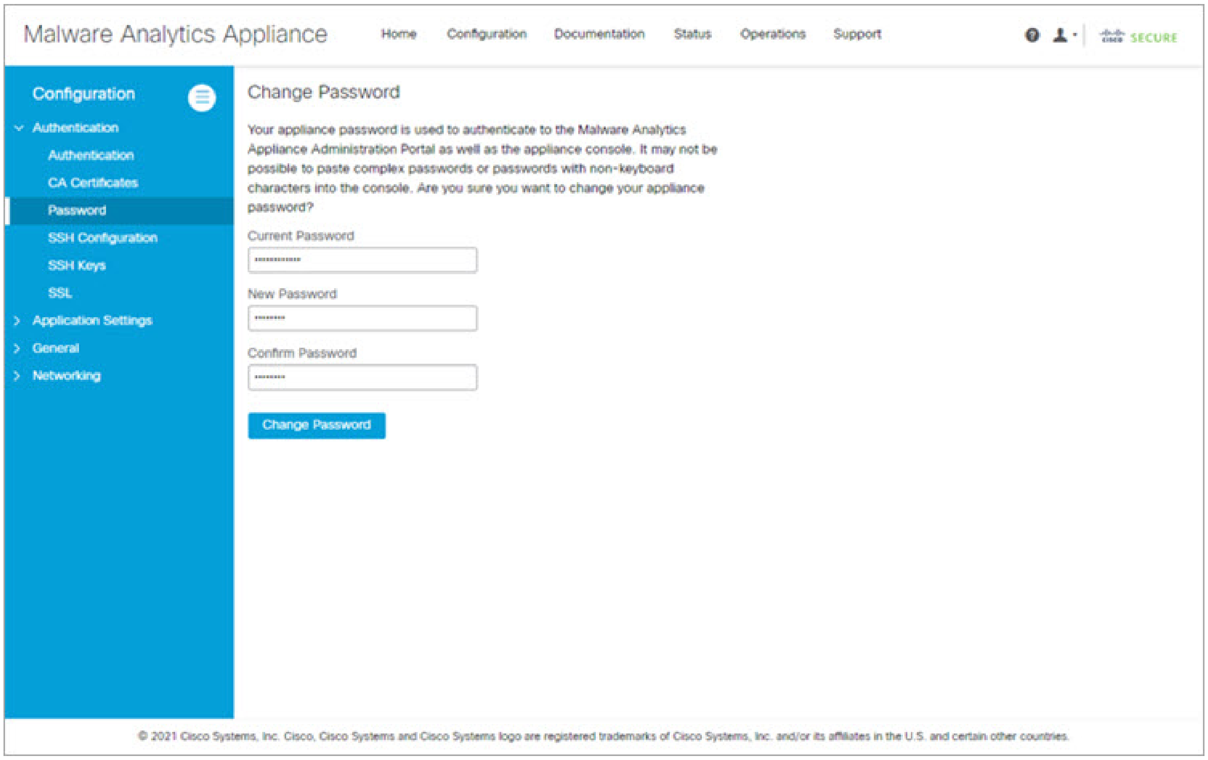
Note It may not be possible to paste complex passwords or passwords with non-keyboard characters into the console so be careful when you change your password.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **Password**.

Figure 18: Password



Change Password

Your appliance password is used to authenticate to the Malware Analytics Appliance Administration Portal as well as the appliance console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the console. Are you sure you want to change your appliance password?

Current Password

New Password

Confirm Password

© 2021 Cisco Systems, 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 3 Enter your **Current Password**, and then enter the **New Password** and **Confirm Password**.

Step 4 Click **Change Password** and confirm the change. Changing a password does not require reconfiguration.

SSH Configuration

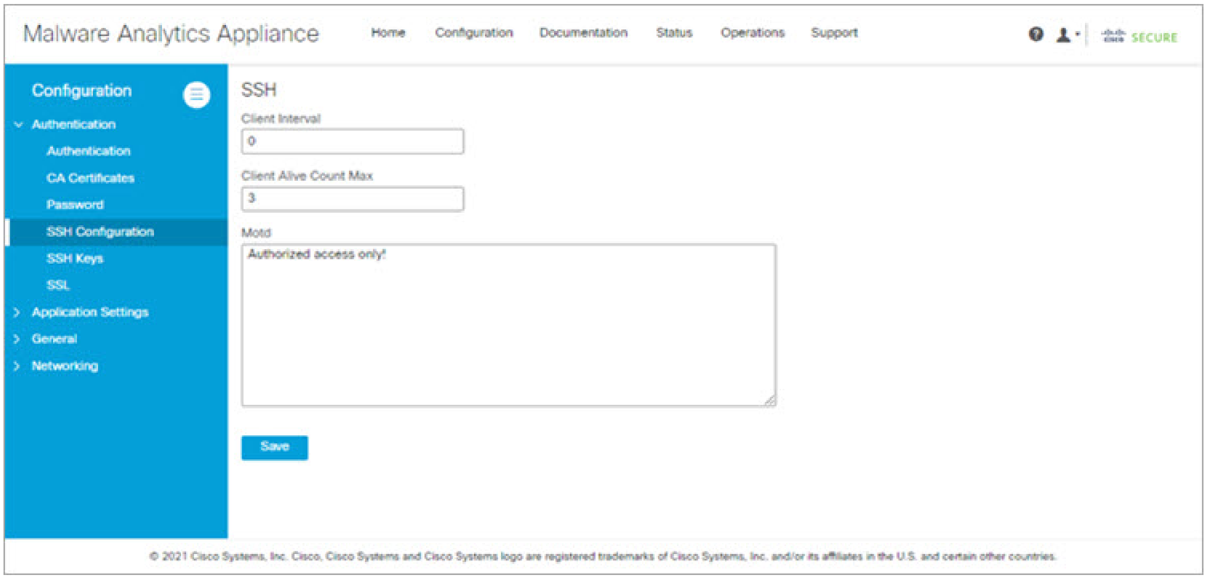
Setting up SSH Configuration provides the Secure Malware Analytics Appliance administrator with access to set the *ClientAliveInterval*, *ClientAliveCountMax*, and *motd* (Message of the Day) on your appliance using the **SSH Configuration** page in the Admin UI.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **SSH Configuration** to open the **SSH Configuration** page.

Figure 19: SSH Configuration



SSH

Client Interval: 0

Client Alive Count Max: 3

Motd: Authorized access only!

© 2021 Cisco Systems, 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 3 Enter the **Client Interval**. *Client Interval* or *ClientAliveInterval* - Sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.

Step 4 Enter the **Client Alive Count Max**. *Client Alive Count Max* or *ClientAliveCountMax* - Sets the number of client alive messages which is sent without SSH receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session.

Step 5 Enter the **Motd** (Message of the Day). It is used to display a message when a remote user login to the Secure Malware Analytics appliance using SSH.

SSH Keys

Setting up SSH keys provides the Secure Malware Analytics Appliance administrator with access to the Admin TUI via SSH (`threatgrid@<host>`); it does not provide root access or a command shell. You can add and remote SSH keys on your appliance using the **SSH Keys** page in the Admin UI.

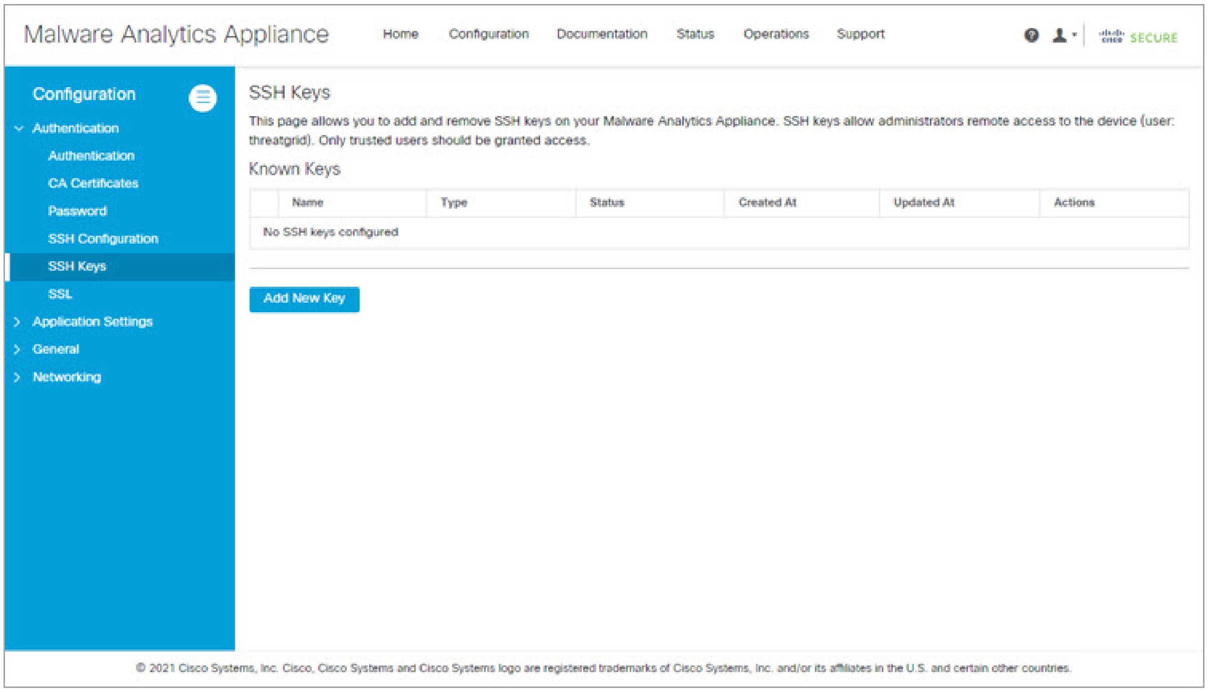
Note Configuring a SSH public key for access to the Secure Malware Analytics Appliances disables password-based authentication via SSH (v2.7.2 and later); this makes SSH authentication methods one or the other, not both. After a successful SSH connection using key-based authentication, the Admin TUI prompts for a password, such that both tokens are required.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose and choose **SSH Keys** to open the **SSH Keys** page.

Figure 20: SSH Keys



SSH Keys

This page allows you to add and remove SSH keys on your Malware Analytics Appliance. SSH keys allow administrators remote access to the device (user: threatgrid). Only trusted users should be granted access.

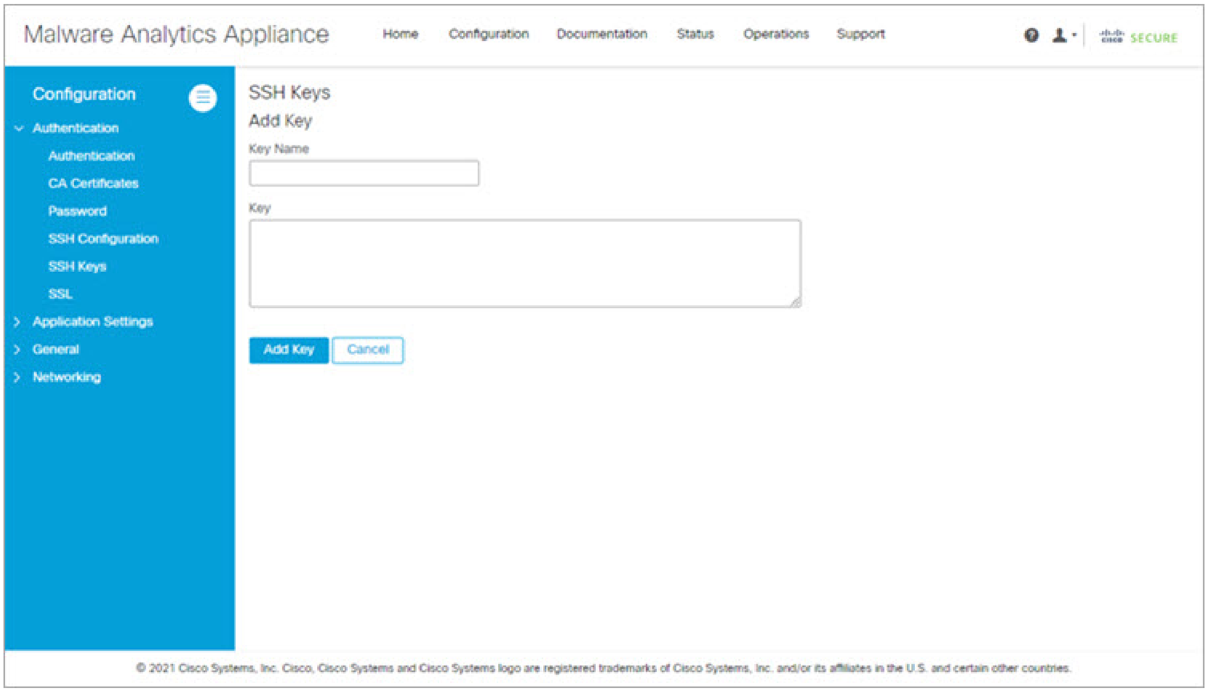
Known Keys

Name	Type	Status	Created At	Updated At	Actions
No SSH keys configured					

© 2021 Cisco Systems, 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 3 Click **Add New Key**.

Figure 21: Add Key



SSH Keys

Add Key

Key Name

Key

© 2021 Cisco Systems, 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 4 Enter the **Key Name** and paste the key into the **Key** field.

Step 5 Click **Add Key**.

SSL

All network traffic passing to and from the Secure Malware Analytics Appliance is encrypted using SSL. The following information is provided to assist you through the steps for setting up SSL certificates to support Secure Malware Analytics Appliance connections with Email Security Appliance (ESA), Web Security Appliance (WSA), Secure Endpoint Private Cloud, and other integrations.

Note A full description of how to administer SSL certificates is beyond the scope of this guide.

Interfaces Using SSL

There are two interfaces on the Secure Malware Analytics Appliance that use SSL:

- **Clean** interface for the Secure Malware Analytics Portal UI and API, and integrations (ESA, WSA, and Secure Endpoint Private Cloud Disposition Update Service).
- **Admin** interface for the Admin UI.

Supported SSL/TLS Version

The following versions of SSL/TLS are supported on the Secure Malware Analytics Appliance:

- TLS v1.0 - Disabled in the Admin interface (v2.7 and later)
- TLS v1.1 - Disabled in the Admin interface (v2.7 and later)
- TLS v1.2

Note TLS v1.0 and TLS v1.1 are disabled in the Admin interface (v2.7 and later), and disabled by default for the main application. If one of these protocols is required for integration compatibility purposes, they can be re-enabled (for the main application only) from tgsh.

Supported Customer-Provided CA Certificates

Customer-provided CA certificates are supported (v2.0.3 and later) to allow customers to import their own trusted certificates or CA certificates.

Self-Signed Default SSL Certificates

The Secure Malware Analytics Appliance is shipped with a set of self-signed SSL certificates and keys already installed. One set is for the Clean interface and the other is for the Admin interface. These SSL certificates can be replaced by an administrator.

The default Secure Malware Analytics Appliance SSL certificate hostname (Common Name) is the appliance serial number (with an additional subjectAltName field for the IP address), and is valid for 1 year. For releases prior to v2.11, the default SSL certificate hostname is **pandem**.

If a different hostname was assigned to the Secure Malware Analytics Appliance during configuration, the hostname and the Common Name in the certificate will no longer match.

The hostname in the certificate must also match the hostname expected by a connecting an ESA or WSA, or other integrating Cisco device or service, as many client applications require SSL certificates where the Common Name used in the certificate matches the hostname of the connecting appliance.

Configuring SSL Certificates

Cisco security products, such as ESA, WSA, and Secure Endpoint Private Clouds, can connect to a Secure Malware Analytics Appliance (inbound connection) and submit samples to it. To accomplish this, the connected appliance or other device must be able to trust the Secure Malware Analytics Appliance SSL certificate.

You must first validate that the hostname matches the Common Name; if it doesn't match, you must regenerate or replace it. You then must export the SSL certificate from the Secure Malware Analytics Appliance, and then import it into the connected appliance or device.

The certificates used for inbound SSL connections on the Secure Malware Analytics Appliance are configured on the **SSL Keys** page. The SSL certificates for the Clean and Admin interfaces can be configured independently.

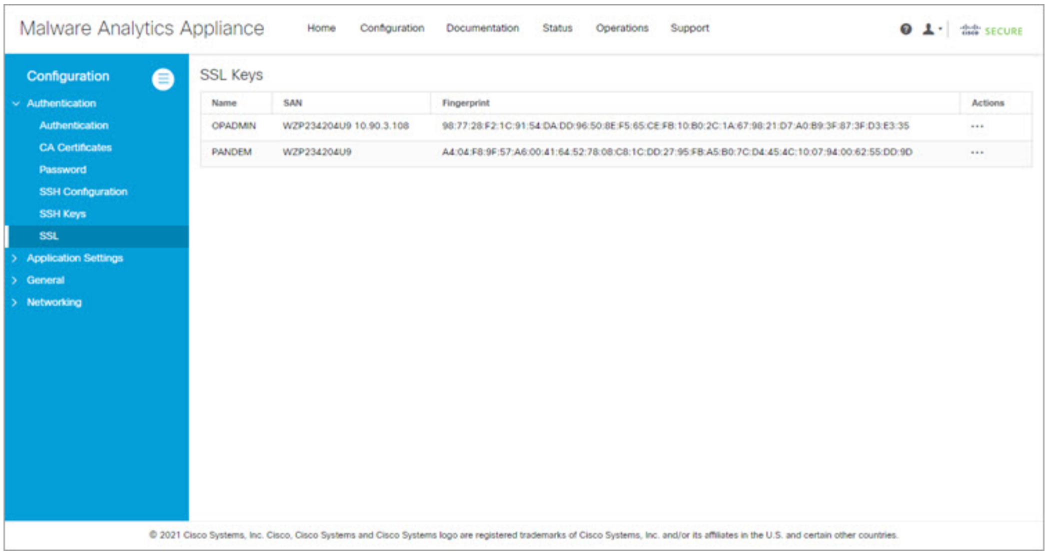
Note For information about outbound SSL connections so that the Secure Malware Analytics Appliance can trust the Cisco Secure Endpoint Private Cloud, see CA Certificates.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **SSL** to open the **SSL Keys** page.

Figure 22: SSL Keys Page



SSL Keys

Name	SAN	Fingerprint	Actions
OPADMIN	WZP234204U9 10.90.3.108	98:77:28:F2:1C:91:54:DA:DD:96:50:8E:F5:65:CE:FB:10:B0:2C:1A:67:98:21:D7:A0:B9:3F:87:3F:D3:E3:35	•••
PANDEM	WZP234204U9	A4:04:F8:9F:57:A6:00:41:64:52:78:08:C8:1C:DD:27:95:FB:A5:B0:7C:D4:45:4C:10:07:94:00:62:55:DD:9D	•••

© 2021 Cisco Systems, 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.

In this example, there are two SSL certificates: **OpAdmin** for the Admin interface, and **Pandem** for the Clean interface.

Step 3 Confirm that the hostname matches the SAN (Subject Alternative Name) used in the SSL. The hostname must match the SAN used in the SSL certificate on the Secure Malware Analytics Appliance. If they do not match, you can regenerate the SSL certificate. See Regenerating SSL Certificates.

Replacing SSL Certificates

SSL certificates usually need to be replaced at some point for various reasons, such as the certificate has expired, the hostname has changed, or to support integrations with other Cisco devices and services.

Cisco ESA, WSA, and other CSA Cisco integrating devices may require an SSL certificate in which the Common Name matches the Secure Malware Analytics appliance hostname. You must replace the default SSL certificate with a newly generated certificate that uses the same hostname to access the Secure Malware Analytics Appliance.

If integrating a Secure Malware Analytics Appliance with an Secure Endpoint Private Cloud to use its Disposition Update Service, you must install the Secure Endpoint Private Cloud SSL Certificate so the Secure Malware Analytics Appliance can trust the connection.

There are several ways to replace an SSL certificate on a Secure Malware Analytics Appliance:

- Regenerating SSL Certificates that uses the current hostname for the SAN.
- Downloading SSL Certificates
- Uploading SSL Certificates; this can be a commercial or enterprise SSL, or one you create using OpenSSL.
- Generating SSL Certificates Using OpenSSL

Regenerating SSL Certificates

You can regenerate a SSL certificate on the **SSL Keys** page if your hostname does not match the SAN in the certificate.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **SSL** to open the **SSL Keys** page.

Step 3 In the **Actions** column, click the (**...**) menu and choose **Regenerate** for the interface that needs a new certificate.

A new self-signed SSL certificate is generated on the Secure Malware Analytics Appliance that uses the current hostname of the appliance in the SAN field of the certificate. The regenerated certificate (.cert file) can be downloaded and installed on the integrating appliance.

Downloading SSL Certificate

The Secure Malware Analytics generated SSL certificates, but not the keys, can be downloaded. A downloaded certificate can be used when setting up a cluster. It can also be installed on integrating devices so they can trust connections from the Secure Malware Analytics appliance. (You will only need to .cert file for this step.)

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **SSL** to open the **SSL Keys** page.

Step 3 From **Actions** (**...**) menu, choose **Download** for the appropriate interface. The SSL Certificate is downloaded.

Uploading SSL Certificates

If you already have a commercial or corporate SSL certificate in place for your organization, you can use that to generate a new SSL certificate for the Secure Malware Analytics Appliance and use the CA cert on the integrating device.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Authentication** in the side navigation and choose **SSL** to open the **SSL Keys** page.

Step 3 In the **Actions** column, click the (**...**) menu and choose **Upload** for the appropriate interface. The **Upload SSL Certificate** page opens.

Step 4 Complete the **Certificate** and **Private Keys** fields and then click **Add Certificate**.

Generating SSL Certificates Using OpenSSL

OpenSSL is a standard open-source SSL tool for creating and managing OpenSSL certificates, keys, and other files. You can manually generate a SSL certificate using OpenSSL when there is no SSL certificate infrastructure already in place on your premises and upload it to the Secure Malware Analytics Appliance (as described in Uploading SSL Certificates). .

Note OpenSSL is not a Cisco product, therefore Cisco does not provide technical support for it. It is recommended that you search the Web for additional information on using OpenSSL. Cisco does offer a SSL library, *Cisco SSL*, for generating SSL certificates.

Procedure

Step 1 Run the following command to generate a new self-signed SSL certificate:

Note
The following example still uses the CN (Common Name) instead of the more contemporary SAN (Subject Alternative Name).

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout tgapp.key -nodes -out
tgapp.cert -subj "/C=US/ST=New York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

openssl - OpenSSL

req - Specifies to use X.509 certificate signing request (CSR) management. X.509 is a public key infrastructure standard that SSL and TLS use for key and certificate management. In this example, this parameter is used to create a new X.509 cert.

-x509 - This modifies the req parameter X.509 to make a self-signed certificate instead of generating a certificate signing request.

-days 3650 - This option sets the length of time for which the certificate will be considered valid. In this example, it is set for 10 years.

-newkey rsa:4096 - This specifies to generate a new certificate and a new key at the same time. Because the required key was not previously created, it must be created with the certificate. The **rsa:4096** parameter indicates to make an RSA key that is 4096 bits long.

-keyout - This parameter indicates where OpenSSl should save the generated private key file that is being created.

-nodes - This parameter indicates that OpenSSL should skip the option to secure the certificate with a passphrase. The appliance needs to be able to read the file, without user intervention, when the server starts up. A certificate that is secured with a passphrase requires that the user enter the passphrase every time the server is restarted.

-out - This parameter indicates where OpenSSL should save the certificate that is being created.

-subj: (Example):

- **C=US** - Country
- **ST=New York** - State
- **L=Brooklyn** - Location
- **O=Acme Co** - Owner's name

- **CN=tgapp.acmeco.com** - Enter the Secure Malware Analytics Appliance FQDN (Fully Qualified Domain Name). This includes the HOSTNAME of the Secure Malware Analytics Appliance (in this example, **tgapp**) and the associated domain name (in this example, **acmeco.com**).

  Important
  You must at least change the Common Name to match the FQDN of the Secure Malware Analytics Appliance Clean interface.

Step 2 Once the new SSL certificate is generated, upload the certificate to the Secure Malware Analytics Appliance from the **SSL Keys** page (see Uploading SSL Certificates). You must also upload the certificate (**.cert** file only) to the Email Security Appliance or Web Security Appliance, if you are integrated with those devices.

Application Settings

The Secure Malware Analytics Appliance application settings are configured in this panel.

Integrations

Integrations with several third-party detection and enrichment services, including TitaniumCloud, Umbrella (OpenDNS), and VirusTotal, can be configured on the appliance using the **Integrations** page.

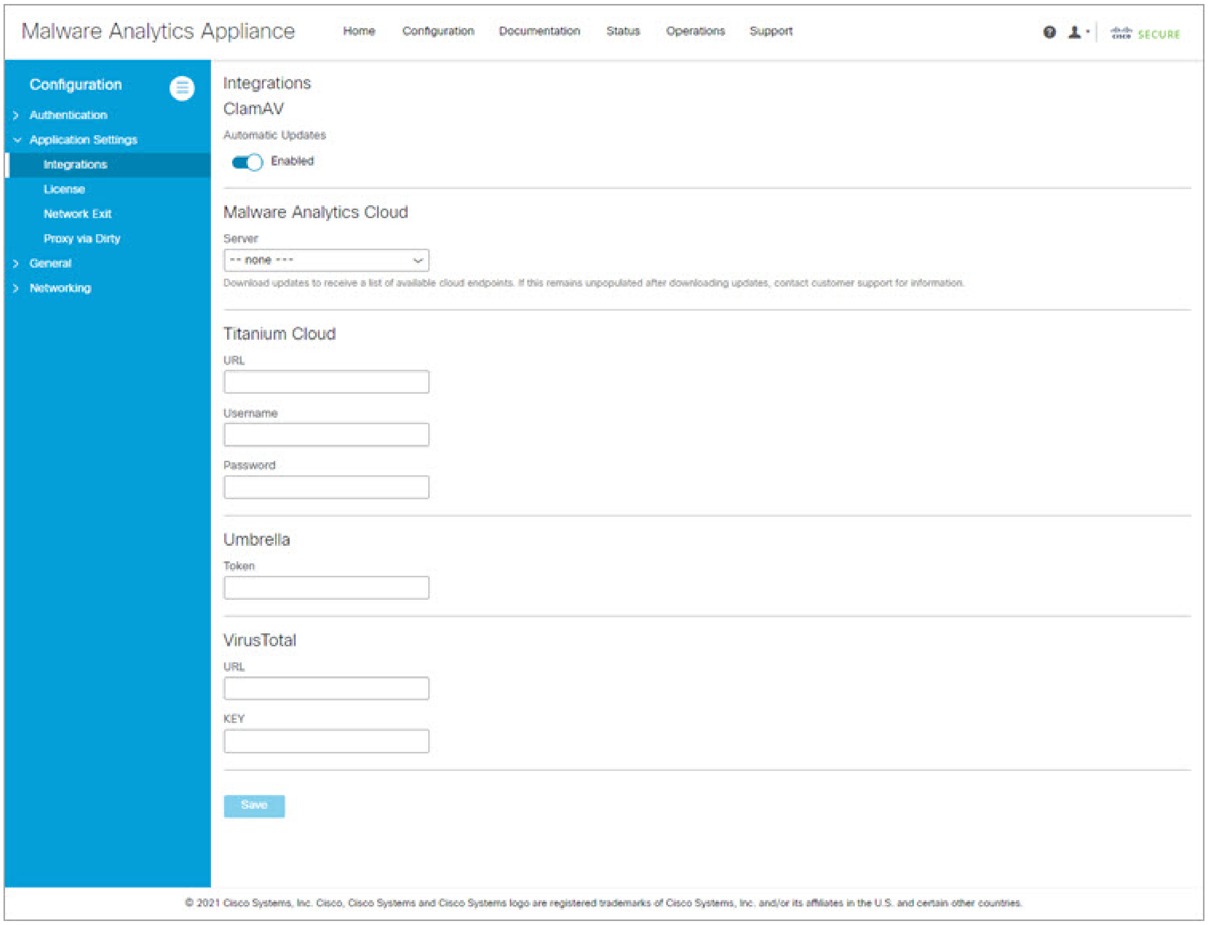
The Cloud Search Federation feature (available in v2.8 and later), provides users with an option in the Secure Malware Analytics portal UI to rerun a search query against the Secure Malware Analytics cloud instance, if a cloud endpoint is configured as described below.

Note If Umbrella (OpenDNS) is not configured, the **whois** information on the Domains entity page in the analysis report (Cloud UI) will not be rendered.

Procedure

Step 1 Navigate to **Configuration** > **Application Settings** > **Integrations**.

Figure 23: Integrations Configuration Page



Integrations

ClamAV

Automatic Updates

● Enabled

Malware Analytics Cloud

Server

-- none ---

Download updates to receive a list of available cloud endpoints. If this remains unpopulated after downloading updates, contact customer support for information.

Titanium Cloud

URL

Username

Password

Umbrella

Token

VirusTotal

URL

KEY

© 2021 Cisco Systems, 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.

Integrations screen appears.

Step 2 Enter the credentials required for each integration.

Note

ClamAV signatures can be automatically updated on a daily basis, and is enabled by default. Enabling ClamAV signatures in malware analysis allows you to detect known malware using ClamAV's database of virus signatures. You can disable the **Automatic Updates** setting in the **ClaimAV** section.

Titanium Cloud (ReversingLabs TitaniumCloud^{TM})

Use the TitaniumCloud Integration Malware Analysis Platform to increase detection, analysis, and response efficiency by identifying files with its global goodware and malware database of over 6 billion files.

To configure an integration with TitaniumCloud, you will need :

a. **URL:** Titanium Cloud URL.

b. **Username:** Username of you TitaniumCloud account.

c. **Password:** Password of you TitaniumCloud account.

Umbrella (Cisco - previously named OpenDNS)

Integrating Umbrella with your existing security infrastructure can help improve malware detection by blocking malicious domains and IPs at the DNS layer, providing real-time threat intelligence, and integrating with other security tools. This can help prevent malware from even connecting to command and control servers or downloading malicious payloads, even if the user clicks on a malicious link or opens an infected attachment. To configure an integration with Umbrella, you can navigate to Admin in the Umbrella portal to get the **Token**.

Note
You need Tier2 or Tier3 Investigate license for the Umbrella integration.

VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and detects viruses, worms, trojans, and all kinds of malware. It integrates easily with Security Operations. Integrating VirusTotal into your security infrastructure can improve malware detection by providing access to a large and comprehensive malware database, the ability to detect new and emerging malware, and the ability to analyze suspicious URLs and files in a sandbox. Before you can use the VirusTotal integration, you must activate the plugin, provide the URL of the activated instance along with the appropriate API key.

Step 3 Click **Save**.

License

When a new appliance is purchased, a license is generated and the **Retrieve License From Server** button on the **Configuration > License** page is enabled. However, if that doesn't work or if there's a special case (such as a license being a custom one-off), then you will be given the license directly, as an encrypted file with a password.

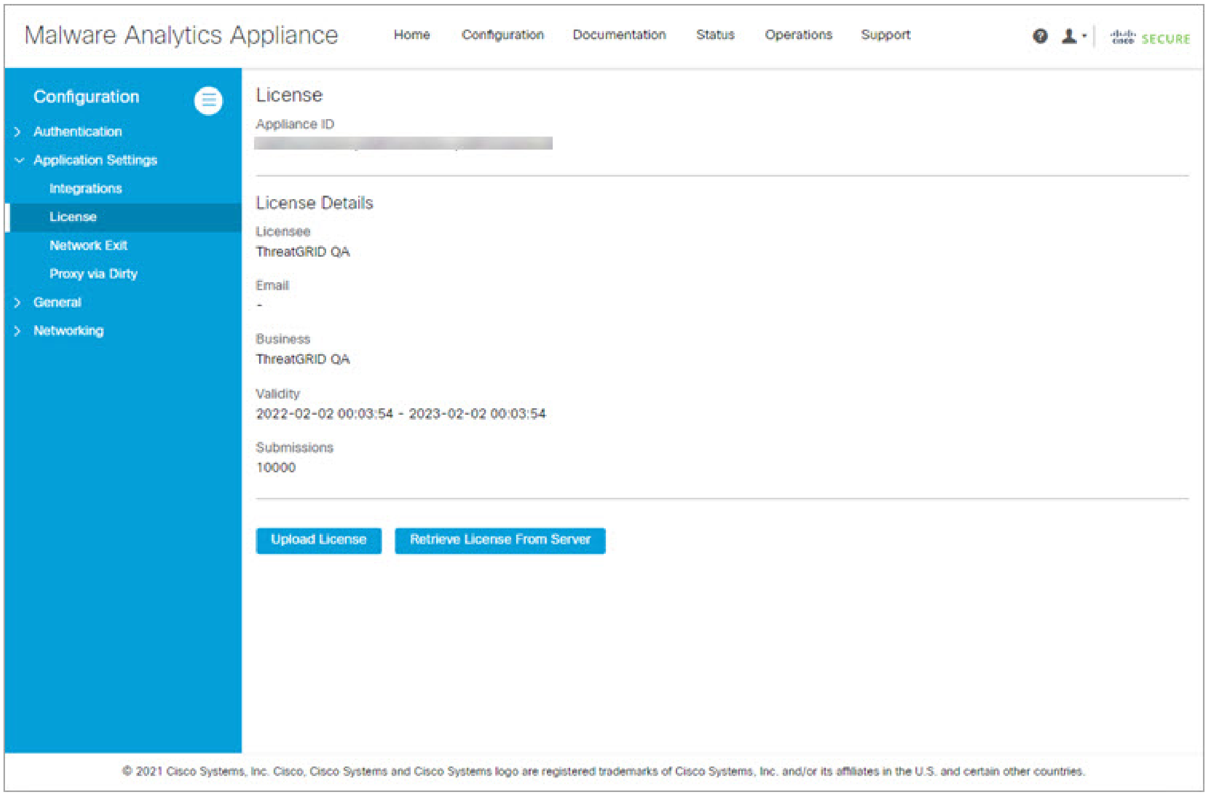
You can view or update your license information using the **License** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Application Settings** in the side navigation and choose **License** to open the **License** page.

Figure 24: License Page



License

Appliance ID

[redacted]

License Details

Licensee

ThreatGRID QA

Email

-

Business

ThreatGRID QA

Validity

2022-02-02 00:03:54 - 2023-02-02 00:03:54

Submissions

10000

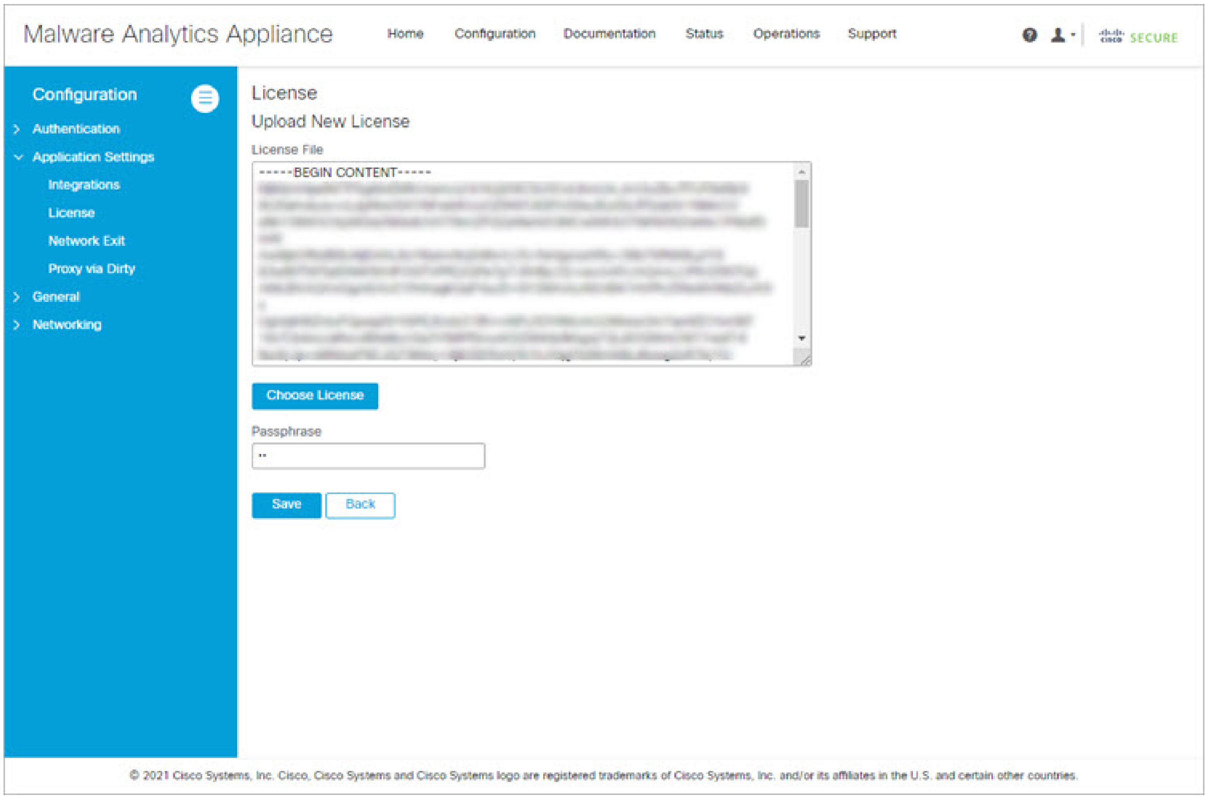
© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Step 3 Upload the license or retrieve it from the server. Typically, you must upload the license for air-gapped appliances.

To Upload License:

a) Click **Upload License** to open the **Upload New License** page.

Figure 25: Upload License



b) Click **Choose License** to open the **File Manager**, choose the license file you received from Secure Malware Analytics (the file has .lic extension), and click **Open**.

The contents of the license are added to the **License File** field.

c) Enter the password that Secure Malware Analytics provided (with the .lic file) in the **Passphrase** field and click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

To Retrieve License from Server:

a) Click **Retrieve License From Server** to retrieve and add the license.
b) Click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

Network Exit

Geographic location is often an important issue for malware analysis. Some types of malware behave differently depending on geographic location, while other types may target a specific area. Similar in concept to VPN, the **Network Exits** mode (available in v2.4.3 and later) makes any outgoing network that is generated during sample analysis appear to exit from that location. Configuration files are automatically distributed and there is no need for support staff to manually install or update them.

Note **tg-tunnel and v2.4.3:** If you were previously using tg-tunnel, you must allow outbound traffic to specific IP addresses and ports required for Network Exit before installing v2.4.3; otherwise, that traffic only needs to be permitted before enabling remote exit use. The required IP addresses and ports change occasionally. See Required IP and Ports for Threat Grid for the most recent list.

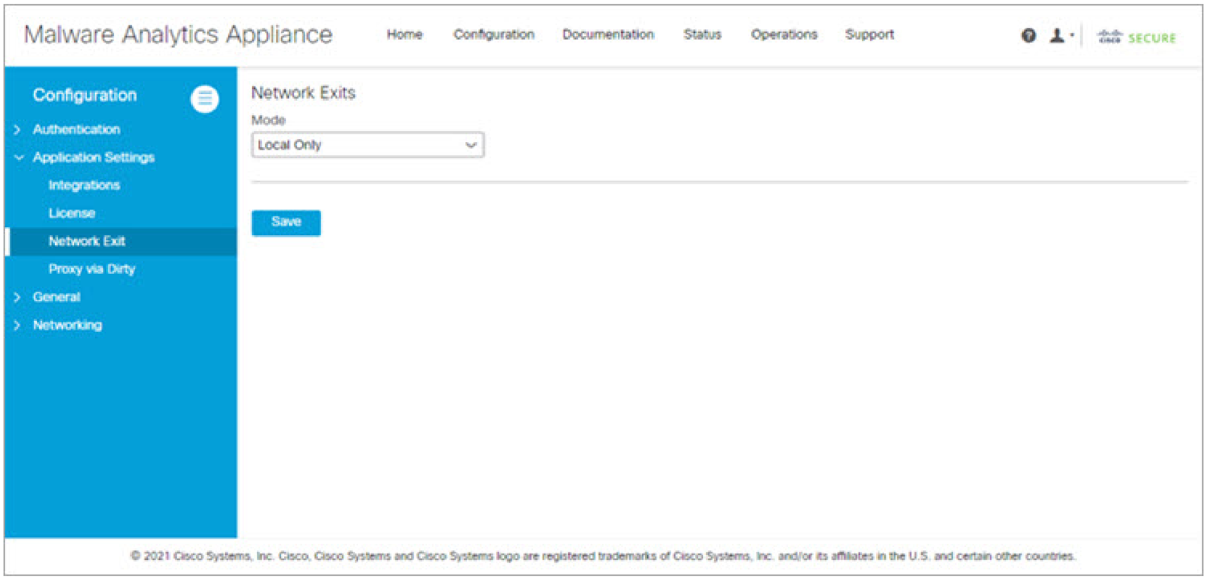
Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Application Settings** in the side navigation and choose **Network Exit** to open the **Network Exits** configuration page.

The setting on this page determines the **Network Exit** options that will be available in the Secure Malware Analytics portal when submitting samples for analysis.

Figure 26: Network Exits Configuration



Network Exits

Mode

Local Only

© 2021 Cisco Systems, 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.

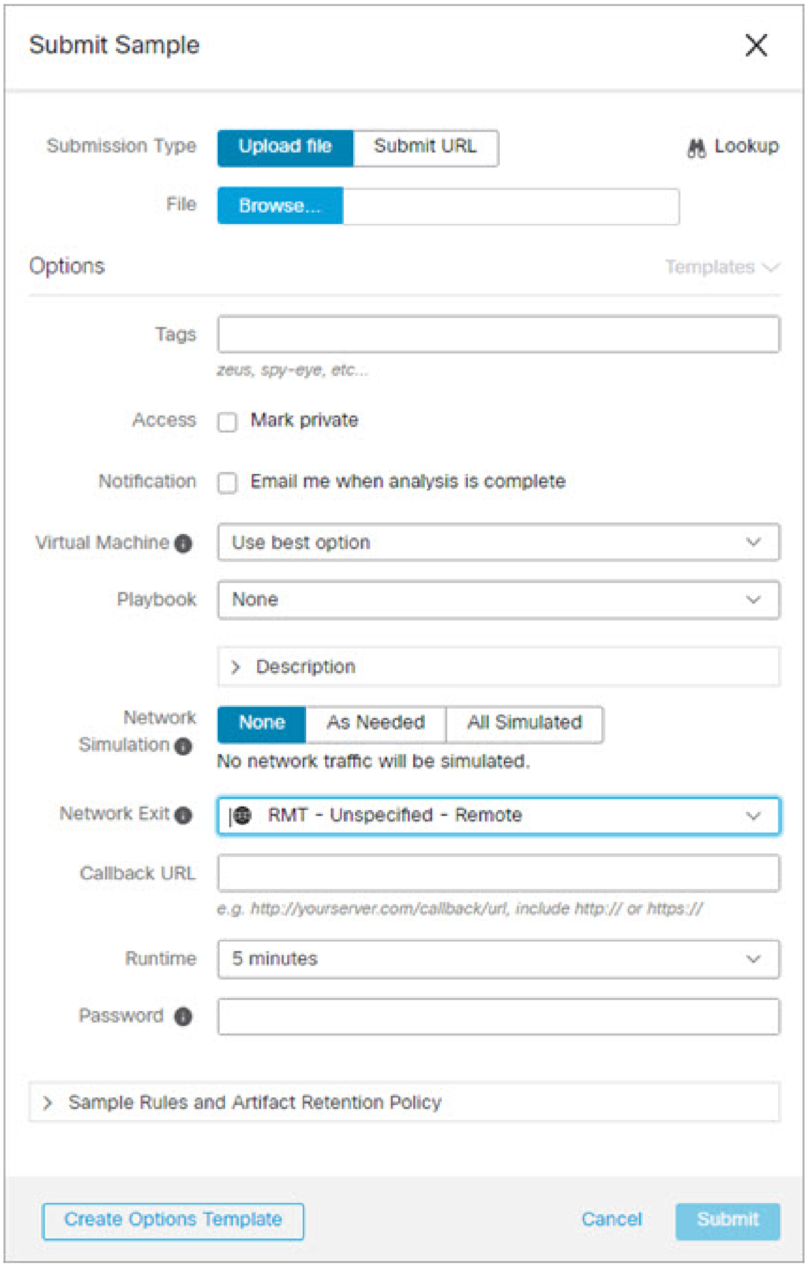
Step 3 From the Mode drop-down list, choose **Local Only**, **Remote Only**, **Both Local and Remote**, or **Simulation Only**.

If you choose **Local Only** or **Remote Only**, the application makes only those options available to users; if you choose **Both Local and Remote**, both options will be available to users.

If you choose **Simulation Only**, the API and UI users cannot choose any option to send network traffic from virtual machines to destinations outside of the local Secure Malware Analytics Appliance.

Accessing private networks, even for DNS lookup, is not allowed even for Network Exit. All malware traffic comes out of the Dirty interface, using the Dirty DNS server configured.

Figure 27: Submit Sample



Submit Sample

Submission Type: Upload file | Submit URL — Lookup

File: Browse...

Options — Templates

Tags: zeus, spy-eye, etc...

Access: □ Mark private

Notification: □ Email me when analysis is complete

Virtual Machine: Use best option

Playbook: None

Description

Network Simulation: None | As Needed | All Simulated

No network traffic will be simulated.

Network Exit: RMT - Unspecified - Remote

Callback URL: e.g. http://yourserver.com/callback/url, include http:// or https://

Runtime: 5 minutes

Password:

Sample Rules and Artifact Retention Policy

Create Options Template — Cancel — Submit

Note

Sometimes it may be necessary to simulate network connections during analysis. Network simulation provides analysts with a way to present network resources to malware samples that may otherwise be unavailable, and for other reasons. For example, you may want to choose a network simulation option to simulate network connections when the upstream servers are not accessible; when they have been taken down; when their DNS records are gone; or if other restrictions on outbound connectivity apply in order to improve sample execution and convictions.

In addition, network simulation can provide at least some connectivity to air-gapped appliances and improve sample execution on them.

The **Network Simulation** option for sample analysis is available on Secure Malware Analytics Appliances v2.7.1 and later. See the Secure Malware Analytics portal UI online help topic for additional information.

Updates Proxy

SOCK5 is an Internet protocol that exchanges network packets between a client and server through a proxy server. If the appliance's dirty interface cannot reach update servers. SOCKS5 proxy is configured to download the updates.

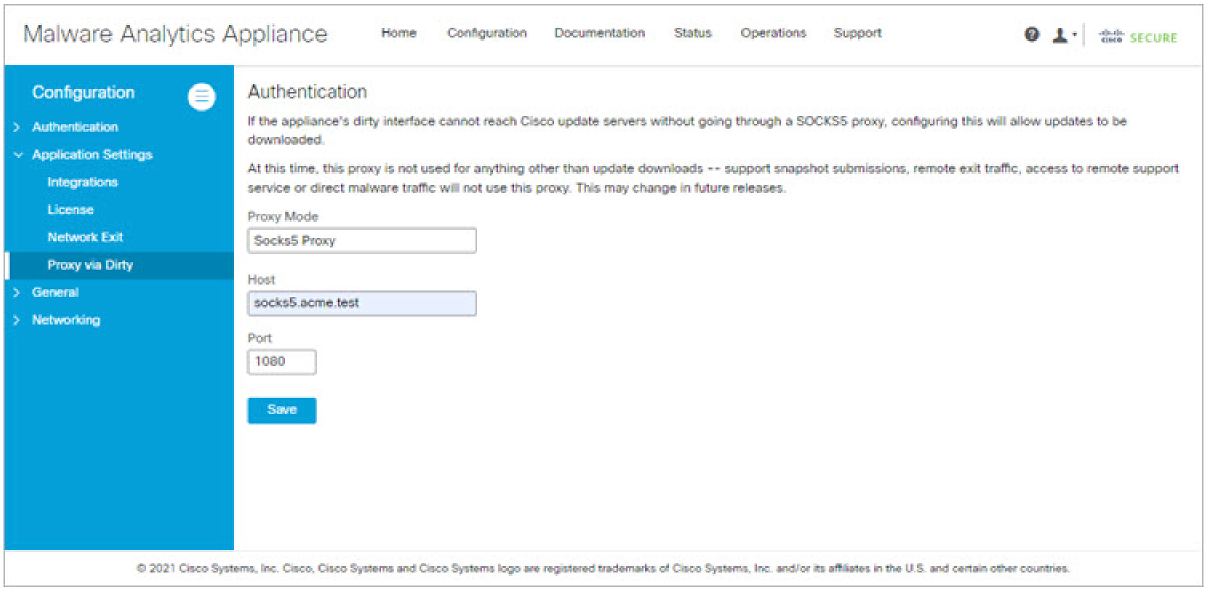
Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Application Settings** in the side navigation and choose **Proxy via Dirty** to open the **Authentication** configuration page.

The setting on this page determines the **Updates proxy** options that will be used to download the updates.

Figure 28: Updates Proxy Configuration



Authentication

If the appliance's dirty interface cannot reach Cisco update servers without going through a SOCKS5 proxy, configuring this will allow updates to be downloaded.

At this time, this proxy is not used for anything other than update downloads -- support snapshot submissions, remote exit traffic, access to remote support service or direct malware traffic will not use this proxy. This may change in future releases.

Proxy Mode: Socks5 Proxy

Host: socks5.acme.test

Port: 1080

© 2021 Cisco Systems, 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 3 From the **Proxy Mode** drop-down list, choose **Socks5 Proxy**.

Step 4 Enter the host in the **Host** field.

Step 5 Enter the port in the **Port** field.

General

The Secure Malware Analytics Appliance general configuration settings are under the General side navigation.

Content Update

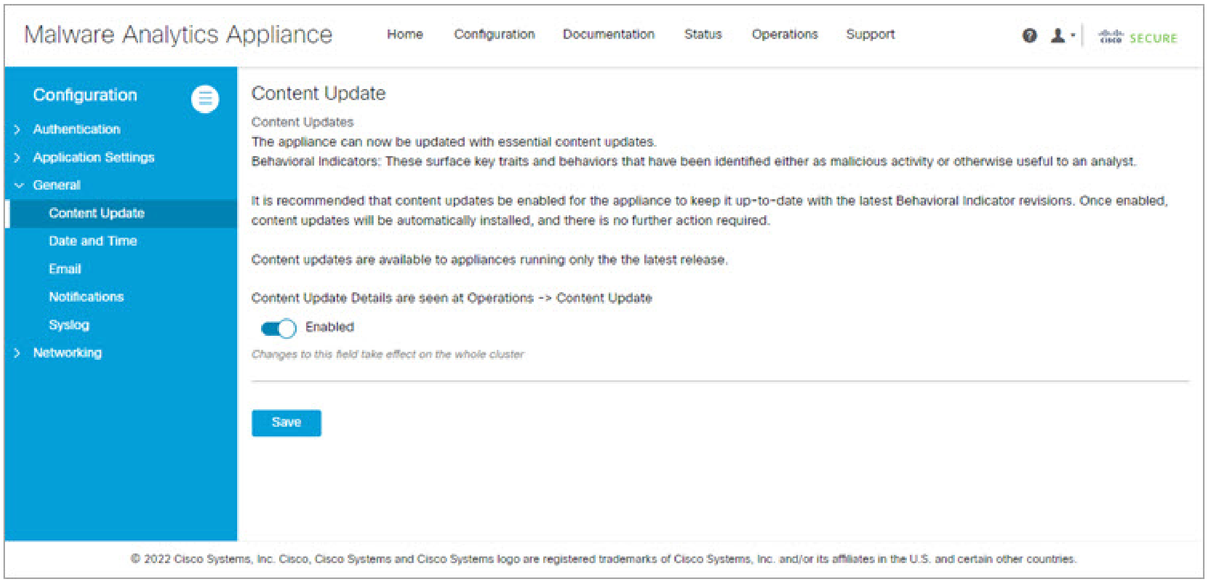
Content Update allows your appliance to receive the latest behavioral indicators automatically while updating the appliances. In order to receive the BIs automatically, you need to toggle the Content Update switch in the **Enabled** position. To enable Content Update, do the following:

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and and choose **Content Update** to open the **Content Update** page.

Figure 29: Content Update



Content Update

Content Updates

The appliance can now be updated with essential content updates.

Behavioral Indicators: These surface key traits and behaviors that have been identified either as malicious activity or otherwise useful to an analyst.

It is recommended that content updates be enabled for the appliance to keep it up-to-date with the latest Behavioral Indicator revisions. Once enabled, content updates will be automatically installed, and there is no further action required.

Content updates are available to appliances running only the the latest release.

Content Update Details are seen at Operations -> Content Update

Enabled

Changes to this field take effect on the whole cluster

© 2022 Cisco Systems, 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.

Note
When you enable the Content Update, it updates all the appliances in the cluster.

Step 3 Toggle the switch from **Disabled** to **Enabled** position.

Note
When enabled, Content Updates are downloaded and applied during the nightly appliance update check.

Step 4 Click **Save**.

Date and Time

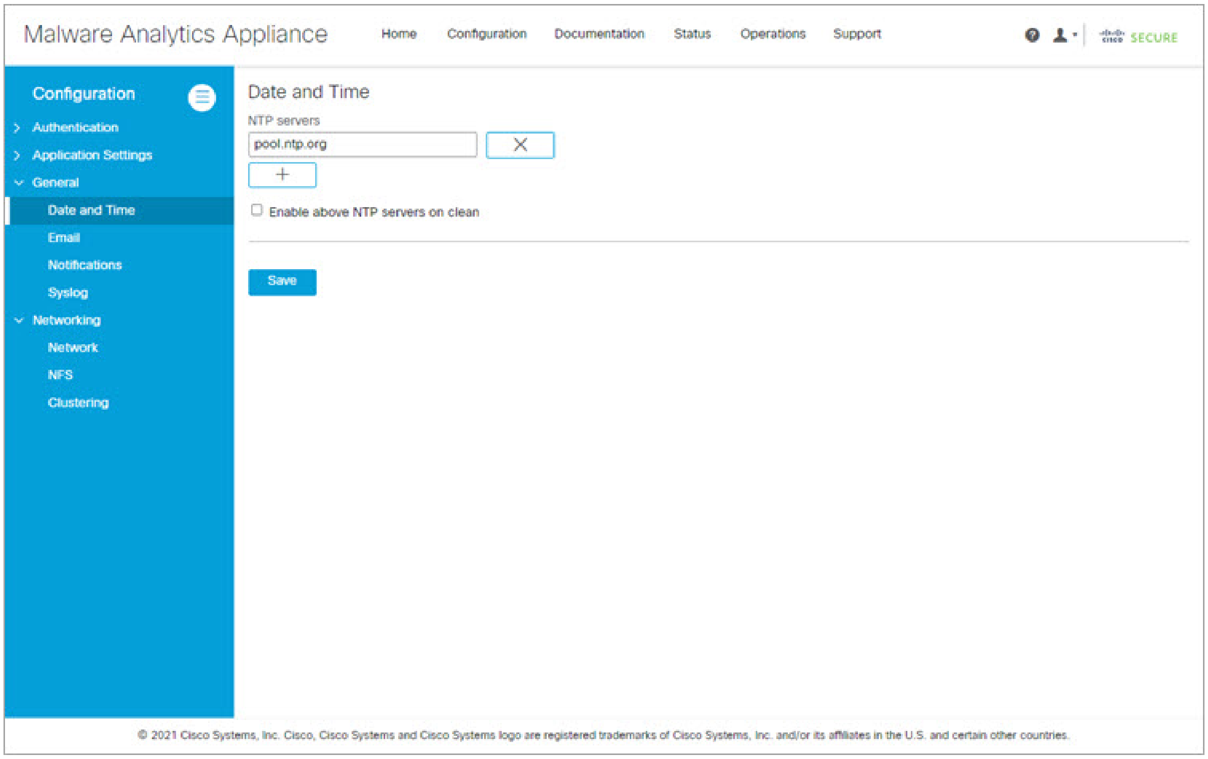
When you initially set up the Secure Malware Analytics Appliance, you specify the Network Time Protocol (NTP) servers to configure the date and time. You can add or delete NTP servers using the **Date and Time** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and and choose **Date and Time** to open the **Date and Time** page.

Figure 30: Date and Time



Date and Time

NTP servers

pool.ntp.org

□ Enable above NTP servers on clean

© 2021 Cisco Systems, 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 3 Add or remove NTP Server(s):

- Click the + icon to add another field and enter the NTP server name or IP address; repeat as needed.
- Click the **x** icon to remove a server.

Step 4 Click **Save**.

Email

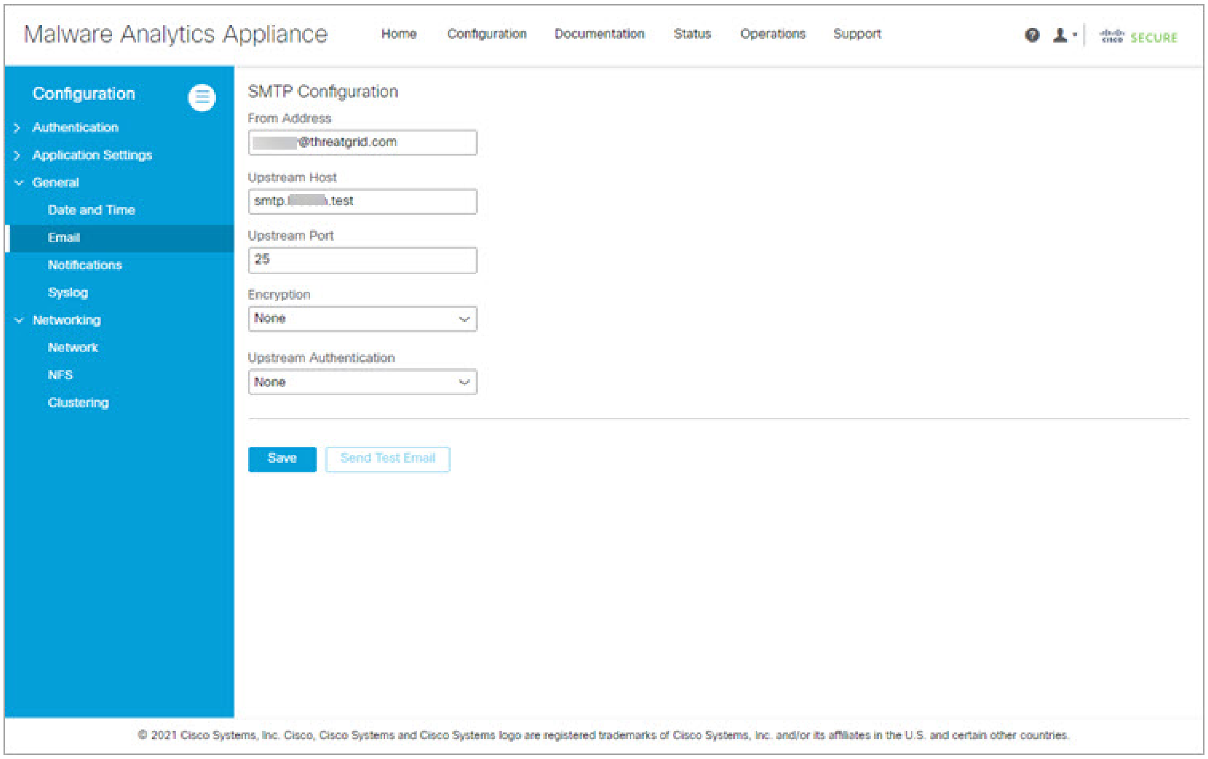
When you initially set up the Secure Malware Analytics Appliance, you configure your email settings. You can modify these settings on the **Email** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and choose **Email** to open the **SMTP Configuration** page.

Figure 31: SMTP Configuration


Malware Analytics Appliance
Home
Configuration
Documentation
Status
Operations
Support
SECURE
Configuration
Authentication
Application Settings
General
Date and Time
Email
Notifications
Syslog
Networking
Network
NFS
Clustering
Save
Send Test Email
© 2021 Cisco Systems, 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.

SMTP Configuration

From Address: [redacted]@threatgrid.com

Upstream Host: smtp.[redacted].test

Upstream Port: 25

Encryption: None

Upstream Authentication: None

Step 3 Make your modifications and click **Save**.

An alert indicating that a reconfiguration is required is displayed. See Applying Configuration Changes.

Step 4 Click **Send Test Email** to test the SMTP configurations.

Notifications

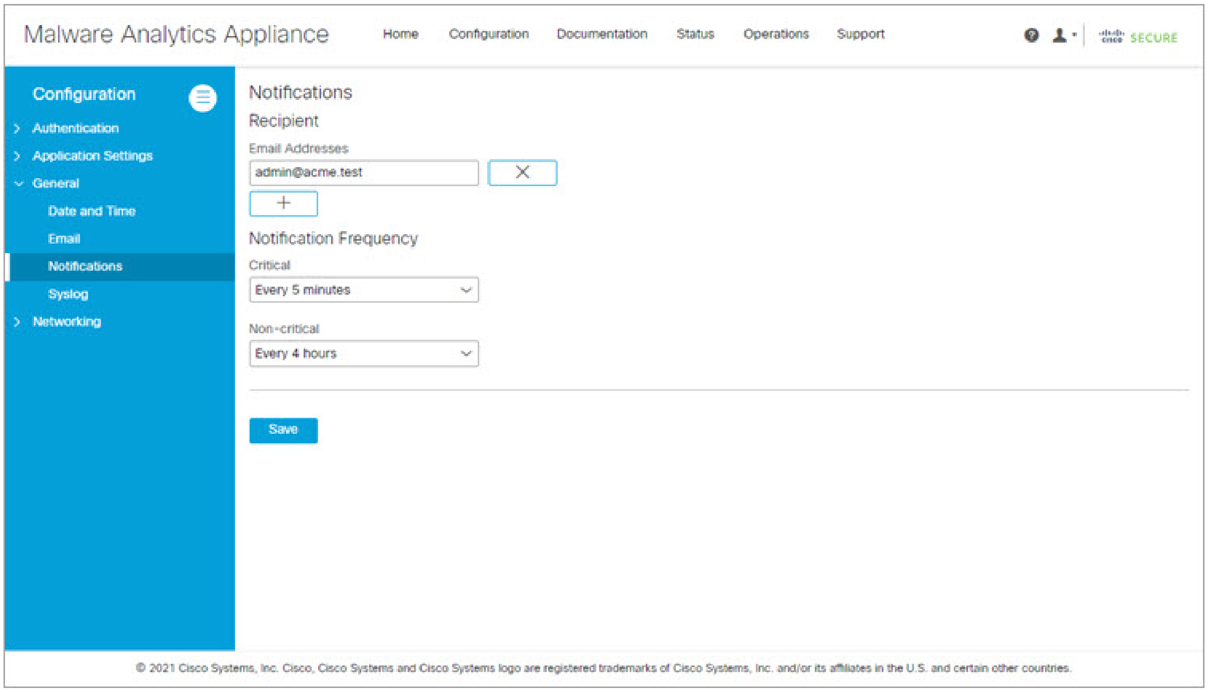
When you initially set up the Secure Malware Analytics Appliance, you configure the notifications to be received via email. You can add or delete recipients, and change the notification frequency using the **Notifications** page.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and choose **Notifications** to open the **Notifications** page.

Figure 32: Notifications


Malware Analytics Appliance
Home
Configuration
Documentation
Status
Operations
Support
SECURE
Configuration
Authentication
Application Settings
General
Date and Time
Email
Notifications
Syslog
Networking
Notifications
Recipient
Notification Frequency
Save
© 2021 Cisco Systems, 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.

Email Addresses: admin@acme.test

Critical: Every 5 minutes

Non-critical: Every 4 hours

Step 3 Under **Recipients**, enter the **Email Address** for at least one notifications recipient. If you need to add multiple email addresses, click the **+** icon to add another field; repeat as needed.

Step 4 Under **Notification Frequency**, choose the settings for **Critical** and **Non-critical** from the drop-down lists.

Step 5 Click **Save**.

Syslog

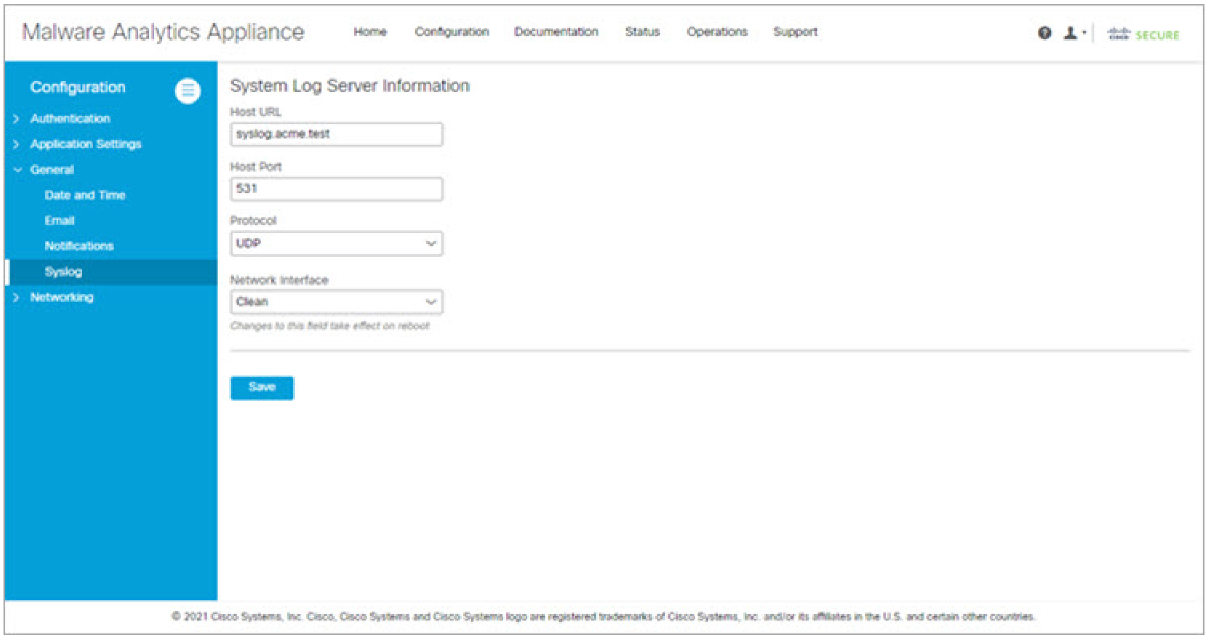
The **System Log Server Information** page is used to configure a system log server to receive syslog messages and Thread Grid notifications.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **General** in the side navigation and choose **Syslog** to open the the **System Log Server Information** page.

Figure 33: System Log Server Information



System Log Server Information

Host URL: syslog.acme.test

Host Port: 531

Protocol: UDP

Network Interface: Clean

Changes to this field take effect on reboot

© 2021 Cisco Systems, 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 3 Complete the fields on the page:

- **Host URL** - Enter the host name or URL for the system log server.
- **Host Port** - Enter the port number for the server.
- **Protocol** - Choose **TCP** or **UDP** from the drop-down list.

Step 4 Click **Save**.

Networking

The Secure Malware Analytics Appliance network configuration settings are under the Networking side navigation.

Network

If you used DHCP for the initial configuration, and you need to adjust the IP assignment from DHCP to your permanent static IP addresses for all three networks, perform the following steps.

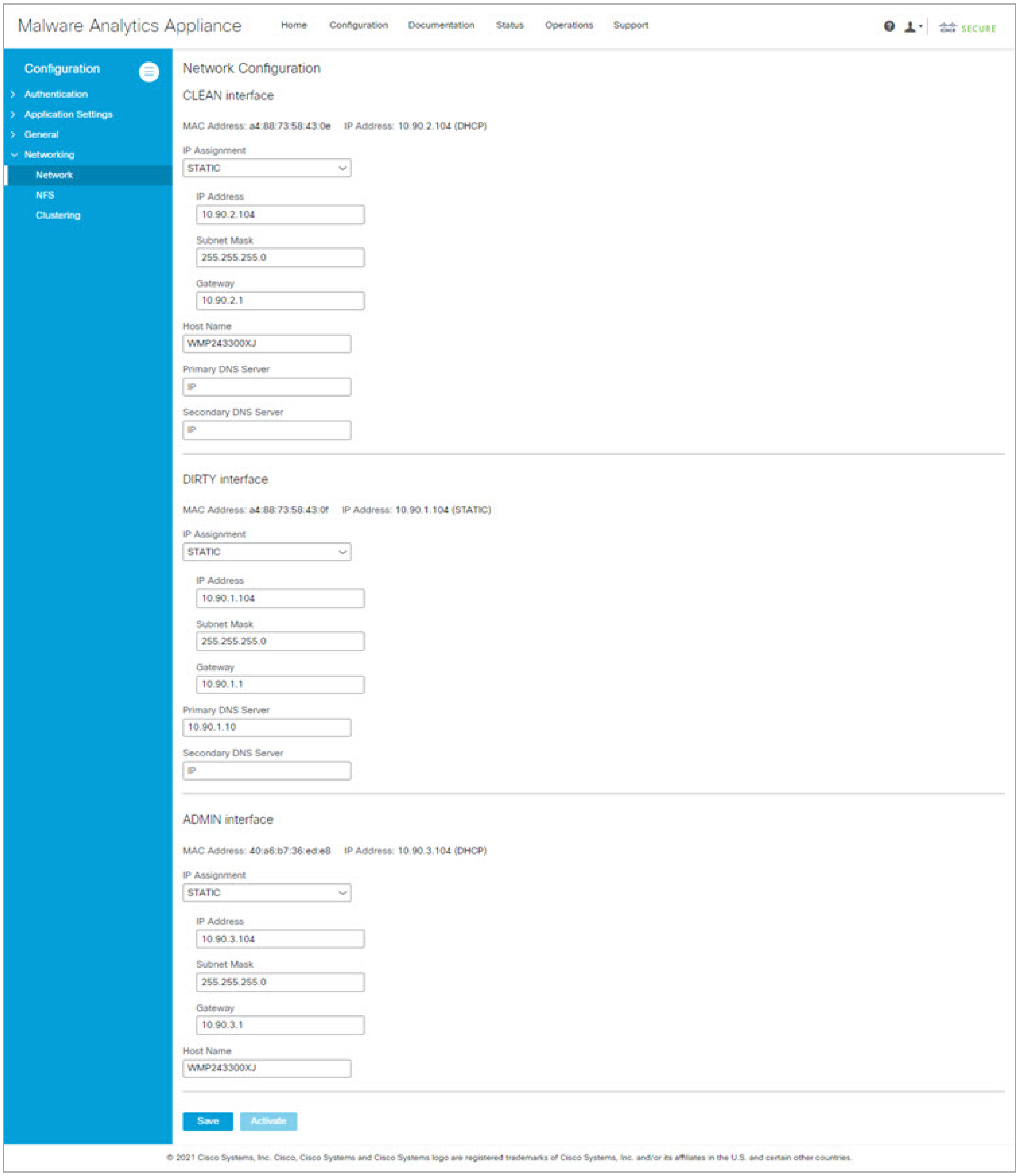
Note The Admin UI does not validate the gateway entries. If you enter the wrong gateway and save it, the Admin UI will not be accessible. You will need to use the console to fix the networking configuration if that was done on the admin interface. If Admin is still valid, you can fix it in the Admin UI and reboot.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Networking** in the side navigation and choose **Network** to open the **Network Configuration** page.

Figure 34: Network Configuration



Network Configuration

CLEAN interface

MAC Address: a4:88:73:58:43:0e IP Address: 10.90.2.104 (DHCP)

IP Assignment: STATIC

IP Address: 10.90.2.104

Subnet Mask: 255.255.255.0

Gateway: 10.90.2.1

Host Name: WMP243300XJ

Primary DNS Server: IP

Secondary DNS Server: IP

DIRTY interface

MAC Address: a4:88:73:58:43:0f IP Address: 10.90.1.104 (STATIC)

IP Assignment: STATIC

IP Address: 10.90.1.104

Subnet Mask: 255.255.255.0

Gateway: 10.90.1.1

Primary DNS Server: 10.90.1.10

Secondary DNS Server: IP

ADMIN interface

MAC Address: 40:a6:b7:36:ed:e8 IP Address: 10.90.3.104 (DHCP)

IP Assignment: STATIC

IP Address: 10.90.3.104

Subnet Mask: 255.255.255.0

Gateway: 10.90.3.1

Host Name: WMP243300XJ

© 2021 Cisco Systems, 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 3 Complete the following fields:

Note

The Admin network settings were configured using the Admin TUI during the initial Secure Malware Analytics Appliance setup and configuration.

- **IP Assignment** - Choose **Static** from the drop-down lists for all three interfaces (Clean, Dirty, and Admin).
- **IP Address** - Enter a static IP address for the Clean or Dirty network interface.
- **Subnet Mask and Gateway** - Complete as appropriate for the type of network interface.
- **Host Name** - Enter the host name for server.
- **Primary DNS Server** - Enter the primary DNS server address.
- **Secondary DNS Server** - Enter the secondary DNS server information.

Note
ADMIN Interface: Select **DISABLED** for **IP Assignment** to reroute the traffic from *Admin* to go through *CLEAN*.

Step 4 Click **Save** to save your network configuration settings, and then click **Activate**.

A message is displayed indicating that reconfiguration is required (see Applying Configuration Changes).

Configuring DNS

By default, DNS uses the Dirty interface. If the hostname of an integrating appliance or service, such as Secure Endpoint Private Cloud, cannot be resolved over the Dirty interface because the Clean interface is used for the integration, a separate DNS server that uses the Clean interface can be configured in the Admin UI.

Procedure

Step 1 Click the **Configuration** tab.

Step 2 Expand **Networking** in the side navigation and choose **Network** to open the **Network Configuration** page.

Step 3 Complete the **DNS** fields for the Dirty and Clean networks.

Step 4 Click **Save**.

NFS

The Secure Malware Analytics Appliance (v2.2.4 or later) supports encrypted backups to NFS-backed storage, initialization of data from such storage, and reset to an empty-database state into which such a backup can be loaded.

Note Reset is different from the Wipe Appliance process; it is used to allow an appliance to be shipped off customer premises without information leakage, and is for backup preparation. The wipe process appropriate for that purpose already exists in the recovery bootloader, but is not suitable for preparing a system to restore a backup.

Content is encrypted with gocryptfs, a third-party open source product.

Note Filename encryption is disabled for performance reasons. Samples and other content in Secure Malware Analytics are not stored with their original names under any circumstances so this does not leak customer-owned data.

We strongly encourage consulting the documentation prior to use. Extended documentation regarding the backup functionality is available, and we strongly encourage consulting it prior to use. For additional technical information and instructions see the *Secure Malware Analytics Appliance Backup Notes and FAQ*.

NFS Requirements

The following NFS requirements must be met for encrypted backups to NFS-backed storage:

- Must be running the NFSv4 protocol over TCP, accessible from the Secure Malware Analytics Appliance admin interface.
- Only root user (UID 0) is allowed to mount. Make sure that UID 0 is allowed while mounting.Windows NFS admins should have users with UID 0 that will be able to write to that location.

  Note For Linux servers, it does not matter as *root_squash* is available by default. But in strict environments *no_root_squash* can be added.

- Configured directory must be writable by **nfsnobody** (UID 65534).
  - Exposing files for write by **nfsnobody** is secure. The only processes on the Secure Malware Analytics Appliance running as **nfsnobody** or with write to **nfsnobody**, are those responsible for encryption of data. Plain text data is exposed under distinct user accounts for different subtrees according to principal of least privilege; the PostgreSQL service on the appliance cannot access Elasticsearch data or the freezer; the Elasticsearch service cannot access PostgreSQL or freezer data.
  - Using the **nfsnobody** account simplifies configuration, preventing the need to build an **idmap.conf** for each customer site, mapping local and remote account names together.
- The NFSv4 server must be accessible via the Admin 10-Gb interface.
- Sufficient storage must be available (see Backup Storage Requirements).
- The system will use these parameters: `rw`, `sync`, `nfsvers=4`, `nofail`

  Note Do not enter conflicting parameters. Manually entering any parameters that conflict with the above parameters is explicitly unsupported and may result in undefined behavior.

- Invalid NFS configuration (or configuration pointing the service to an incorrectly configured NFS server) will generally cause the process of applying configuration to fail. Correcting this configuration in the Admin UI and reapplying should result in success.

Backup Storage Requirements

Total storage required for a backup store should not require more than 5.6 TB. A backup store consists of the following components:

- **Object Store** - This is normally the bulk of the storage in use. Data retention for the bulk component of a backup store follows the same policies and limits documented for the Secure Malware Analytics Appliance release in use and places maximum storage use for this component as 4.1 TB. See the Secure Malware Analytics Appliance Data Retention Notes.
- **PostgreSQL database store** - This contains two full backups of the PostgreSQL store, and a chain of WAL logs sufficient to allow replay from the oldest of the retained full backups. This should be less than 500 GB in total.
- **Elasticsearch snapshot store** - This should be less than 1 TB in total.

Backup Expectations

The following backup expectations should be considered:

- **Included in Backup** - The initial release of the Secure Malware Analytics Appliance backup process includes the following customer-owned bulk data:
    - Samples
    - Analysis results, artifacts, flagging
    - Application-layer (not Admin UI) organization and user account data.
    - Databases (including users and organizations)
    - Configuration done within the Face or Mask portal UI
- **Not Included in Backup** - The following is not included in the initial release of the Secure Malware Analytics Appliance backup process:
    - System logs
    - Previously downloaded and installed updates
    - Configuration inside the appliance Admin UI, including SSL keys and CA certificates
- **Other Expectations** - Other considerations about the backup process include:
    - PostgreSQL base backup takes place on a 24-hour cycle. Database backup cannot be restored, and a warning will be displayed, until this has successfully completed at least once.
    - Elasticsearch backup takes place incrementally, once every 5 minutes.
    - Freezer backup takes place on an ongoing basis, with a job following behind every 24 hours to handle any objects which were missed from the ongoing backup.
    - Generating a new key creates a new, independent backup store. Like the original, this new store is not valid until a base backup has taken place on a 24-hour cycle.

Backup Data Retention

During a backup, data is retained as follows:

- **PostgreSQL** - The last two successful backups and all WAL segments since those backups are retained.
- **Elasticsearch** - The last two 5-minute snapshots are retained.
- **Bulk Storage** - The same retention policy followed and documented for a single Secure Malware Analytics Appliance is used for the shared store.

If you want to retain historical data for longer periods, it is strongly recommended that you use a NFS server with filesystem- or block-layer snapshot support.

Database base backups are only retained until a new base backup has been successfully created.

Note Backup copies of the virtual machine images are created on the RAID-1 storage array, to be used in the event of a reset following a bulk-storage failure. Early Cisco Secure Malware Analytics Appliance models (based on the UCS C220-M3 platform) have less storage than later models, and are more likely than other units to have less than 25 percent of disk space remaining available on the RAID-1 file system after installing Secure Malware Analytics Appliance v2.9, which will trigger a service notice.

For later model hardware, being at less than 25 percent of remaining storage on the RAID-1 array after installing the v2.9 release is not normal and should be raised to customer support.

Strictly Enforce Retention Period Limits

The **strict_retention** option in **tgsh** (v2.6 or later) allows you to strictly enforce the retention period limit by not storing artifacts from analysis for more than fifteen (15) days. When this option is enabled, files are deleted during the first nightly pruning on which they are more than 15 days old.

Note The time period of 15 days cannot be configured or changed.

Artifacts refers to the samples themselves and other things generated from them. Artifacts do not include the analysis report HTML, which is subject to its original limits as otherwise documented. Artifacts also do not include database entries and search indexes.

The **strict_retention** option is disabled (false) by default. To enable the hard-pruning of artifacts after 15 days, set the option to true in **tgsh**:

```
configure set strict_retention true
```

Backup Frequency

The backup frequency of data is as follows:

- For bulk storage of samples, artifacts and reports, content is continuously backed up. Additionally, a pass is performed to look for and transfer missing content on a 24-hour cycle.
- For the PostgreSQL database, a base backup is created on a 24-hour cycle, and incremental content is continually added thereafter, either as soon as a 16-MB threshold of newly-written database content is reached, or not less than once every 5 minutes.

- For the Elasticsearch database, content is incrementally added to the backup store on a 5-minute cycle.

Backup frequency cannot be controlled or tuned because doing so would make estimates regarding storage usage, restore-process time, and performance overhead invalid.

Backup Related Service Notices

The following service notices may be displayed during the backup process:

- **Network storage not mounted** - Check that the network file system being used as a backend is fully operational, and then try reapplying configuration through the Admin UI or rebooting your appliance.
- **Network storage not working** - Check that the network file system being used as a backend is fully operational; if the system does not recover within 15 minutes of correcting any problems with the NFS server, try rebooting your appliance.
- **Backup file system access failure** - Contact customer support.
- **No PostgreSQL backup found** - This is a normal condition between the point in time when a backup store has been configured and the point in time when the first base backup (run automatically on a 24-hour cycle) takes place. Note that until this is complete, a backup is not considered complete and cannot be restored. If and only if this message persists for more than 48 hours, contact customer support.
- **Newest PostgreSQL base backup more than two days old** - This indicates that the system has not been successful in generating a new base backup for PostgreSQL. If not remediated, it can result in unbounded usage on the backup store (to retain a full chain of writes necessary to restore from an increasingly old backup point), and unacceptably long processing time needed for a restore to take place. Contact Support.
- **Backup Creation Messages** - These reflect errors detected when starting or triggering a backup.
- **ES Backup (Creation) Inactive** - Indicates that when Elasticsearch was started, the backup store was unavailable. This can be remediated by rebooting the appliance, or (if NFS and the encryption service are now functional) by logging into **tgsh** and running the command service `restart elasticsearch.service`.
- **Backup Maintenance Messages** - These reflect errors detected when checking status of previously created backups.
- **ES Backup (Maintenance) snapshot (...) status FAILED** - This indicates that in the most recent attempt to update the backup of the Elasticsearch database, no indices could be successfully written. Check that the NFS server is functional and has free space; if no issue can be identified and the issue persists, contact customer support.
- **ES Backup (Maintenance) snapshot (...) status INCOMPATIBLE** - Should only occur immediately after an appliance upgrade installing a new version of Elasticsearch; will be displayed until the backup store has been upgraded to be compatible with this new release. Restoring from an incompatible backup may require customer service assistance, should a failure occur while in this state.
- **ES Backup (Maintenance) snapshot (...) status PARTIAL** - Contains one of two messages in the body: No prior successful backups seen, so retaining. (if we're keeping a partial backup as better than none at all); or Prior successful backups exist, so removing. (if we're discarding that partial backup with the intent to retry later).
- **ES Backup (Maintenance) - Backup required (...) ms** - Occurs if a backup requires more than 60 seconds. This is not necessarily an error: Elasticsearch performs periodic maintenance which can cause

significant write load even on idle systems. However, if it takes place consistently when under periods of low load, investigate storage performance or contact customer service for assistance.

- **ES Backup (Maintenance)** - Unable to query Elasticsearch snapshot status - Elasticsearch could not be contacted; and this failure took place after a backup creation was successfully started. Generally, this will occur in conjunction with other appliance failures, and remediation should focus on those issues. If this error is seen when the appliance is otherwise fully functional and does not go away of its own accord, contact customer support.

Appliance Backup

Perform the following steps to perform a backup of the Secure Malware Analytics Appliance:

Procedure

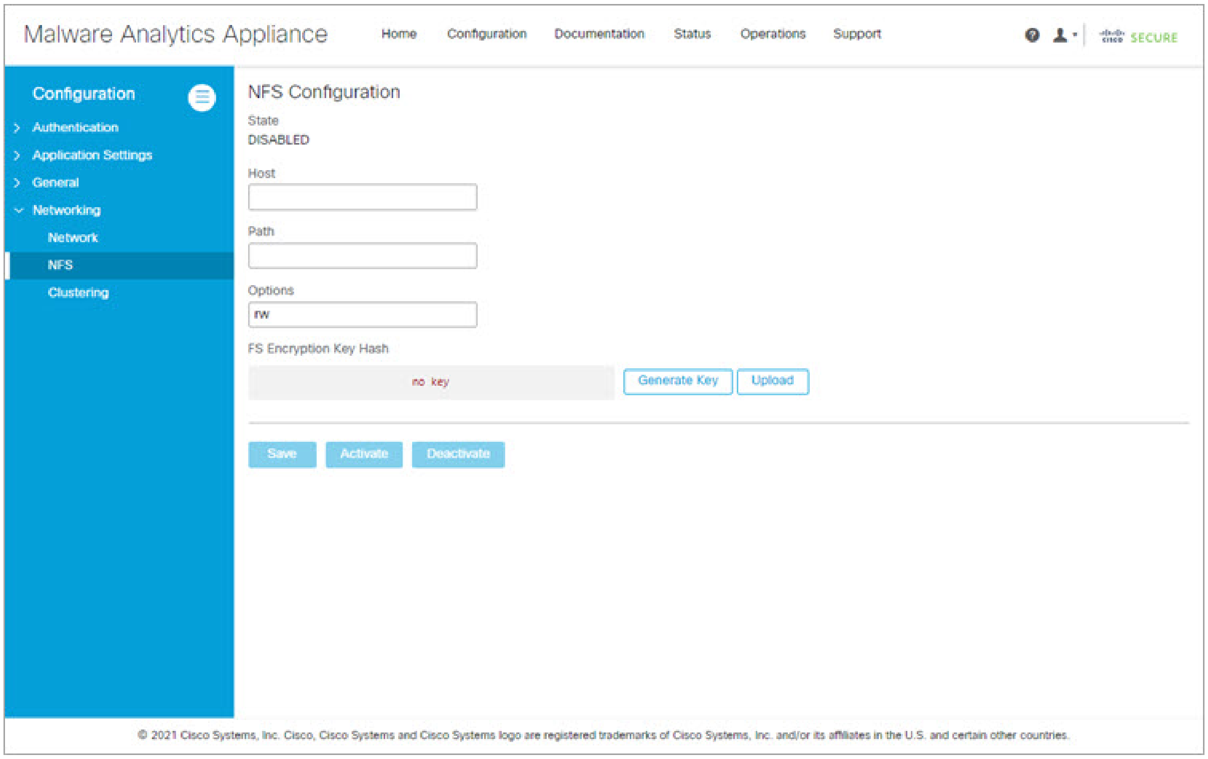
Step 1 Create the backup target directory according to the NFS.

Step 2 Click the **Configuration** tab.

Step 3 Expand **Networking** in the side navigation and choose **NFS** to open the **NFS Configuration** page.

Note
If you completed the NFS configuration during the initial appliance setup and you have the encryption key, you can skip step 3 through step 5. Otherwise, you must obtain an encryption key to restore the backup data.

Figure 35: NFS Configuration



NFS Configuration

State
DISABLED

Host

Path

Options
rw

FS Encryption Key Hash
no key

© 2021 Cisco Systems, 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 4 Enter the following information:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server under which files will be stored.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4. The default is **rw**.
- **FS Encryption Key Hash** - Click **Generate Key** to generate a new encryption key. You will need this key to restore backups later. (At that time, click **Upload** and upload the key required for the backup.)

Step 5 Click **Save**. The page refreshes and a **FS Encryption Password Key ID** is displayed.

The first time you configure this page, options to **Delete** or **Download** the encryption key become visible. The **Upload** option is available if you have NFS enabled but do not have a key created. Once you create a key, the **Upload** button changes to **Download**. (If you delete the key, the **Download** button becomes **Upload** again.)

Note
If the key correctly matches the one used to create a backup, the **Key ID** displayed in Admin UI after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key.

Step 6 Click **Activate** to activate the key.

Important
The user is responsible for backing up the encryption key and securely storing it; Secure Malware Analytics does not retain a copy. Backup cannot be completed without this key.

Step 7 Reset the backup restore target as described in Reset Appliance as Backup Restore Target.

Step 8 Restore the backup data as described in Restore Backup Content, on page 72.

Reset Appliance as Backup Restore Target

Before an appliance can be used as a restore target, it must be in a preconfigured state. Appliances ship in this state. However, getting one back to the preconfigured state once it has been configured requires explicit administrative action.

Caution Performing this process will destroy customer-owned data. Read all of the documentation before performing any tasks, and be very careful before proceeding. .

Note Reset is not the same as the secure wipe that is available in recovery mode; only the recovery-mode secure wipe is appropriate to completely remove customer-owned data from an appliance before shipping it to a DLP reimaging center. However, the secure wipe in recovery mode is not a replacement for this reset: secure wipe renders an appliance unusable until reimaged, while this reset prepares an appliance to restore a backup.

Data Reset

The data reset process was updated in Secure Malware Analytics Appliance v2.7 and later and is now more comprehensive. While the Wipe process (in the recovery bootloader menu) is still required for a firm guarantee of the destruction of all customer-related data, the reset process now clears operating system logs and other state which was previously left in place.

A successfully reset Secure Malware Analytics Appliance now has a new randomly-generated password displayed on its console (identical to behavior in newly-installed state). This improved process now reboots multiple times, and can be invoked from recovery mode (as opposed to the prior process, which could only be successfully invoked when booted into regular operation).

The Secure Malware Analytics Appliance (v2.7 and later) uses XFS as the primary file system. If a Secure Malware Analytics Appliance has its data reset, the datastore will be changed to a XFS file system. This improves forward compatibility and provides OS-level support for I/O usage monitoring on a per-service basis.

The data reset process now also requires sufficient storage to contain all content necessary for a fresh install on the system SSDs. Any pre-existing data is only deleted after the presence and validity of this content has been ensured. It is possible that systems that have been in use for an extended period (particularly first-generation hardware), may not have sufficient space immediately available. If this is the case, customer support can assist, if needed.

Returning a Target Appliance to Preconfigured State

If you are not restoring to a system fresh from manufacturing, the restore target appliance must be returned to the preconfigured state by clearing pre-existing data and NFS-related configuration from the system.

Procedure

Step 1 Access the Admin TUI via the Secure Malware Analytics Appliance TTY, or SSH.

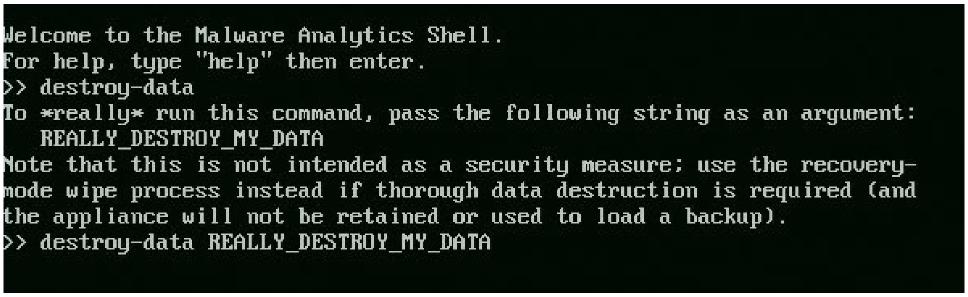
Step 2 Choose the **Console** option to enter **tgsh**.

Note
Entering **tgsh** via Recovery Mode is not suitable for this use case.

Step 3 At the **tgsh** prompt, enter the command `destroy-data`. Carefully read and follow the instructions provided with the prompt.

Caution
There is no Undo from this command. All data will be destroyed.

Figure 36: The destroy-data REALLY_DESTROY_MY_DATA Command and Argument



```
Welcome to the Malware Analytics Shell.
For help, type "help" then enter.
>> destroy-data
To *really* run this command, pass the following string as an argument:
   REALLY_DESTROY_MY_DATA
Note that this is not intended as a security measure; use the recovery-
mode wipe process instead if thorough data destruction is required (and
the appliance will not be retained or used to load a backup).
>> destroy-data REALLY_DESTROY_MY_DATA
```

The following data is destroyed:

- Samples

- Analysis results, artifacts, flagging
- Application-layer (not the Admin UI) organization and user account data
- Databases (including users and organizations)
- Configuration done within the Face or Mask portal UI
- NFS configuration and credentials
- The local copy of the encryption key used for NFS

Returning Non-Target Appliance to Preconfigured State

If another system or Secure Malware Analytics Appliance is actively writing to the backup that is being restored, for example, a test restore of content being written by a second master Secure Malware Analytics Appliance actively used in production, return that Secure Malware Analytics Appliance to the preconfigured state.

Procedure

Step 1 Generate a consistent, writable copy of the datastore.

Step 2 Point the Secure Malware Analytics Appliance that is doing the test restore to the writable copy instead of to the store which is being continuously written.

Once the Secure Malware Analytics Appliance is in a preconfigured state, it can function as the target for the backup store as described in Restore Backup Content.

Restore Backup Content

Important

- The system is unavailable for sample submission during the restore process.
- Only one server can be running with data from a given backup store active at a time.
- Backups can only be restored from the Admin UI.
- Set up the same NFS store and encryption key, as previously used, with a process identical to the original process. Setting up a Secure Malware Analytics Appliance with a prior NFS store and encryption key will trigger a restore.
- To test the restore process on a different Secure Malware Analytics Appliance while the primary Secure Malware Analytics Appliance is still operational, make a copy of a consistent snapshot of the backup store and point the new Secure Malware Analytics Appliance (with the encryption key uploaded) to it.

Perform the following steps to restore the backup content:

Procedure

Step 1 Click the **Configuration** tab and choose **NFS** to open the **NFS Configuration** page.

Step 2 Click **Upload** to retrieve the backup key previously generated when configuring the server on which the backup was created.

If the key correctly matches the one used to create a backup, the **Key ID** displayed in the Admin UI should match the name of a directory in the configured path. The install wizard checks for a directory matching the backup key, and if it finds one, begins restoring the data to that location.

Note
There is no progress bar. The amount of time required to restore data depends on the size of the backup and other factors. In testing, a 1.2-GB restore is quick, while a 1.2-TB restore required over 16 hours. For large restores it may appear that the install has hung so be patient. The Admin UI will report that the restore has succeeded, and the appliance will start up.

Step 3 Confirm that the restored data looks the same as the original data.

Clustering

Clustering increases the capacity of a single system by joining several Secure Malware Analytics Appliances together into a cluster (consisting of 3 to 7 nodes). It helps recovery from failure of one or more appliances in the cluster, depending on the cluster size. Each Secure Malware Analytics Appliance in a cluster saves data in the shared file system, and has the same data as the other nodes in the cluster.

Important If you have questions about installing or reconfiguring clusters, contact Cisco Support for assistance to avoid possible destruction of data.

Features

Clustering Secure Malware Analytics Appliances offers the following features:

- **Shared Data** - Every Secure Malware Analytics Appliance in a cluster can be used as if it a standalone; each one is accessing and presenting the same data.
- **Sample Submissions Processing** - Submitted samples are processed on any one of the cluster members, with any other member able to see the analysis results.
- **Rate Limits** - The submission rate limits of each member are added up to become the cluster's limit.
- **Cluster Size** - The preferred cluster sizes are 3, 5, or 7 members; 4- and 6-node clusters are supported, but with availability characteristics similar to a degraded cluster (a cluster in which one or more nodes are not operational) of the next size up.
- **Tiebreaker** - When a cluster is configured to contain an even number of nodes, the one designated as the tiebreaker gets a second vote in the event of an election to decide which node has the primary database.

Each node in a cluster contains a database, but only the database on the primary node is actually used; the others just have to be able to take over if and when the primary node goes down. Having a tiebreaker can prevent the cluster from being down when exactly half the nodes have failed, but only when the tiebreaker is not among the failed nodes.

Odd-numbered clusters will not have a tied vote. In an odd-numbered cluster, the tiebreaker role only becomes relevant if a node (not the tiebreaker) is dropped from the cluster; it then becomes even-numbered.

Limitations

Clustering Secure Malware Analytics Appliances has the following limitations:

- When building a cluster of existing standalone Secure Malware Analytics Appliances, only the first node (the initial node) can retain its data. The other nodes must be manually reset because merging existing data into a cluster is not allowed.

  Remove existing data with the destroy-data command, as documented in Reset Appliance as Backup Restore Target

Important Do not use the Wipe Appliance feature as it will render the appliance inoperable until it's returned to Cisco for reimaging.

- Adding or removing nodes can result in brief outages, depending on cluster size and the role of the member nodes.
- Clustering on the M3 server is not supported. Contact Opening a Support Case if you have any questions.
- Starting with 2.20 SMA Appliance release, two-node clusters are not supported. Two nodes are not enough to keep quorum if a node goes down unexpectedly, and gives no availability guarantees, even with previous support for a tiebreaker node.

Requirements

Important **Clustering in Airgapped Deployments Strongly Discouraged** - Due to the increased complexity of debugging, appliance clustering is **strongly discouraged** in airgapped deployments or other scenarios where a customer is unable or unwilling to provide L3 support access to debug.

The following requirements must be met when clustering Secure Malware Analytics Appliances:

- **Version** - All Secure Malware Analytics Appliances must be running the same version to set up a cluster in a supported configuration; it should always be the latest available version.
- **Clust Interface** - Each Secure Malware Analytics Appliance requires a direct interconnect to the other Secure Malware Analytics Appliances in the cluster; a SFP+ must be installed in the Clust interface slot on each Secure Malware Analytics Appliance in the cluster (not relevant in a standalone configuration).

  Direct interconnect means that all Secure Malware Analytics Appliances must be on the same layer-two network segment, with no routing required to reach other nodes and no significant latency or jitter. Network topologies where the nodes are not on a single physical network segment are not supported.

- **Data** - A Secure Malware Analytics Appliance can only be joined to a cluster when it does not contain data (only the initial node can contain data). Moving an existing Secure Malware Analytics Appliance into a data-free state requires the use of the database reset process (available in v2.2.4 or later).

Important Do not use the destructive Wipe Appliance process, which removes all data and renders the application inoperable until it's returned to Cisco for reimaging.

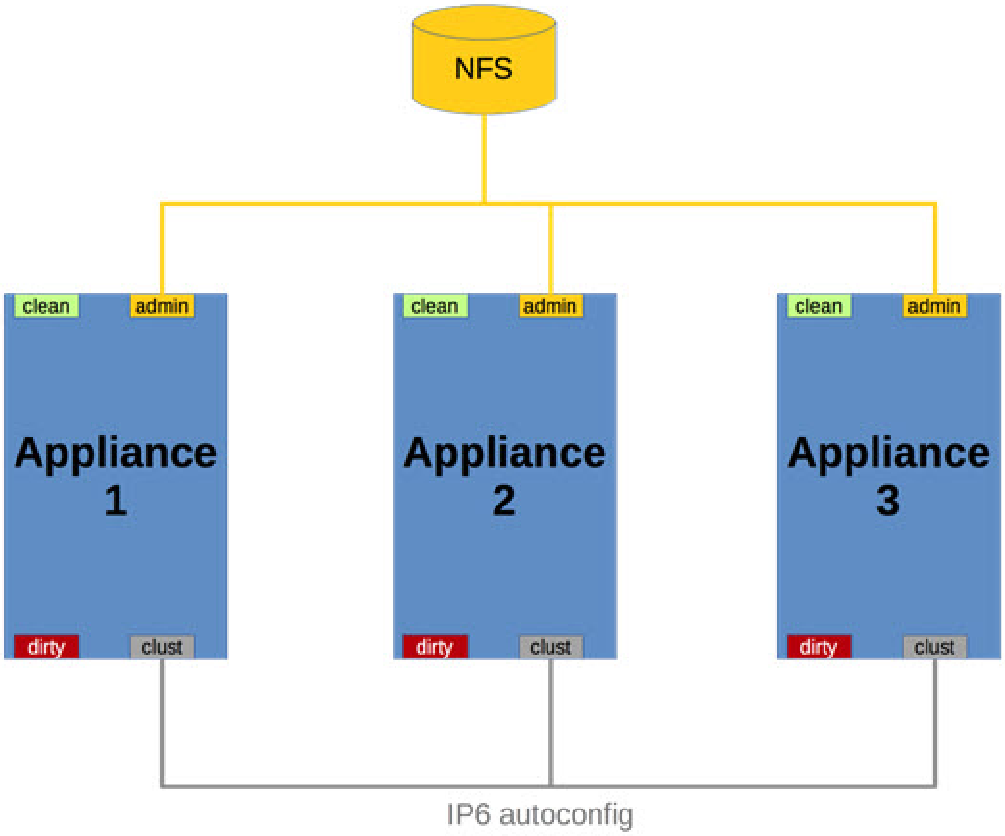
- **SSL Certificates** - If you are installing SSL certificates signed by a custom CA on one cluster node, then the certificates for all of the other nodes should be signed by the same CA.

Networking and NFS Storage

Clustering Secure Malware Analytics Appliances requires the following networking and NFS storage considerations:

- Secure Malware Analytics Appliance clusters require a NFS store to be enabled and configured. It must be available via the Admin interface and accessible from all cluster nodes.
- Each cluster must be backed by a single NFS store with a single key. While that NFS store may be initialized with data from a pre-existing Secure Malware Analytics Appliance, it must not be accessed by any system that is not a member of the cluster while the cluster is in operation.
- The NFS store is a single point of failure, and the use of redundant, highly reliable equipment for that role is essential.
- The NFS store used for clustering must keep its latency consistently low.

Figure 37: Clustering Network Diagram



Building a Secure Malware Analytics Appliance Cluster

Building a Secure Malware Analytics Appliance cluster in a supported manner requires that all members be on the same version, which should always be the latest available version. This may mean that all of the members have to be built standalone first to get fully updated.

If the Secure Malware Analytics Appliance has been in use as a standalone appliance prior to clustering, only the data of the first member can be preserved. The others need to be reset as part of the build.

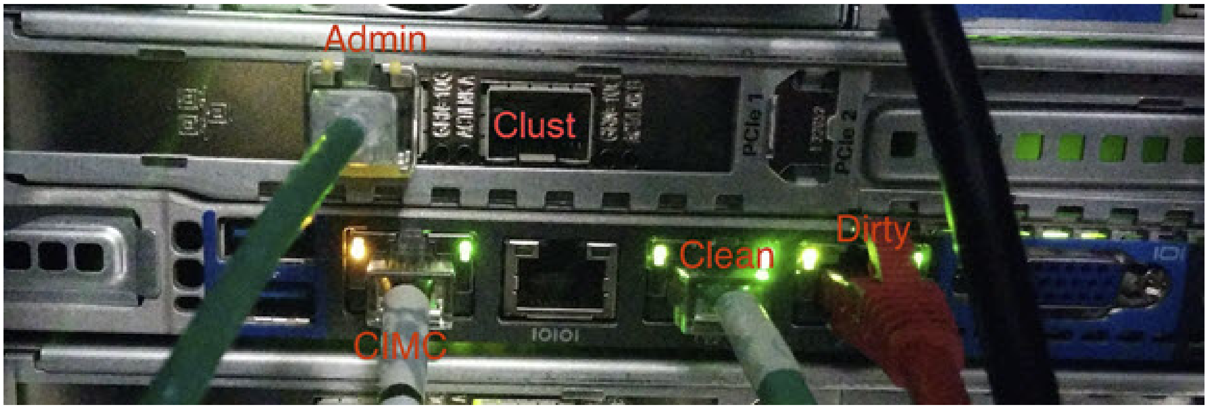
Start a new cluster with an initial node, and then join other Secure Malware Analytics Appliances to it. There are two distinct paths that are available for building a new cluster:

- Start Building Cluster from Existing Standalone Appliance
- Start Building Cluster with New Appliance

Clust Interface Setup

Each appliance in the cluster requires an additional SFP+ for the Clust interface. Install a SFP+ module in the fourth (non-Admin) SFP port. On the M5, this is the second SPF interface from the left (see the Cisco Threat Grid M5 Hardware Installation Guide for more information).

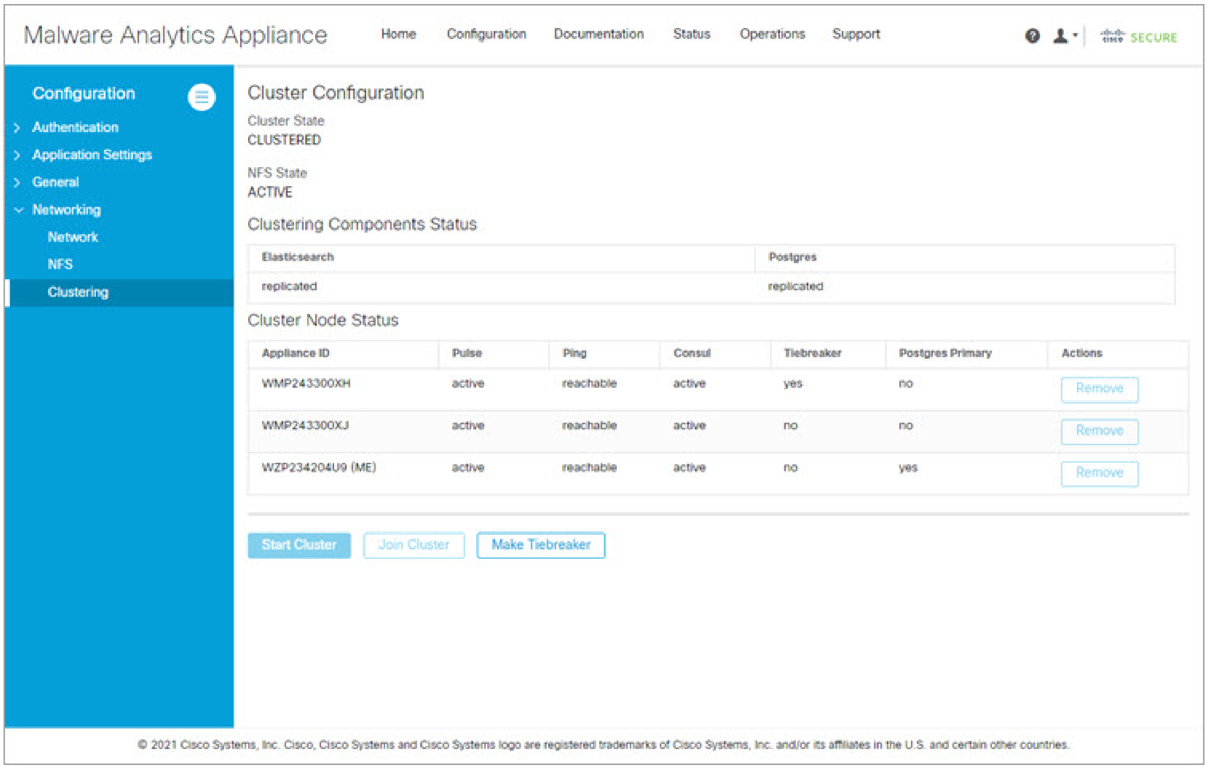
Figure 38: Clust Interface Setup for Cisco UCS M4 C220



Cluster Configuration

Clusters are configured and managed in the Admin UI on the **Cluster Configuration** page **(Configuration > Networking > Clustering)**. This section describes the fields on this page to gain an understanding of an active and healthy cluster (the screenshot shows a cluster with three nodes).

Figure 39: Cluster Configuration for Active Cluster



Cluster Configuration

Cluster State
CLUSTERED

NFS State
ACTIVE

Clustering Components Status

Elasticsearch	Postgres
replicated	replicated

Cluster Node Status

Appliance ID	Pulse	Ping	Consul	Tiebreaker	Postgres Primary	Actions
WMP243300XH	active	reachable	active	yes	no	Remove
WMP243300XJ	active	reachable	active	no	no	Remove
WZP234204U9 (ME)	active	reachable	active	no	yes	Remove

Cluster Prerequisites

- The appliance must be fully set up and configured.
- The NFS State must be **Active**.

Cluster State

- **Unconfigured** - Not yet configured as explicitly part of a cluster or as a standalone Secure Malware Analytics Appliance; you make this choice in the initial setup wizard if the prerequisites for clustering have been met.
- **Pending_NFS_Enable** - Cluster is pending NFS enablement.
- **Pending_NFS_Key** - Cluster is pending NFS key.
- **Standalone** - Appliance is configured as a standalone node; cannot be configured as part of a cluster without a reset.
- **Clustered** - Is clustered with one or more other Secure Malware Analytics Appliances.
- **Unknown** - Status cannot be determined.

Clustering Components Status

- **Elasticsearch**- The service used for queries that require search functionality.
- **PostgreSQL** - The service used for queries that require up-to-date, definitive data (such as account lookups).

Both services are described with one of the following status values:

- **Replicated** - Everything is working properly. Additionally, everything required to take over on failure is also in place. The appliance is able to tolerate failure and continue working. Being in a replicated state does not mean that a failure will have zero downtime. Rather, a failure should entail zero data loss and constrained downtime (less than a minute in normal circumstances, with the exception of any active analysis on the specific cluster node that fails).

  Maintenance operations that bring down nodes should only be performed when the cluster is in the replicated state.

  For a fully replicated cluster, recovery should be automatic and require less than a minute to complete in any normal scenario.
- **Available** - Everything is working properly and the referenced service is available for use (that is, it can service API and user requests), but it is not replicated.
- **Unavailable** - The service is known to be non-functional.

For more information, see the *Secure Malware Analytics Appliance Clustering FAQ* on Cisco.com.

Cluster Nodes Status

- **Pulse** - Indicates whether the node is actively connected to and using the NFS store (not during initial setup, but while running services).
- **Ping** - Describes whether the cluster node can be seen over the Clust interface.
- **Consul** - Indicates whether the node is participating in the consensus store. This requires both a network connection over Clust and a compatible encryption key.
- **Postgres Primary** - Indicates whether the node is the PostgreSQL primary node.

Start Building Cluster from Existing Standalone Appliance

When you start building a cluster of Secure Malware Analytics Appliances, you must start the cluster with the first node being either an existing standalone Secure Malware Analytics Appliance or a new appliance. This section describes how to build a cluster from an existing standalone Secure Malware Analytics Appliance, which allows you to preserve existing data from one appliance and use it to start a new cluster.

Note

- An existing backup must be available on NFS from which the cluster is started.
- All other nodes to be joined to the cluster must have data removed before joining; the data from additional nodes cannot be merged into the cluster.
- In releases prior to v2.4.3, standalone Secure Malware Analytics Appliances with data backed up to NFS no longer require a database reset and restore-from-backup to become the initial node of a new cluster. If you have a Secure Malware Analytics Appliance with an earlier version, we suggest that you upgrade to v2.4.3 or later and then perform a reset operation prior to initializing a new cluster.

Perform the following steps to start building the first node in a cluster from an existing standalone appliance:

Procedure

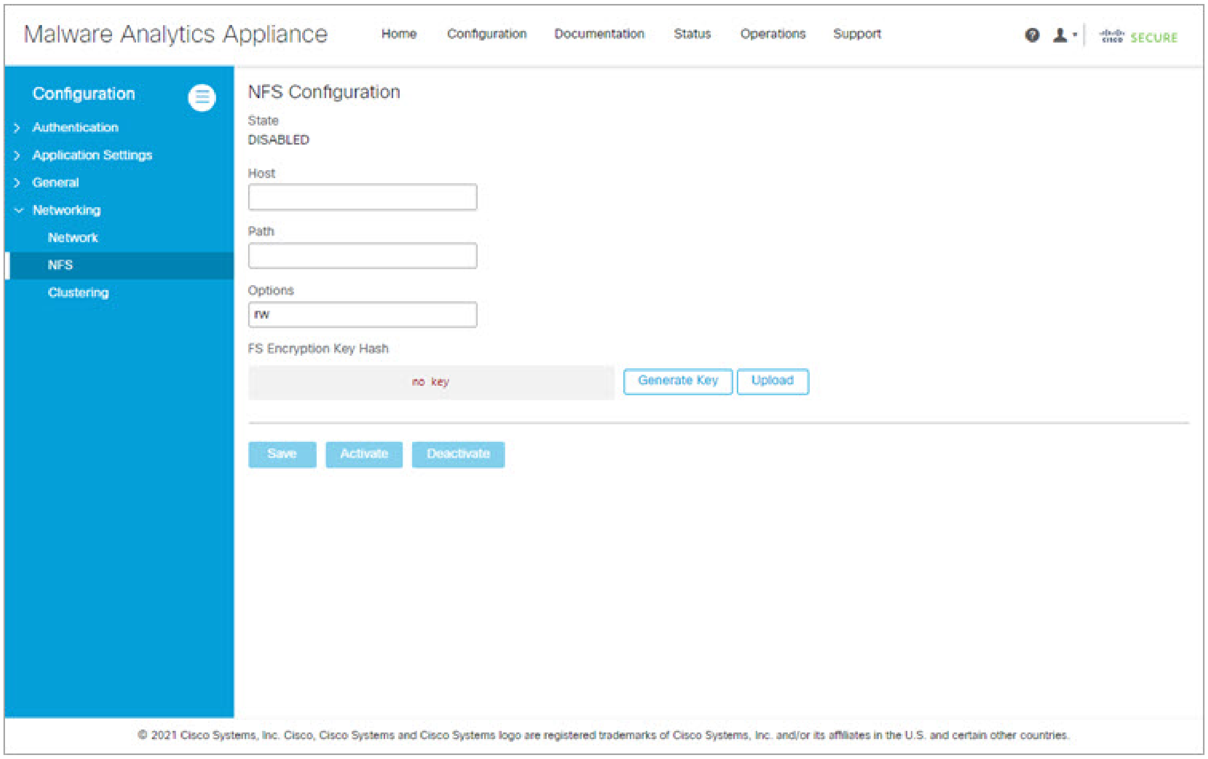
Step 1 Fully update the Secure Malware Analytics Appliance to the latest version. Depending on which version is currently running, this may require more than one update cycle to reach the latest version.

Step 2 If not already completed, configure NFS for backup of the appliance:

Note
This step describes the default Linux NFS server implementation; it may be different for your server setup.

a) Click the **Configuration** tab.
b) Expand **Networking** in the side navigation and and choose **NFS** to open the **NFS Configuration** page.

Figure 40: NFS Configuration



NFS Configuration

State

DISABLED

Host

Path

Options

rw

FS Encryption Key Hash

no key

© 2021 Cisco Systems, 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.

c) Complete the following fields:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server where files will be stored. This does not include the Key ID suffix, which will be added automatically.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

d) Click **Save**.

The page refreshes and the **Generate Key** button becomes available.

The first time you configure this page, the **Remove** and **Download** buttons are available for removing and downloading the encryption key.

The **Upload** button is available if you have NFS enabled but no key created. Once you create a key, the **Upload** button changes to **Download**. If you delete the key, the **Download** button becomes **Upload** again.

Note
If the key correctly matches the one used to create a backup, the **KeyID** displayed in the Admin UI after upload should match the name of a directory in the configured path. Backups cannot be restored without the encryption key. The configuration process includes the process of mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

e) Click **Generate Key** to generate a new NFS encryption key.

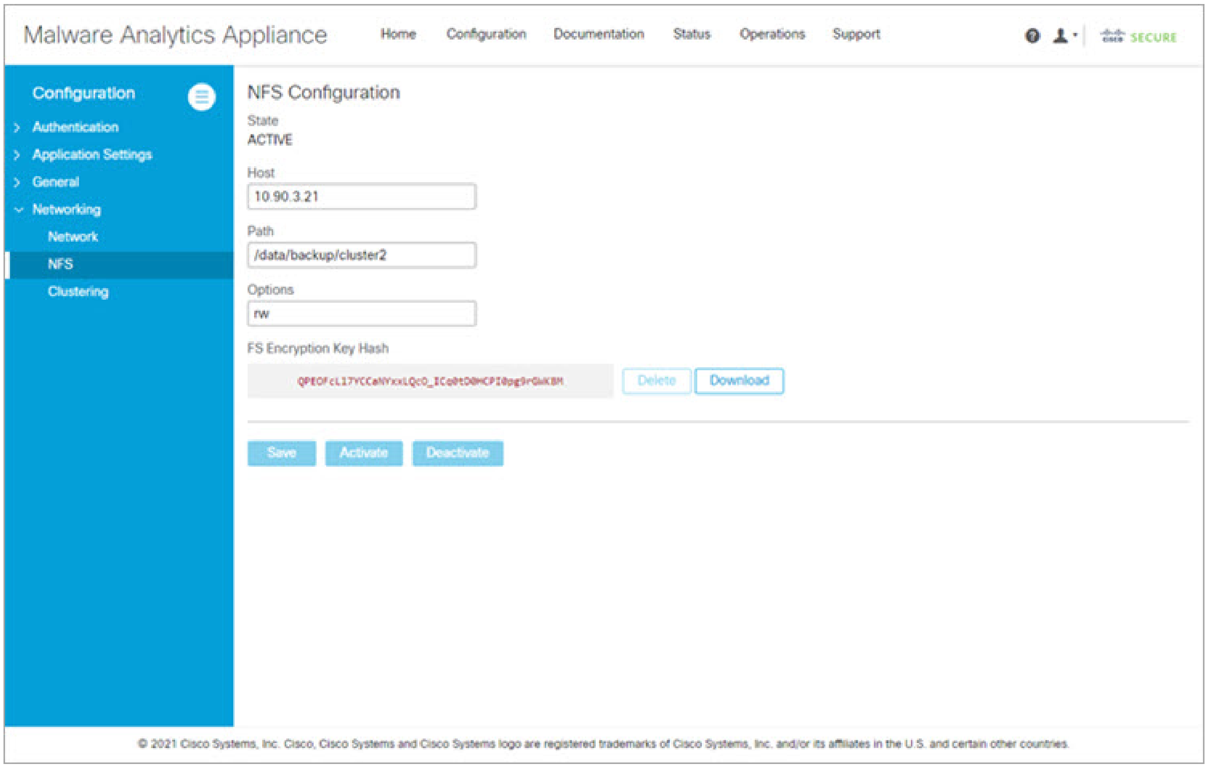
f) Click **Save**.

The page refreshes and the **Key ID** is displayed; the **Activate** and **Download** buttons become available.

g) Click **Activate**.

After a few seconds, the **State** becomes **Active**.

Figure 41: NFS Active



NFS Configuration

State
ACTIVE

Host
10.90.3.21

Path
/data/backup/cluster2

Options
rw

FS Encryption Key Hash
QPEOFcL17YCCaNYxxLQcO_ICq0tD0HCPI0pg9rGWKBM

© 2021 Cisco Systems, 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.

h) Click **Download** to download the backup encryption key. Save the generated file in a secure location. You will need the key for joining additional nodes to the cluster.

Important
If this step is missed, all data will be lost in the following steps.

Step 3 Complete the configuration, as needed, and reboot the Secure Malware Analytics Appliance to apply the NFS backup configuration.

Step 4 Perform a backup.

Note
If you do the backup at least 48 hours in advance, as recommended, and there are no service notices indicating problems with the backup, then the following manual steps are unnecessary.

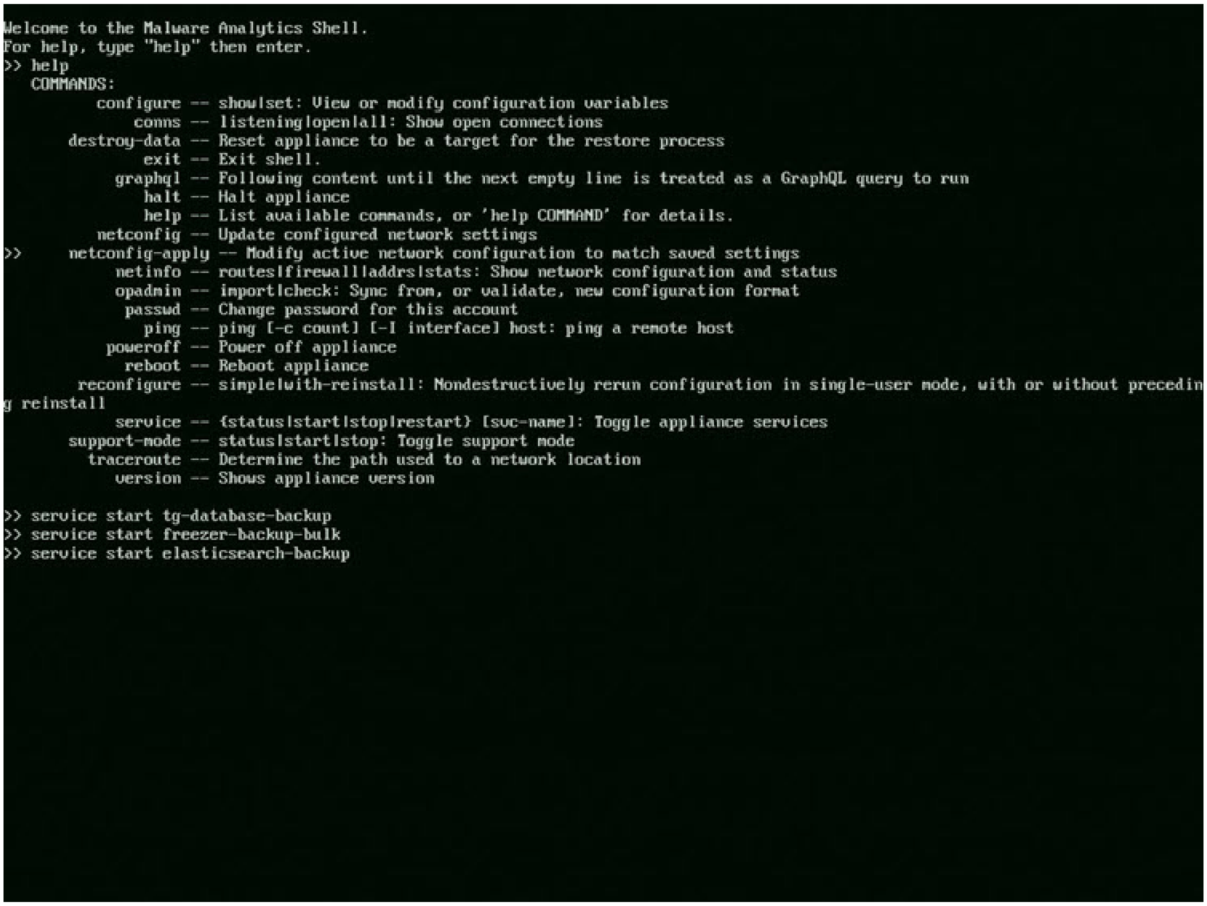
Backup and other service notices are available in the Secure Malware Analytics portal UI from the icon in the upper-right corner. If a service notice **There is no PostgreSQL backup yet** is displayed, DO NOT PROCEED.

If you want your backup to be useable without waiting for 48 hours then manually initiate a backup of all data to NFS to ensure it's complete. Performing the manual backup is only necessary if you are setting up backup immediately before rebuilding the standalone appliance in a cluster.

a) Open **tgsh** and enter the following commands:

```
service start tg-database-backup.service
service start freezer-backup-bulk.service
service start elasticsearch-backup.service
```

Figure 42: Initiating a Backup of All Data to NFS



```
Welcome to the Malware Analytics Shell.
For help, type "help" then enter.
>> help
   COMMANDS:
          configure -- show|set: View or modify configuration variables
              conns -- listening|open|all: Show open connections
       destroy-data -- Reset appliance to be a target for the restore process
               exit -- Exit shell.
            graphql -- Following content until the next empty line is treated as a GraphQL query to run
               halt -- Halt appliance
               help -- List available commands, or 'help COMMAND' for details.
          netconfig -- Update configured network settings
>>     netconfig-apply -- Modify active network configuration to match saved settings
            netinfo -- routes|firewall|addrs|stats: Show network configuration and status
            opadmin -- import|check: Sync from, or validate, new configuration format
             passwd -- Change password for this account
               ping -- ping [-c count] [-I interface] host: ping a remote host
           poweroff -- Power off appliance
             reboot -- Reboot appliance
        reconfigure -- simple|with-reinstall: Nondestructively rerun configuration in single-user mode, with or without precedin
g reinstall
            service -- {status|start|stop|restart} [svc-name]: Toggle appliance services
       support-mode -- status|start|stop: Toggle support mode
         traceroute -- Determine the path used to a network location
            version -- Shows appliance version

>> service start tg-database-backup
>> service start freezer-backup-bulk
>> service start elasticsearch-backup
```

b) Wait about 5 minutes after the last command returns.

Step 5 In the Secure Malware Analytics portal UI, check for service notices. If any notices indicate a backup process failure, such as a warning that there is no PostgreSQL backup yet, then DO NOT PROCEED.

Important
Do not continue unless these processes have completed successfully.

Step 6 Click the **Configuration** tab.

Step 7 Expand **Networking** in the side navigation and choose **Clustering** to open the **Clustering Configuration** page.

Step 8 Click **Start Cluster**.

Step 9 On the confirmation dialog, click **OK**.

The **Clustering Status** changes to **Clustered**.

Step 10 Finish the installation. This initiates a restore of the data in cluster mode.

What to do next

Now you can begin joining other Secure Malware Analytics Appliances to the new cluster, as described in Joining Secure Malware Analytics Appliances to a Cluster.

Start Building Cluster with New Appliance

When you start building a cluster of Secure Malware Analytics Appliances, you can start the cluster with the first node being new Secure Malware Analytics Appliance. This method of building a cluster can be used for new appliances that are shipped with cluster-capable versions of the software, or for existing appliances that have had their data reset.

Note Remove existing data with the `destroy-data` command, as documented in Reset Appliance as Backup Restore Target. Do not use the Wipe Appliance feature.

Procedure

Step 1 Set up and begin the Admin UI configuration as normal.

Step 2 Configure the Network and License.

Step 3 Click the **Configuration** tab.

Step 4 Expand **Networking** in the side navigation and choose **NFS** to open the **NFS Configuration** page.

Note
See the figures in Start Building Cluster from Existing Standalone Appliance.

Step 5 Complete the following fields:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server where the files will be stored. This does not include the Key ID suffix, which will be added automatically.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

Step 6 Click **Save**.

The page refreshes, and the **Generate Key** and **Activate** buttons become available.

Step 7 Click **Generate Key** to generate a new NFS encryption key.

Step 8 Click **Activate**.

The **State** changes to **Active**.

Step 9 Click **Download** to download a copy of the encryption key for safekeeping. You will need the key for joining additional nodes to the cluster.

Step 10 On the **Cluster Configuration** page, click **Start Cluster**, and then click **OK** on the confirmation dialog.

The **Clustering State** changes to **Clustered**.

Step 11 Complete the remaining steps in the wizard and click **Start Installation**. This initiates a restore of the data in cluster mode.

Step 12 Open the **Cluster Configuration** page and check the health of the new cluster.

What to do next

Proceed to Joining Secure Malware Analytics Appliances to a Cluster.

Joining Secure Malware Analytics Appliances to a Cluster

This section describes how to join new and existing Secure Malware Analytics Appliances to a cluster.

Note A Secure Malware Analytics Appliance can be joined to an existing cluster only when it contains no data; unlike the initial appliance, which may contain data.

Also, it is critically important that the Secure Malware Analytics Appliance that is joining a cluster has the latest software version installed (all nodes in a cluster must be running the same version). This may require setting up the Secure Malware Analytics Appliance and update it, then reset the data, and join it to the cluster.

Add one node at a time, and wait for Elasticsearch and PostgreSQL to reach the state of **Replicated** before adding the next node. The **Replicated** status is expected in clusters of two or more nodes.

Note The wait for the state change for Elasticsearch and PostgreSQL to reach **Replicated** does not apply to the single-node case. If you are initializing a single-node cluster from a backup, you should wait for the restore to be completed and the application to be visible in the UI before adding the second node.

When joining a Secure Malware Analytics Appliance to a cluster, the NFS and clustering must be configured during the initial setup.

Joining Existing Appliances to a Cluster

Perform the following steps to join an existing Secure Malware Analytics Appliance to a cluster:

Procedure

Step 1 Update the Secure Malware Analytics Appliance to the latest version. This may require several update cycles depending on the current version that is installed. All nodes in a cluster must be the same version.

Step 2 Run the `destroy-data` command in **tgsh** to remove all data; when joining an existing Secure Malware Analytics Appliance to a cluster, all data must be removed prior to being merged into the cluster. See Reset Appliance as Backup Restore Target.

After running the `destroy-data` command on an existing Secure Malware Analytics Appliance, it basically becomes a new node, and joining it to a cluster follows the same steps as Joining New Appliances to a Cluster.

Joining New Appliances to a Cluster

Perform the following steps to join a new Secure Malware Analytics Appliance to a cluster:

Procedure

Step 1 Begin the new Admin UI configuration as described in the Cisco Secure Malware Analytics Appliance Getting Started Guide.

Step 2 In the **NFS Configuration** page, specify the **Host** and **Path** to match the configurations you entered in first node in the cluster.

Step 3 Click **Upload** for **FS Encryption Key Hash** and choose the NFS encryption key you downloaded from the first node when you started the new cluster.

Step 4 Click **Save**.

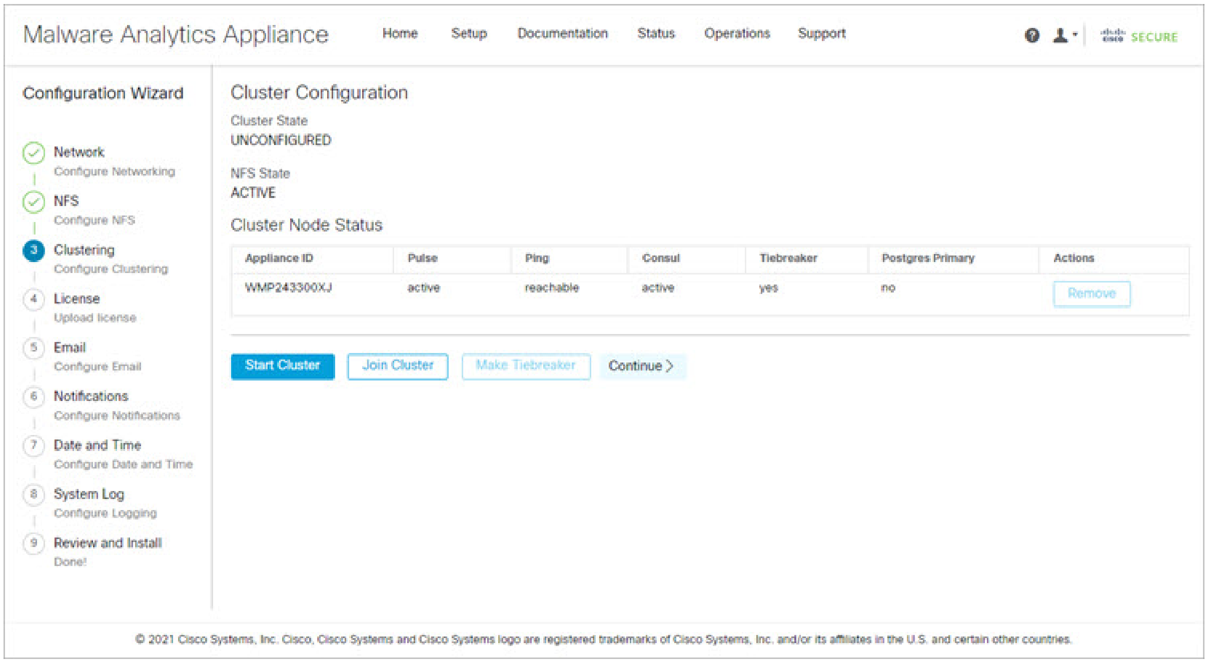
The page refreshes; the **Key ID** is displayed and the **Activate** button is enabled.

Step 5 Click **Continue**.

Cluster Configuration screen appears with the first node.

Step 6 Click **Join Cluster** and then click **OK** on the confirmation dialog.

Figure 43: Cluster Configuration



Cluster Configuration

Cluster State
UNCONFIGURED

NFS State
ACTIVE

Cluster Node Status

Appliance ID	Pulse	Ping	Consul	Tiebreaker	Postgres Primary	Actions
WMP243300XJ	active	reachable	active	yes	no	Remove

The **Cluster State** changes to **Clustered**.

Step 7 Repeat the Step 1 through Step 10 for each node you want to join to the cluster.

Removing a Cluster Node

To remove a node from a cluster, navigate to the **Cluster Configuration** page (**Configuration > Clustering**) and click **Remove** in the **Action** column for the node to be removed.

- Removing a node from the cluster indicates that it should no longer be considered part of the cluster, rather than a node that is temporarily down. You should remove a Secure Malware Analytics Appliance when it is being decommissioned; either being replaced with different hardware or will be rejoined to a cluster only after its data has been reset.
- Removing a node indicates to the system that you are not going to re-add a node, or if you do re-add it, it has been reset.
- A node is not marked as having been permanently removed from a cluster if it has pulse (is actively writing to NFS), or is active on consul (part of the consensus store).

To replace a still-live node (in a cluster with less than seven nodes), add the new node, wait for the cluster to go green, then remove the old one offline using the **Remove** button. This alerts the system that it's not coming back.

When you first take the node offline, the cluster status changes to yellow. After you click **Remove**, the status reverts back to green (since the cluster will resize such that it no longer expects the now-removed node to be present).

Tip A node that is missing (failed or powered down) will eventually time out and be available to remove.

Resizing a Cluster

When a node is removed from a cluster using the **Remove** button, the cluster resizes; this may affect the number of failures it is expected to tolerate. If a cluster is resized in such a way as to change the number of expected failure tolerances (as defined in Failure Tolerances), it will force an Elasticsearch restart, which will cause a brief service interruption.

Exception: This does not include a system other than the PostgreSQL master being rebooted or having a transient failure. Disruption should be minimal in that case except for clients actively using that node, or if samples are running on it.

If you add a Secure Malware Analytics Appliance that was not already part of the cluster, or if you click **Remove**, and this changes the cluster size such that the number of tolerated failures is changed, then there will be a brief interruption as the rest of the cluster reconfigures.

Failure Tolerances

In the event of a failure, clustered Secure Malware Analytics Appliances will not lose any data, with the exception of any analysis being actively run by the failed node, and will recover service with a minimal (less than one minute) service disruption period and no user involvement.

Most failures will recover in less than a minute if the number of available nodes is not smaller than the number shown in the **Nodes Required** column in the **Failure Tolerances** table; or will recover after the number of available nodes increases to meet that count. This is true if the cluster was in a healthy state prior to failures (as indicated by services listed as **Replicated** on the **Clustering** page).

The number of failures a cluster of a given size is expected to tolerate is shown in the following table.

Table 2: Failure Tolerances

Cluster Size	Failures Tolerated	Nodes Required
1	0	1
3	1	2
4	1	3
5	2	3
6	2	4
7	3	4

These figures represent best-case scenarios. If the cluster is not showing green across the board when all nodes are up, then it may not be able to tolerate the full failure count indicated.

For example, if you have a 5-node cluster size with 2 failures tolerated, 3 nodes required, and all 5 appliances are actively processing data, the cluster will be able to reconfigure itself and continue operation without human administrative action if up to 2 failures take place.

Another consideration, in a 5-, 6-, or 7-node cluster, the +1 in the number of failures tolerated means that the percentage of nodes that can fail is higher, which is particularly important because the number of nodes acts as a multiplier to the failure rate. (If you have two nodes, and each has a hardware fault once every 10 years, then you just change your hardware fault rate to once every 5 years.)

Failure Recovery

Most failures recover automatically. If not, you should contact Opening a Support Case, or restore the data from backups. See Restore Backup Content for more information.

API/Usage Characteristics

Status of samples submitted to any node in a cluster may be queried from any other node in the cluster; there is no need to track to which individual node a submission took place.

Processing of sample submissions made to one node will be split across all nodes in the cluster; there is no need to actively load-balance from the client side.

Operational/Administrative Characteristics

Service may be temporarily disrupted during a failover event; samples which were actively running during a failover will not be automatically rerun.

In the context of clustering, capacity refers to throughput, not storage. A cluster with three nodes prunes data to the same maximum storage levels as a single Secure Malware Analytics Appliance. Consequently, a cluster of three 5000-sample appliances, with a total 15,000-samples/day rate limit, will (when used at full capacity), have retention minimums of 33 percent shorter than the 10,000-sample/day estimates provided in the *Threat Grid Appliance Data Retention Notes* on Cisco.com.

Sample Deletion

Support for deleting samples is available on Secure Malware Analytics Appliances (v2.5.0 or later):

- The **Delete** option is available in the **Actions** menu in the samples list.

- The **Delete** button is available in the upper-right corner of the sample analysis report.

Note It may take up to 24 hours for backup copies of deleted samples to be removed from all nodes.

Deleted samples are removed from the shared NFS store immediately; removed from the node processing the deletion request immediately, but the other nodes will lag until the nightly cron job is run. In clustered mode, the NFS store is considered the primary source for samples, so even if the sample is not physically removed from other nodes, it should no longer be retrievable from any of them.

In Secure Malware Analytics Appliance v2.7 and later, sample deletion is extended to include artifacts, which matches the behavior of the cloud product.

CHAPTER 5

Status

The **Status** menu in the Admin UI is used by administrators to view system information, such as installed system packages and their version, detailed logs, and available storage.

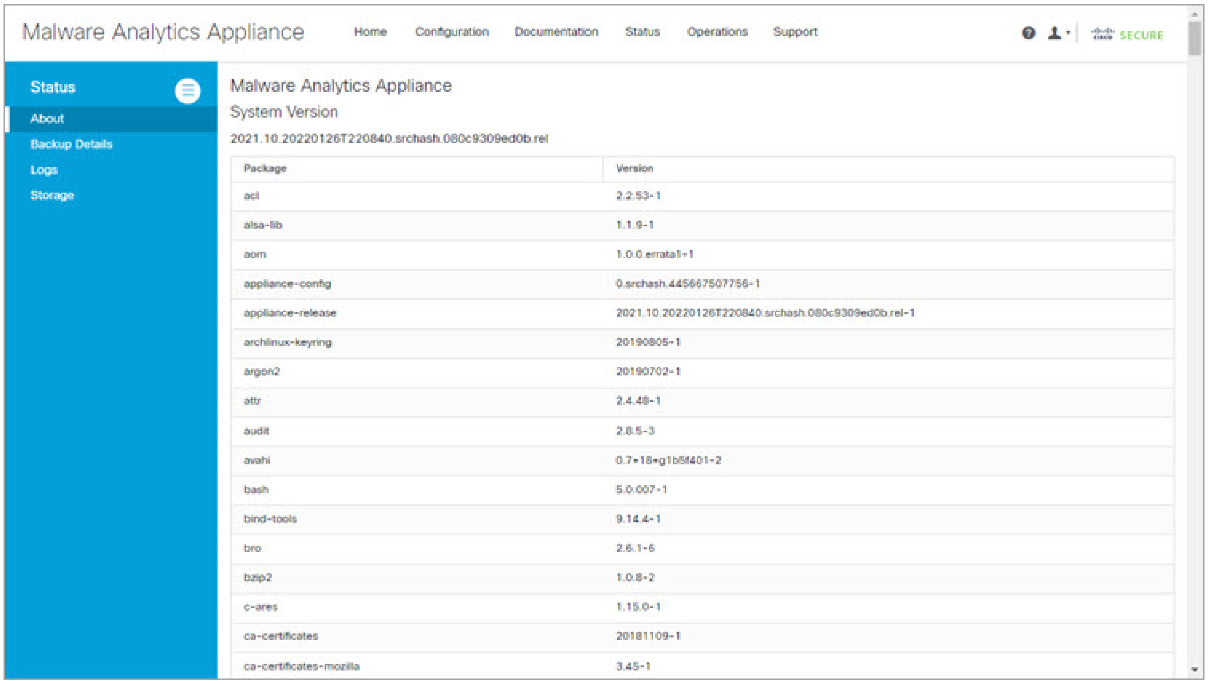
About

You can view the installed packages and their version on the **System Version** page in the Admin UI.

Procedure

Step 1 Click the **Status** tab and choose **About** to open the **System Version** page.

Figure 44: System Version



Malware Analytics Appliance

System Version

2021.10.20220126T220840.srchash.080c9309ed0b.rel

Package	Version
acl	2.2.53-1
alsa-lib	1.1.9-1
aom	1.0.0.errata1-1
appliance-config	0.srchash.445667507756-1
appliance-release	2021.10.20220126T220840.srchash.080c9309ed0b.rel-1
archlinux-keyring	20190805-1
argon2	20190702-1
attr	2.4.48-1
audit	2.8.5-3
avahi	0.7+18+g1b5f401-2
bash	5.0.007-1
bind-tools	9.14.4-1
bro	2.6.1-6
bzip2	1.0.8-2
c-ares	1.15.0-1
ca-certificates	20181109-1
ca-certificates-mozilla	3.45-1

Step 2 View the packages that are installed and their versions. The release version is shown in the upper portion of the page.

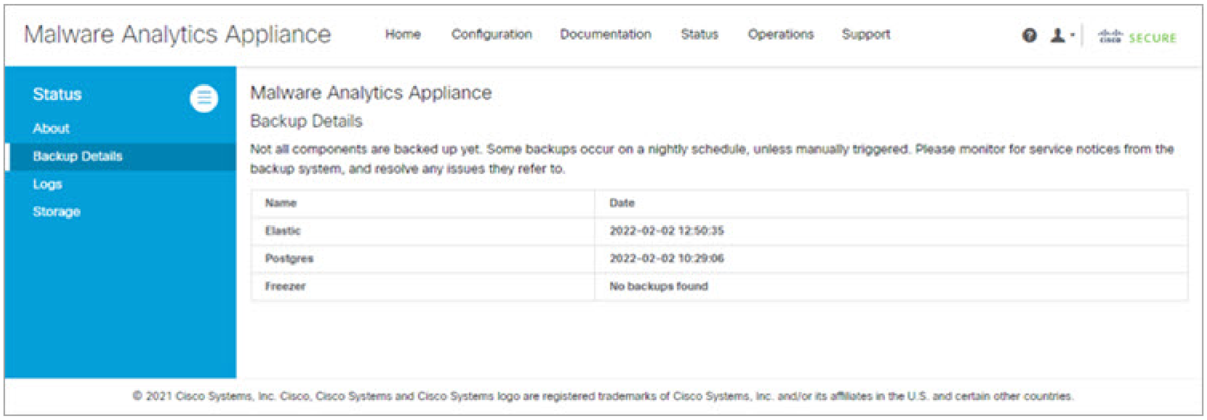
To identify the build number and corresponding release version, see the *Cisco Secure Malware Analytics Appliance Version Lookup Table*.

Backup Details

You can view detailed backup information on the **Backup Details** page, which displays the most recent time at which complete, non-incremental (where applicable) backups of PostgreSQL, Elasticsearch, and Sand Castle freezer data were successfully completed.

Click the **Status** tab and choose **Backup Details** to open the **Backup Details** page.

Figure 45: Backup Details



Malware Analytics Appliance

Backup Details

Not all components are backed up yet. Some backups occur on a nightly schedule, unless manually triggered. Please monitor for service notices from the backup system, and resolve any issues they refer to.

Name	Date
Elastic	2022-02-02 12:50:35
Postgres	2022-02-02 10:29:06
Freezer	No backups found

© 2021 Cisco Systems, 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.

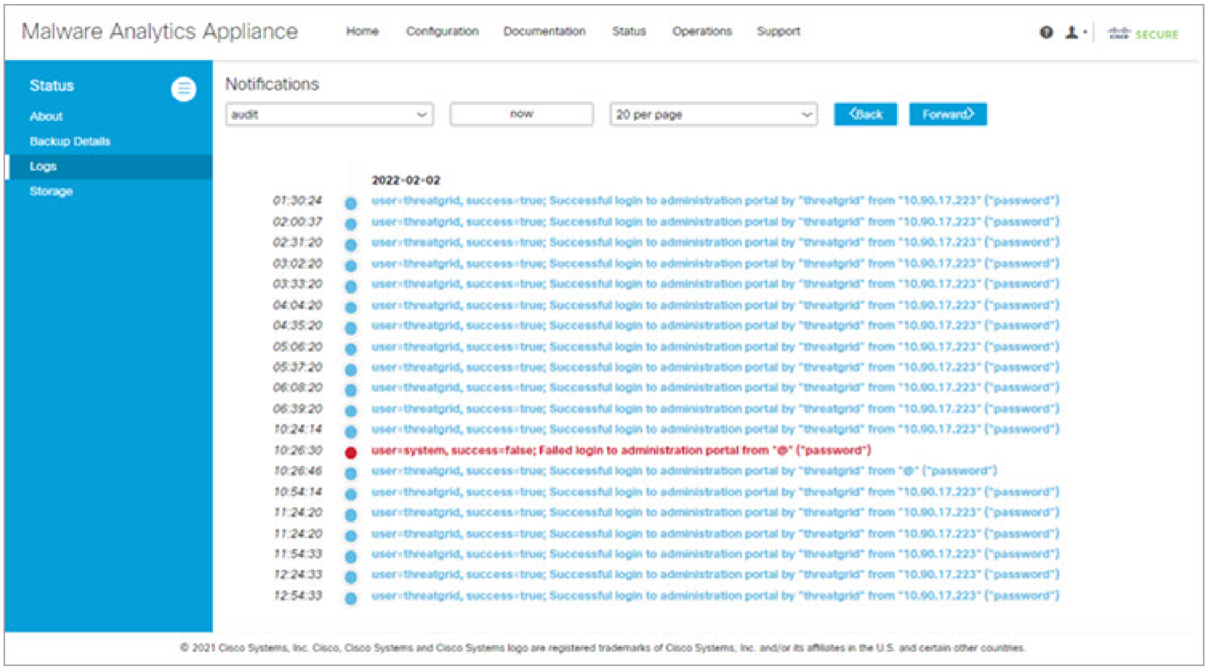
Logs

You can view detailed log information, including historical system logs, on the **Notifications** page.

Procedure

Step 1 Click the **Status** menu and choose **Logs** to open the **Notifications** page.

Figure 46: Notifications



Notifications

```
                2022-02-02
01:30:24  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
02:00:37  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
02:31:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
03:02:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
03:33:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
04:04:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
04:35:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
05:06:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
05:37:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
06:08:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
06:39:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
10:24:14  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
10:26:30  ●  user=system, success=false; Failed login to administration portal from "@" ("password")
10:26:46  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "@" ("password")
10:54:14  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
11:24:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
11:24:20  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
11:54:33  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
12:24:33  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
12:54:33  ●  user=threatgrid, success=true; Successful login to administration portal by "threatgrid" from "10.90.17.223" ("password")
```

© 2021 Cisco Systems, 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 Filter the logs that are displayed by choosing the type of notification from the drop-down list, and specify the number of records to be displayed on the page.

Use the **Back** and **Forward** buttons to navigate between pages.

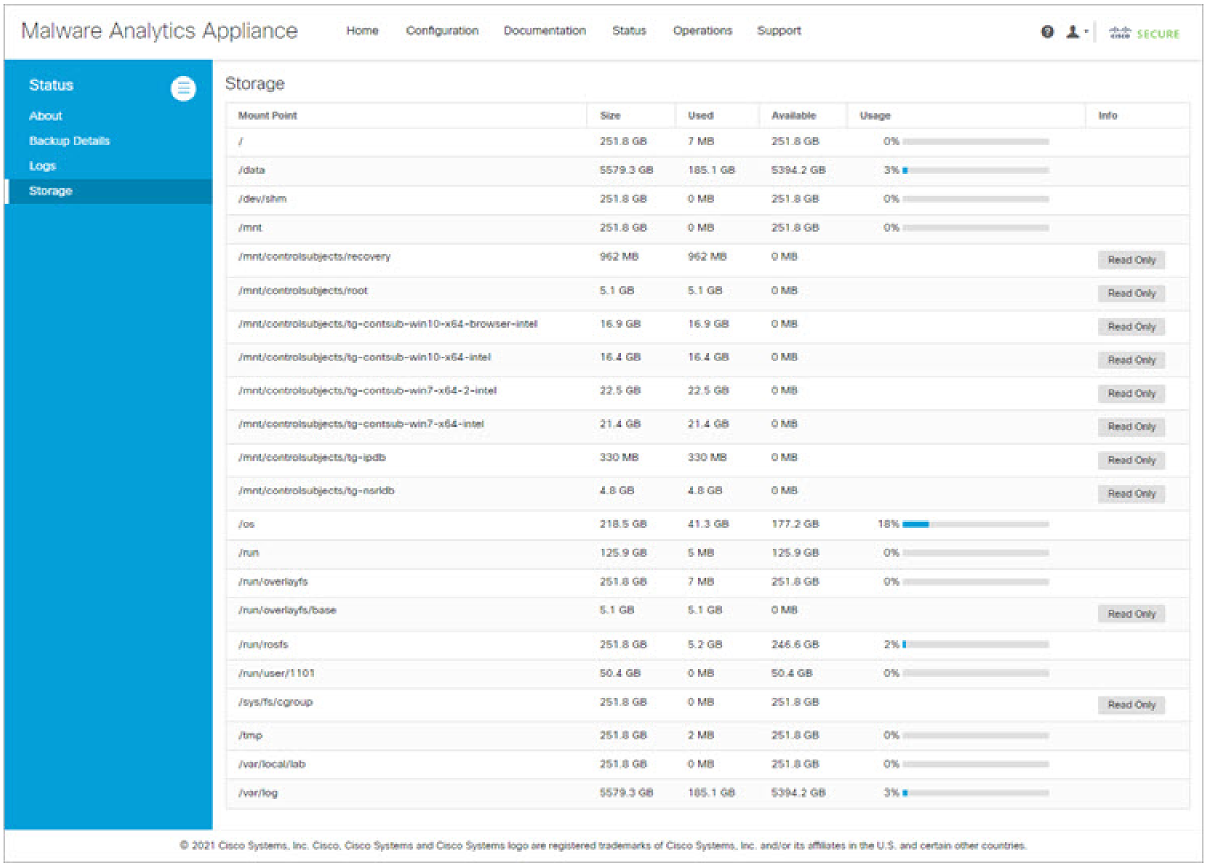
Storage

You can view the available storage on the Secure Malware Analytics Appliance from the **Storage** page.

Procedure

Step 1 Click the **Status** tab and choose **Storage**.

Figure 47: Storage



Storage

Mount Point	Size	Used	Available	Usage	Info
/	251.8 GB	7 MB	251.8 GB	0%	
/data	5579.3 GB	185.1 GB	5394.2 GB	3%	
/dev/shm	251.8 GB	0 MB	251.8 GB	0%	
/mnt	251.8 GB	0 MB	251.8 GB	0%	
/mnt/controlsubjects/recovery	962 MB	962 MB	0 MB		Read Only
/mnt/controlsubjects/root	5.1 GB	5.1 GB	0 MB		Read Only
/mnt/controlsubjects/tg-contsub-win10-x64-browser-intel	16.9 GB	16.9 GB	0 MB		Read Only
/mnt/controlsubjects/tg-contsub-win10-x64-intel	16.4 GB	16.4 GB	0 MB		Read Only
/mnt/controlsubjects/tg-contsub-win7-x64-2-intel	22.5 GB	22.5 GB	0 MB		Read Only
/mnt/controlsubjects/tg-contsub-win7-x64-intel	21.4 GB	21.4 GB	0 MB		Read Only
/mnt/controlsubjects/tg-ipdb	330 MB	330 MB	0 MB		Read Only
/mnt/controlsubjects/tg-nsrldb	4.8 GB	4.8 GB	0 MB		Read Only
/os	218.5 GB	41.3 GB	177.2 GB	18%	
/run	125.9 GB	5 MB	125.9 GB	0%	
/run/overlayfs	251.8 GB	7 MB	251.8 GB	0%	
/run/overlayfs/base	5.1 GB	5.1 GB	0 MB		Read Only
/run/rosfs	251.8 GB	5.2 GB	246.6 GB	2%	
/run/user/1101	50.4 GB	0 MB	50.4 GB	0%	
/sys/fs/cgroup	251.8 GB	0 MB	251.8 GB		Read Only
/tmp	251.8 GB	2 MB	251.8 GB	0%	
/var/local/lab	251.8 GB	0 MB	251.8 GB	0%	
/var/log	5579.3 GB	185.1 GB	5394.2 GB	3%	

Step 2 View the size of the directories, amount of used storage, and the amount of available storage.

CHAPTER 6

Operations

The **Operations** menu is used by administrators to perform operational tasks on the Secure Malware Analytics Appliance. This chapter describes these tasks, including activating configuration changes, reloading the Admin UI, managing jobs and power settings, and updating the appliance.

Activate

Changes to the Admin UI configuration settings must be saved, and several changes also require that you finalize the changes with a reconfiguration. Configuration changes do not take effect until reconfiguration is completed.

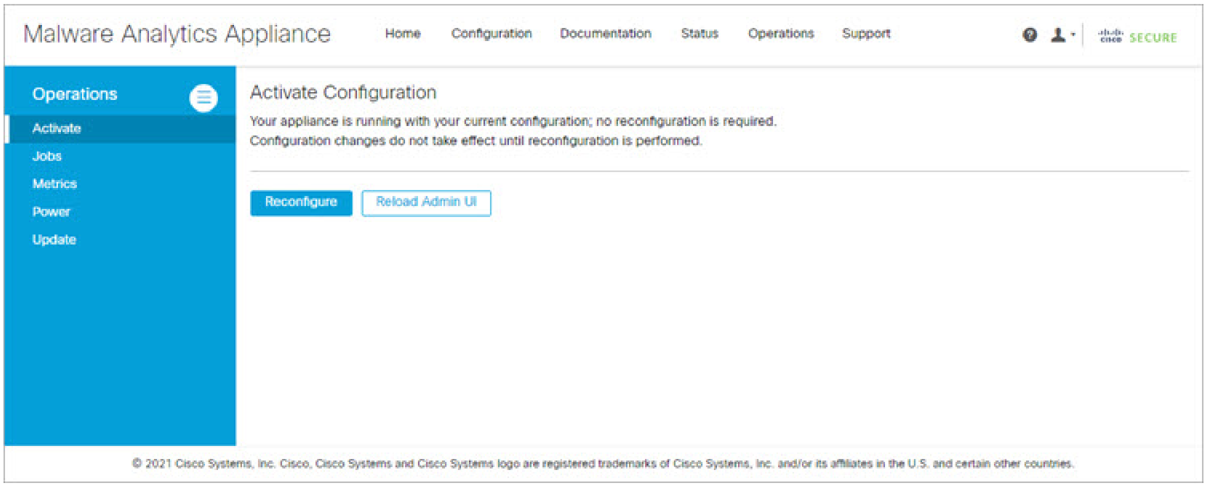
If a reconfiguration is required, a light orange alert message appears in a banner in the upper portion of the page. When you click the **Reconfigure** button on this banner, it takes you to **Activate Configuration** page in the **Operations** menu. From this page, you can apply the configuration changes and also reload the Admin UI.

Procedure

Step 1 Click **Reconfigure** on the alert message to launch the reconfiguration process.

Step 2 On the **Activate Configuration** page, click **Reconfigure** to run the reconfiguration job.

Figure 48: Activate Configuration



Activate Configuration

Your appliance is running with your current configuration; no reconfiguration is required.
Configuration changes do not take effect until reconfiguration is performed.

© 2021 Cisco Systems, 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 3 On the confirmation dialog, click **Reconfigure** to start the reconfiguration job.

Configuration is activated, and messages on its progress are displayed in the jobs window. Details are kept in the Jobs page if you need to review error messages or other information.

When completed, a confirmation message is displayed indicating the reconfiguration was successful.

Step 4 Click **Continue**.

Step 5 If you want to refresh the Admin UI, click **Reload Admin UI**.

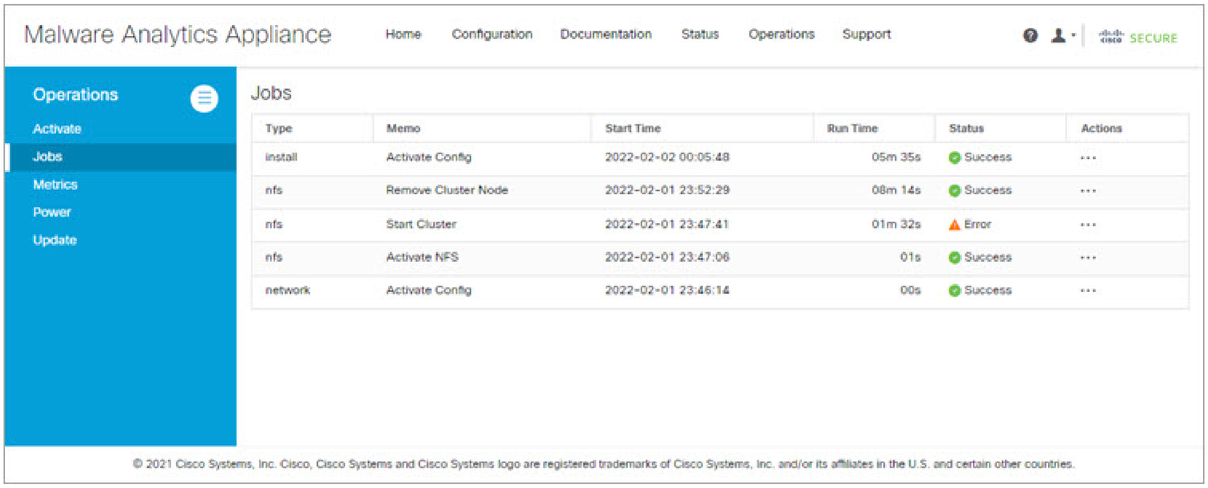
Jobs

You can view the jobs that have been run on the Secure Malware Analytics Appliance using the **Jobs** page in the Admin UI. You can use this page to view error messages or other information about a specific job.

Procedure

Step 1 Click the **Operations** tab and choose **Jobs**.

Figure 49: Jobs



Jobs

Type	Memo	Start Time	Run Time	Status	Actions
install	Activate Config	2022-02-02 00:05:48	05m 35s	● Success	...
nfs	Remove Cluster Node	2022-02-01 23:52:29	08m 14s	● Success	...
nfs	Start Cluster	2022-02-01 23:47:41	01m 32s	▲ Error	...
nfs	Activate NFS	2022-02-01 23:47:06	01s	● Success	...
network	Activate Config	2022-02-01 23:46:14	00s	● Success	...

© 2021 Cisco Systems, 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.

The job type, start time, run time, and status is displayed for each job.

Step 2 Click the **Details** button in the **Actions** column to view information about the job.

Power

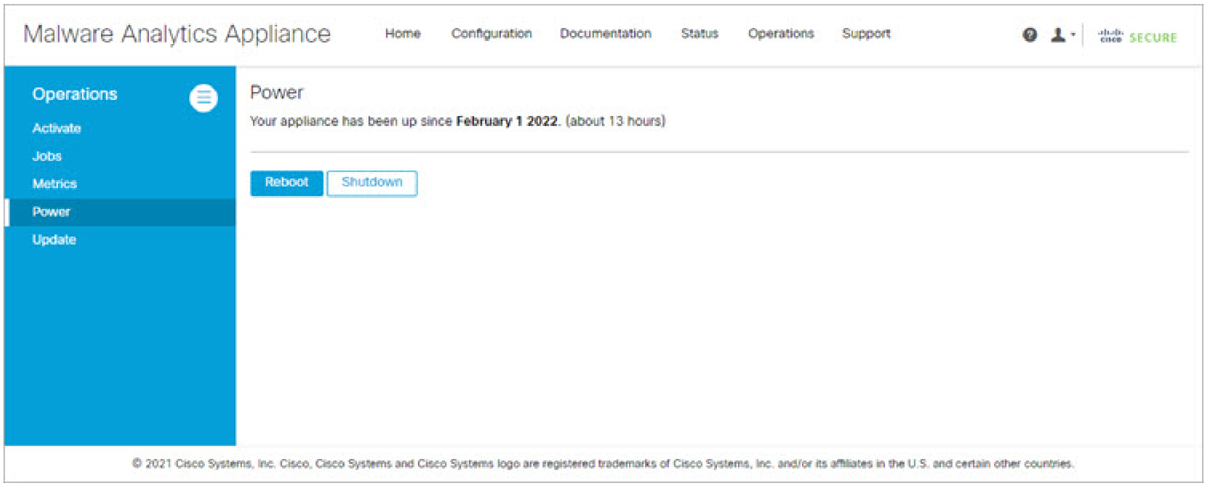
You can reboot or shut down the Secure Malware Analytics Appliance from the **Power** page in the Admin UI.

Note The GNU GRUB bootloader is completely removed from the Secure Malware Analytics Appliance software stack. Whereas our prior configuration did not allow unsigned configuration files to be loaded (and thus was not vulnerable to CVE-2020-10713), the new boot mechanism removes GRUB entirely.

Procedure

Step 1 Click the **Operations** tab and choose **Power**.

Figure 50: Power



Power

Your appliance has been up since **February 1 2022**. (about 13 hours)

© 2021 Cisco Systems, 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.

The date from which your appliance has been powered up is displayed.

Step 2 Click **Reboot** to restart the appliance, or **Shutdown** to completely shut the appliance off.

Update

Before you can update the Secure Malware Analytics Appliance with newer versions, you must have completed the initial setup and configuration steps as described in the *Cisco Secure Malware Analytics Appliance Getting Started Guide*.

Note If you have a new Secure Malware Analytics Appliance that shipped with an older version of software and want to install updates, you must first complete the initial configuration. Updates will not download unless the license is installed, and may not apply correctly if the Secure Malware Analytics Appliance has not been fully configured, including the database.

You can check for new updates (**Operations** > **Update**) and apply them.

Configuration now happens as part of the regular boot process. With each reboot, the appliance is reset to a completely pristine software loadout (with code signatures checked at runtime). Configuration operations that previously happened only during a reconfiguration cycle with multiple reboots now occur as part of every boot cycle. This means that:

- The reconfigure with reinstall operation is made redundant.
- Installing upgrades is now faster, and only requires one reboot.

The following considerations should be observed when installing updates:

- Secure Malware Analytics Appliance updates are applied through the Admin UI.

- If the update server sends an update, the client moves all the way forward to that version. It's not always possible to skip interim releases; when not possible, the update server will require the appliance to install the release before it can download the next update.
- If the server allows you to download a version, you are eligible to move to that version directly; that is, with no intervening reboots beyond those needed for a single upgrade.
- Updates are one-directional: you cannot revert to a previous version after you upgrade to a more recent version.
- For offline (airgapped) update process, see Update Secure Malware Analytics Appliance.

Version Lookup Table

To identify the correct build number and corresponding release version, see the *Cisco Secure Malware Analytics Appliance Version Lookup Table*.

Updates Port

The Secure Malware Analytics Appliance downloads release updates over SSH, port 22.

- Release updates can also be applied from the textual (curses) interface, not just from the web-based administrative interface (Admin UI).
- Systems using DHCP need to explicitly specify DNS. An upgrade of a system without a DNS server explicitly specified will fail.

Database Schema Updates

Historically, on standalone appliances, database migrations associated with updates occurred while the system was offline in single-user mode, except in a cluster, where the updates occurred after the first upgraded node came back online. (The exception to this was for unusually long updates that could be run in the background, which were handled on a case-by-case basis.)

Secure Malware Analytics Appliance (v2.5.0 and later) updates the database schema after the system finishes reboot, which may cause the boot process to take slightly longer. (Very long reboots continue to be handled on a case-by-case basis.)

In prior releases, non-clustered systems with backup support enabled would make a best-effort attempt to operate correctly when their NFS server was down. Due to changes in ElasticSearch functionality, we can no longer guarantee this behavior.

Background Elasticsearch index migration to ES6-native indexes is enabled in v2.7.2 and later. This migration must successfully complete before any version of the Secure Malware Analytics Appliance which requires Elasticsearch 7.0 or newer is installed.

Note Elasticsearch index migration may cause substantial delays in the NFS backup process, causing related warnings. These warnings should be disregarded, as service notices indicate that index migration is actively ongoing. You should only raise a ticket with Support if the index migration process fails to make progress over an extended period.

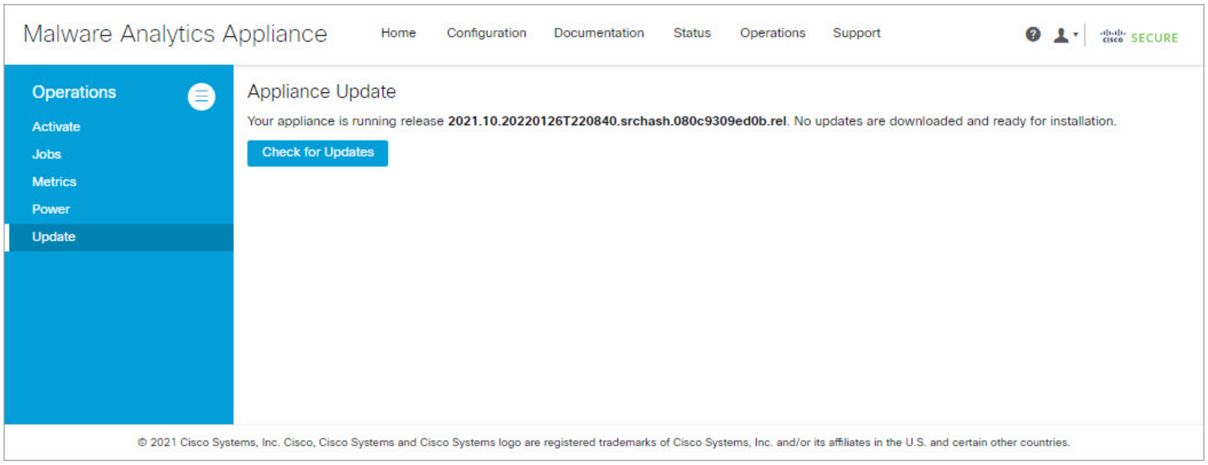
Installing Updates

Perform the following steps to check for updates and to update the Secure Malware Analytics Appliance.

Procedure

Step 1 Click the **Operations** tab and choose **Update** to open the**Appliance Updates** page.

Figure 51: Appliance Updates Page



Appliance Update

Your appliance is running release **2021.10.20220126T220840.srchash.080c9309ed0b.rel**. No updates are downloaded and ready for installation.

© 2021 Cisco Systems, 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.

The current release version is displayed in the upper portion of the page. It also informs you if there is an update available to install. For information about the release versions, see the *Cisco Secure Malware Analytics Appliance Version Lookup Table*.

Step 2 Click **Check for Updates**.

A check is run to see if there is a more recent update/version of the Secure Malware Analytics Appliance software, and if so, downloads it. This may take some time.

Step 3 Once the update has been downloaded, click **Apply Update** to install it.

Troubleshooting Updates

This section includes issues that may occur while updating the appliance and how to resolve them.

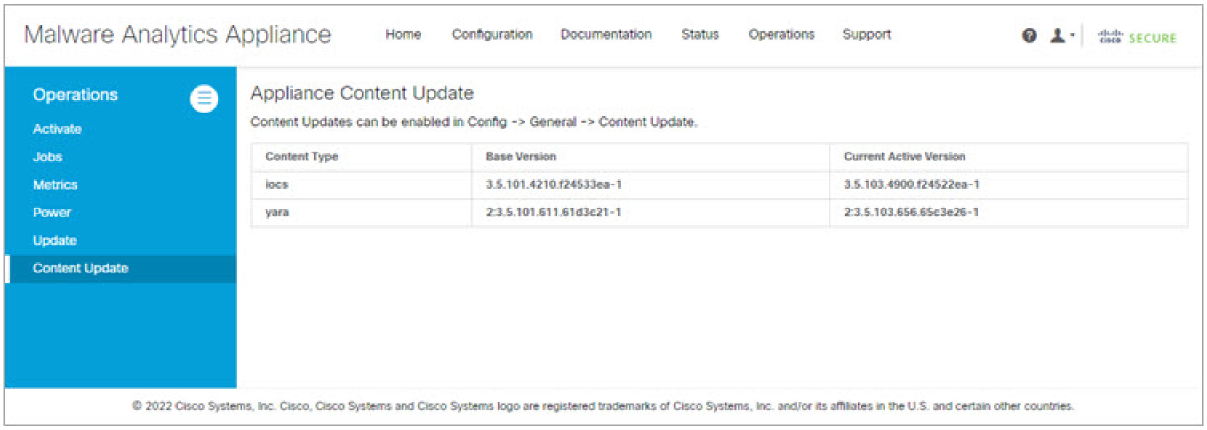
Database Upgrade Not Successful Message

A *database upgrade not successful* message may be displayed if a new Secure Malware Analytics Appliance is running an older version of PostgreSQL and the automated database migration process failed. It is critical that this be fixed prior to any upgrade to v2.0. See *Cisco Threat Grid Appliance Release Notes v2.0.1* for more information.

Appliance Content Update

The Appliance Content Update page provides the base and the current version of the behavioral indicators or iocs (Indicators of Compromise) and yara.

Figure 52: Appliance Content Update



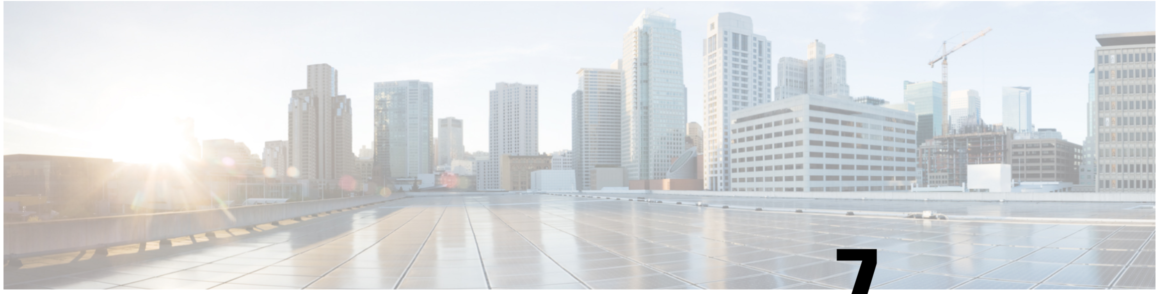
Appliance Content Update

Content Updates can be enabled in Config -> General -> Content Update.

Content Type	Base Version	Current Active Version
iocs	3.5.101.4210.f24533ea-1	3.5.103.4900.f24522ea-1
yara	2:3.5.101.611.61d3c21-1	2:3.5.103.656.65c3e26-1

© 2022 Cisco Systems, 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.

Note Update your appliance to the latest *iocs* and *yara* while you update the appliance. For more information on updating the appliance, see Update, on page 96.



CHAPTER 7

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

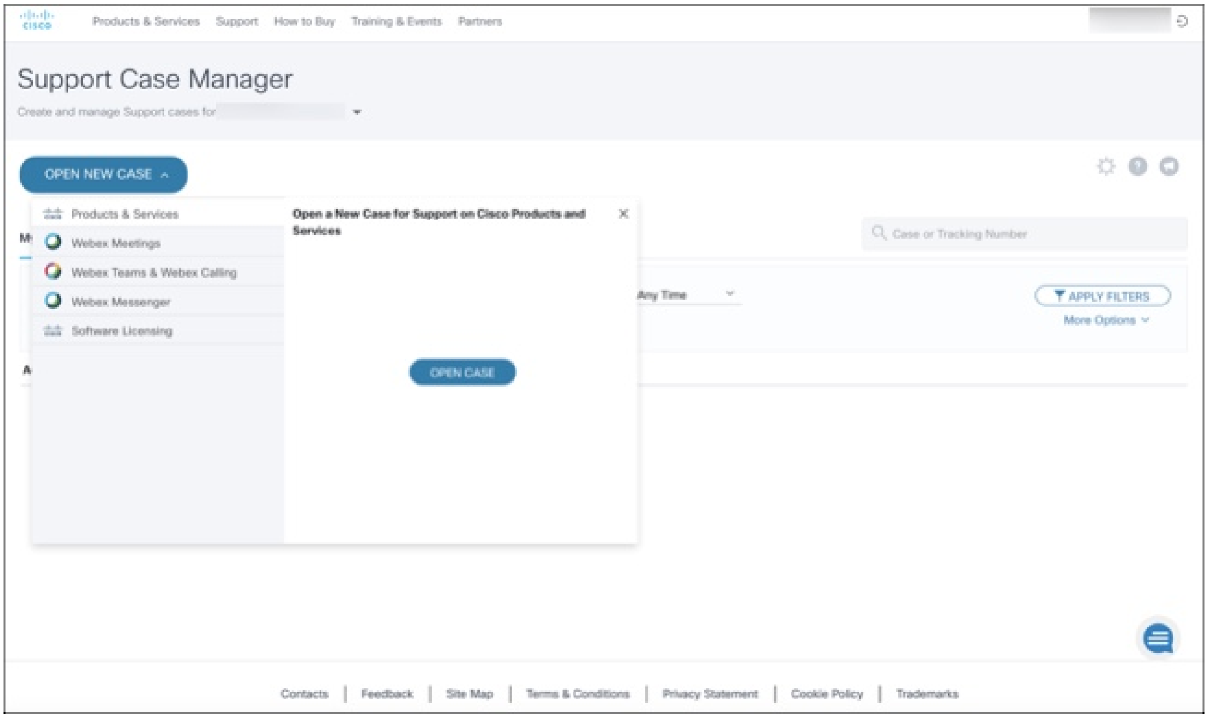
If you have questions or require assistance with Secure Malware Analytics, open a case in Support Case Manager, which is located at https://mycase.cloudapps.cisco.com/case.

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.

Procedure

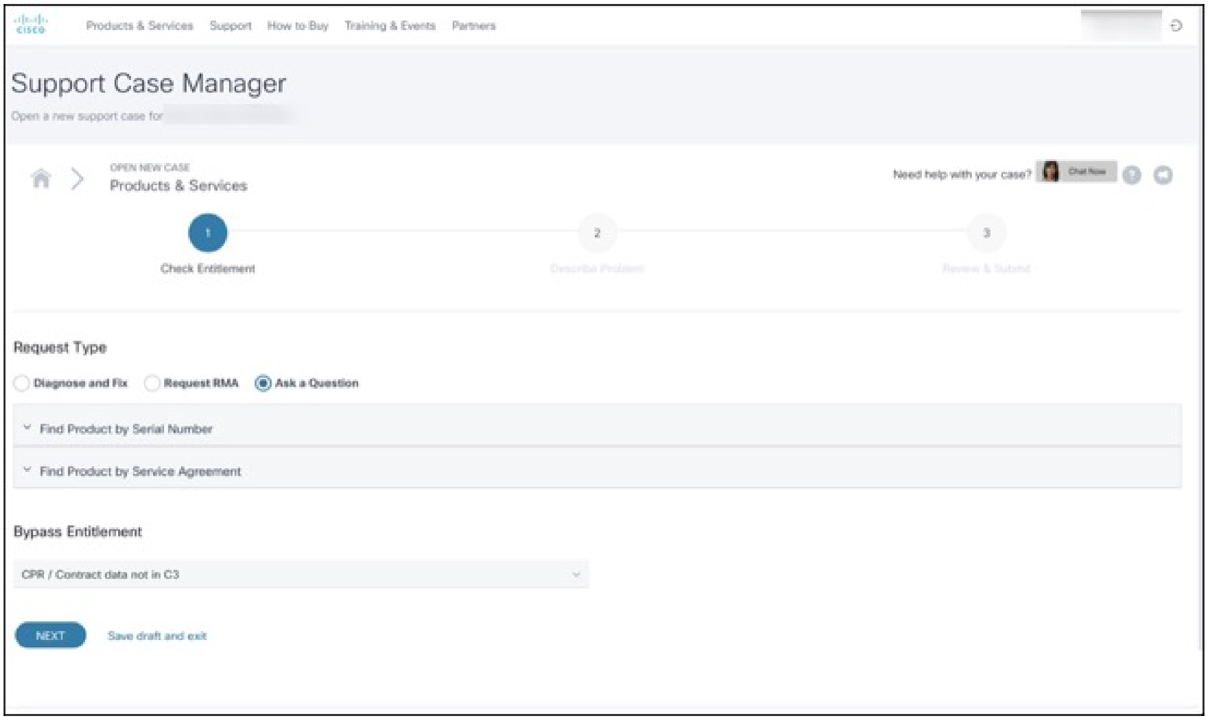
Step 1 In Support Case Manager, click **Open New Case** > **Open Case**.

Figure 53: Open New Case


Products & Services
Support
How to Buy
Training & Events
Partners
Support Case Manager
Create and manage Support cases for [redacted]
OPEN NEW CASE
Products & Services
Webex Meetings
Webex Teams & Webex Calling
Webex Messenger
Software Licensing
Open a New Case for Support on Cisco Products and Services
OPEN CASE
Case or Tracking Number
Any Time
APPLY FILTERS
More Options
Contacts | Feedback | Site Map | Terms & Conditions | Privacy Statement | Cookie 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.

Figure 54: Check Entitlement



Request Type

○ Diagnose and Fix ○ Request RMA ● Ask a Question

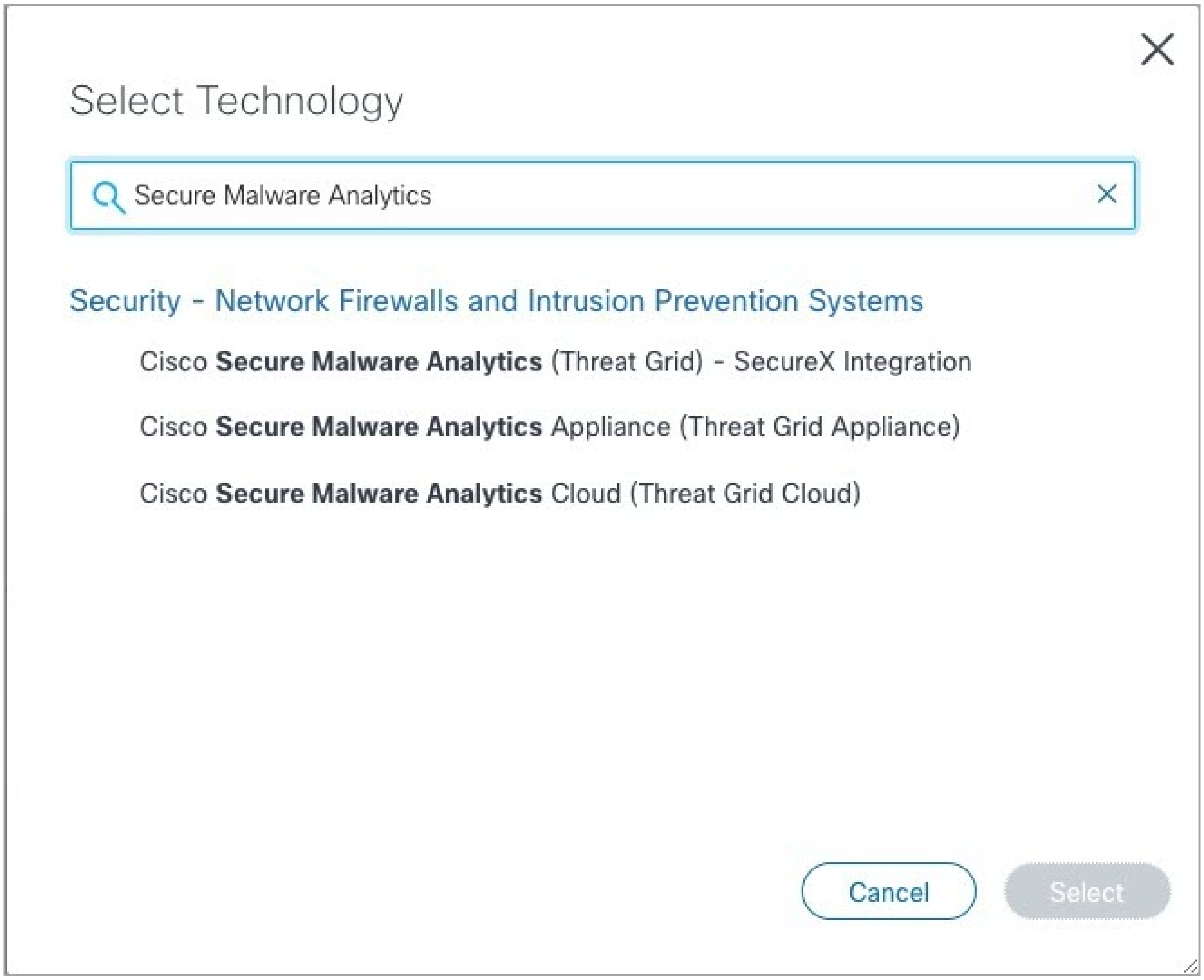
Bypass Entitlement

CPR / Contract data not in C3

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 55: Select Technology



Select Technology

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 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.

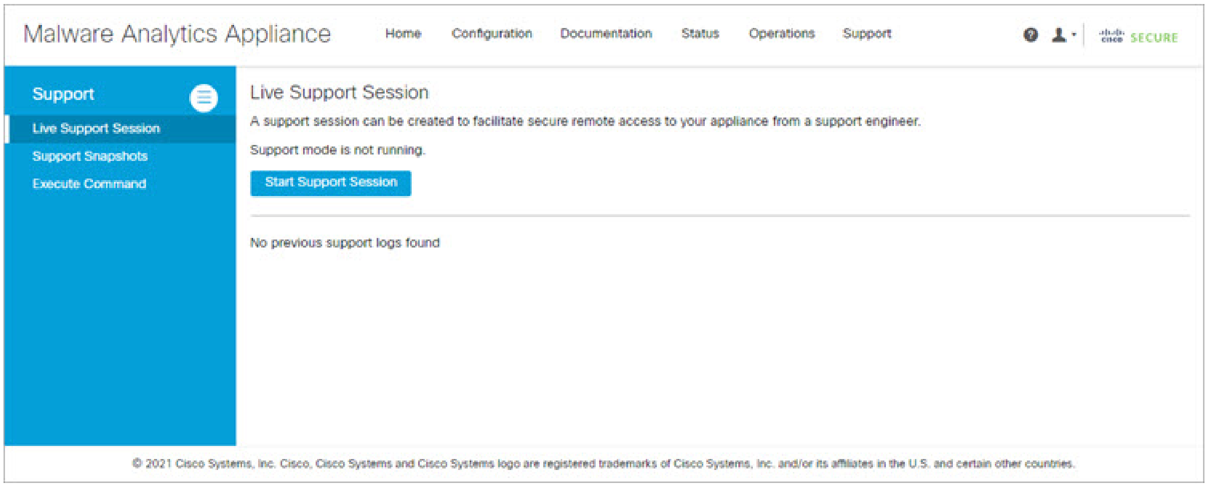
Starting a Live Support Session

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

Procedure

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

Figure 56: Live Support Session



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.

No previous support logs found

© 2021 Cisco Systems, 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

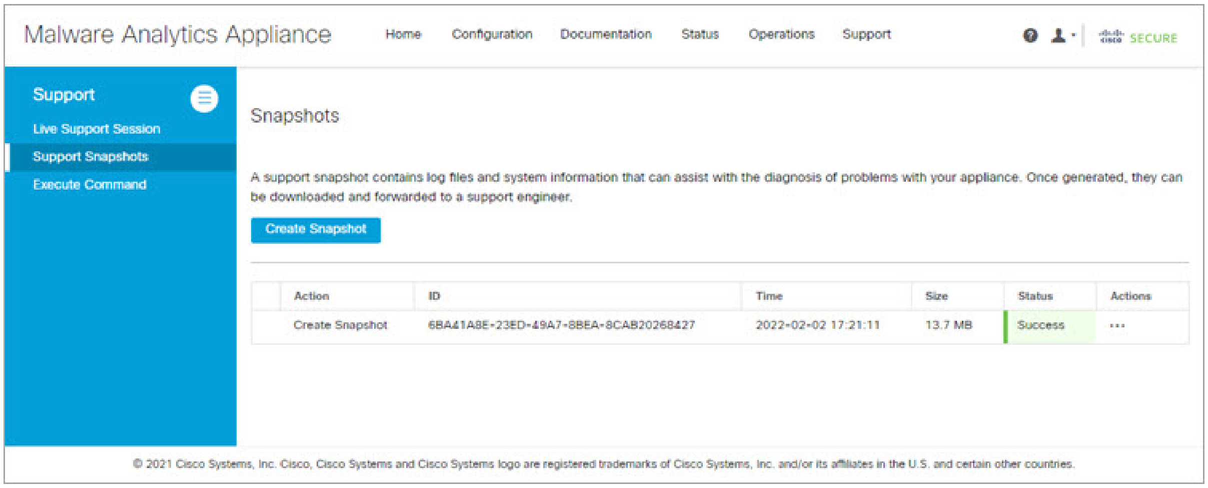
A support snapshot is basically a snapshot of the running system, which contains logs, psoutput, etc., to help Support staff troubleshoot any issues.

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

Procedure

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

Figure 57: Support Snapshots



Snapshots

A support snapshot contains log files and system information that can assist with the diagnosis of problems with your appliance. Once generated, they can be downloaded and forwarded to a support engineer.

	Action	ID	Time	Size	Status	Actions
	Create Snapshot	6BA41A8E-23ED-49A7-8BEA-8CAB20268427	2022-02-02 17:21:11	13.7 MB	Success	•••

© 2021 Cisco Systems, 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 **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.

CHAPTER 8

Organizations and Users

Secure Malware Analytics is installed on the Secure Malware Analytics Appliance with a default organization and Admin user. Once the set up and the network configuration is completed, you can create additional organization and user accounts, so users can log in and begin submitting malware samples for analysis.

Adding organizations, users, and administrators may require planning and coordination among multiple users and teams, depending on your organization. This chapter describes how to manage organizations and users in Secure Malware Analytics and includes the following topics:

Creating a New Organization

Users are always affiliated with an organization; before you can add users, you must first create the organization so you can add them to it. You must be logged in as an Admin to create a new organization, which is performed on the **Managing Organizations** page in the Secure Malware Analytics portal UI.

Important You cannot delete an organization from this interface once it has been created so plan this task carefully.

Procedure

Step 1 Log into the Secure Malware Analytics portal as Admin.

Step 2 Click the **Administration** tab and choose **Manage Organization**. The **Organizations** page opens and shows all the organizations on the appliance.

Step 3 Click **New Organization** in the upper-right corner of the page to open the **New Organization** dialog.

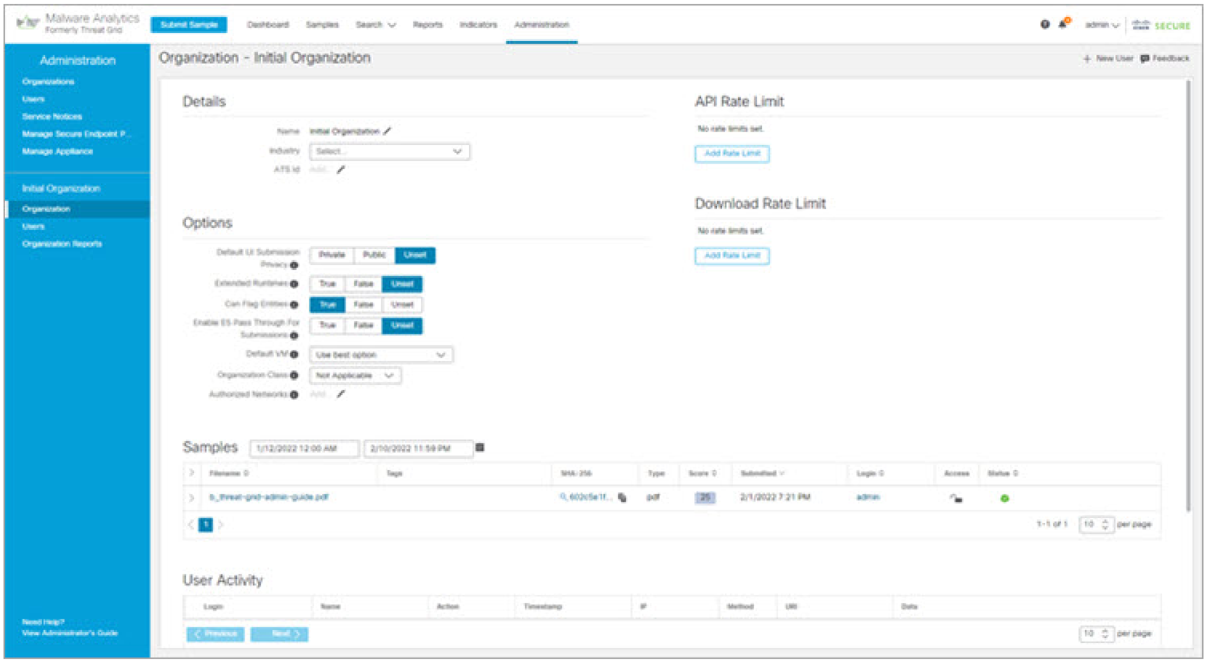
Step 4 Complete the following information:

- **Name** - Add a name for the organization (there is currently no size limit to the name).

- **Industry** - Choose the type of business from the **Industry** drop-down list. If none of the industries on the list are applicable, then leave it set to **Unknown**, and contact Secure Malware Analytics Opening a Support Case to request that an option be added.
- **ATS Id** - Enter the Advanced Threat Services ID.

Step 5 Click **Submit**. The new organization is created and is now visible in the list of Organizations.

Figure 58: Organization Page for the Default Initial Organization



Organization - Initial Organization

Details

Name: Initial Organization
Industry: Select...
ATS Id: Add

API Rate Limit

No rate limits set.

Add Rate Limit

Download Rate Limit

No rate limits set.

Add Rate Limit

Options

Default UI Submission Privacy	Private	Public	[✓ Unset]
Extended Runtimes	True	False	[✓ Unset]
Can Flag Entities	[✓ True]	False	Unset
Enable ES Pass Through For Submissions	True	False	[✓ Unset]

Default VM: Use best option
Organization Class: Not Applicable
Authorized Networks: Add

Samples 1/12/2022 12:00 AM 2/10/2022 11:59 PM

Filename	Tags	SHA-256	Type	Score	Submitted	Login	Access	Status
b_threat-grid-admin-guide.pdf		602c5e1f...	pdf	25	2/1/2022 7:21 PM	admin		●

1-1 of 1 10 per page

User Activity

Login	Name	Action	Timestamp	IP	Method	URI	Data

< Previous Next > 10 per page

Step 6 Edit the newly created organization and complete the following information:

- **Options** - Complete as appropriate.
- **Rate Limit** - Set the default user submission rate limit.

  The API rate limit is global for the Secure Malware Analytics Appliance under the terms of the license agreement. This affects API submissions only, not manual sample submissions. The rate limit in the license applies to the organization.

  You can also set sample submission rates on individual users, as documented in the Secure Malware Analytics portal online Help.

  Rate limits are based on a 24-hour window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error and a message about how long to wait before retrying.

Once the organization is created, the Admin or Organization Admin can manage it.

Managing Users

For instructions and documentation on creating and managing user accounts, including how to add users, see the Secure Malware Analytics Portal UI online help:

In the navigation bar, click **Help** > **Using Secure Malware Analytics Online Help** > **Managing Secure Malware Analytics Users**.

Note Users can only be removed via the API, and only if they have not submitted samples.

Managing device user accounts for integrating Email Security Appliances, Web Security Appliances, and other devices is described in Activating a New Device User Account.

Removing Organizations and Users

Organizations and users can be removed by an admin user with the Secure Malware Analytics API. An organization can only be removed if it has no users; if it has users, you must delete them before removing the organization. However, users can only be deleted if they have not submitted any samples.

- To remove an organization, use the Secure Malware Analytics API: /api/v3/organizations/:org-id and DELETE.
- To remove a user, use the Secure Malware Analytics API: /api/v3/users/:user-id and DELETE.

See the Secure Malware Analytics portal online help for API endpoint details.

Activating a New Device User Account

When the Cisco Email Security Appliance, Web Security Appliance, or other Cisco Sandbox API integration connects and registers itself with a Secure Malware Analytics Appliance, a new Secure Malware Analytics user account is automatically created. The initial status of the user account is de-activated. The device user account must be manually activated by a Secure Malware Analytics Appliance administrator before it can be used for submitting malware samples for analysis.

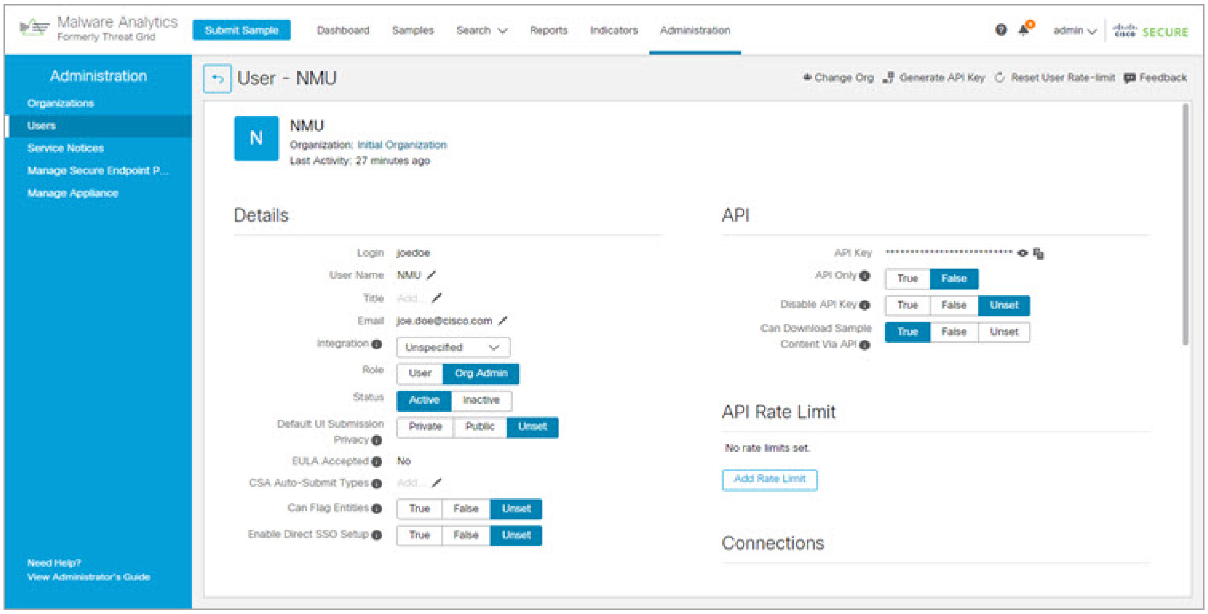
Procedure

Step 1 Log into the Secure Malware Analytics Portal UI as Admin.

Step 2 Click the **Administration** tab and choose **Manage Users**.

Step 3 Locate the device user account and open the **User Details** page.

Figure 59: User Details



User - NMU

N NMU
Organization: Initial Organization
Last Activity: 27 minutes ago

Details

Login	joedoe
User Name	NMU
Title	Add...
Email	joe.doe@cisco.com
Integration	Unspecified
Role	User [✓ Org Admin]
Status	[✓ Active] Inactive
Default UI Submission Privacy	Private Public [✓ Unset]
EULA Accepted	No
CSA Auto-Submit Types	Add...
Can Flag Entities	True False [✓ Unset]
Enable Direct SSO Setup	True False [✓ Unset]

API

API Key	••••••••••••••••••••••••••••
API Only	True [✓ False]
Disable API Key	True False [✓ Unset]
Can Download Sample Content Via API	[✓ True] False Unset

API Rate Limit

No rate limits set.

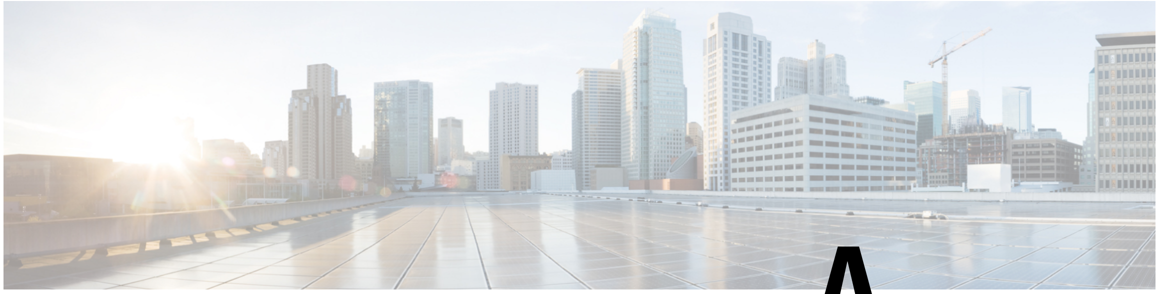
Connections

The user status is currently **Inactive**.

Step 4 Click **Activate**.

Step 5 On the confirmation dialog, confirm the action.

The integrating appliance or device can now communicate with the Secure Malware Analytics Appliance.



APPENDIX A

Inbound and Outbound Connections

You can set up Secure Malware Analytics Appliance to communicate with other Cisco appliances, devices, and services using inbound and outbound connections. Encrypted SSL connections allow other appliances (such as Email Security Appliance and Web Security Appliance) to submit possible malware samples to Secure Malware Analytics for analysis (inbound connections).

In addition, Secure Malware Analytics Appliance can be set up to communicate with Secure Endpoint Private Cloud for the Disposition Update Service through an outbound connection.

This appendix provides instructions for setting up both inbound and outbound connections.

- Connecting ESA or WSA to Secure Malware Analytics Appliance, on page 111
- Connecting Secure Endpoint Private Cloud to Secure Malware Analytics Appliance, on page 113

Connecting ESA or WSA to Secure Malware Analytics Appliance

Connections between the Secure Malware Analytics Appliance and Cisco Email Security Appliances (ESA) or Web Security Appliances (WSA) are enabled by the Cisco Sandbox API (CSA API) and are often referred to as CSA Integrations. The ESA/WSA must be registered with the Secure Malware Analytics Appliance before it can submit samples for analysis.

Before the ESA/WSA can be registered with the Secure Malware Analytics Appliance, the ESA/WSA administrator must first set up the SSL certificate connection as appropriate for their appliance and their network environment.

ESA/WSA Documentation

See the instructions for Enabling and Configuring File Reputation and Analysis Services in the ESA/WSA product documentation:

- *Cisco Email Security Appliance User Guides*
- *Cisco Web Security Appliance User Guides*

Note The Secure Malware Analytics Appliance is often referred to as an analysis service, or private cloud file analysis server in these guides.

Inbound Connection Overview

When setting up an inbound connection, the following tasks must be performed:

- **Set Up SSL Certificate** - The Secure Malware Analytics Appliance SSL certificate SAN (Subject Alternative Name), or the CN (Common Name) needs to match the hostname and the ESA/WSA expectations; for a successful connection with an integrating ESA/WSA, this must be the same hostname by which the integrating ESA/WSA identifies the Secure Malware Analytics Appliance.

  Depending on your requirements, you may need to regenerate the self-signed SSL certificate on the Secure Malware Analytics Appliance so it uses the current hostname in the SAN/CN field, then download it to your working environment and upload and install it onto the integrating ESA/WSA.

  Alternatively, you may need to replace the current Secure Malware Analytics Appliance SSL certificate by uploading an enterprise or commercial SSL certificate (or a manually generated certificate). For detailed instructions, see Configuring SSL Certificates.

- **Verify Connectivity** - Once the SSL certificate setup is complete, the next step is to verify that the ESA/WSA can communicate with the Secure Malware Analytics Appliance. The ESA/WSA must be able to connect to the Clean interface of the Secure Malware Analytics Appliance over your network. Follow the instructions in the product documentation to verify that the Secure Malware Analytics Appliance and ESA/WSA can communicate with each other (see Connecting ESA or WSA to Secure Malware Analytics Appliance).

- **Complete the ESA/WSA File Analysis Configuration** - Enable the **File Analysis Security** service and configure the advanced settings.

- **Register ESA/WSA with Secure Malware Analytics Appliance** - An ESA/WSA that is configured according to the product documentation, registers itself automatically with the Secure Malware Analytics Appliance. Upon registration of the connecting device, a new Secure Malware Analytics user is automatically created with the Device ID as the login ID, and a new organization is created with a name based on the same ID. An administrator must activate the new Device user account.

- **Activate the New ESA/WSA Account on the Secure Malware Analytics Appliance** - When the ESA/WSA or other integration connects and registers itself with the Secure Malware Analytics Appliance, a new Secure Malware Analytics user account is automatically created. The initial status of the user account is de-activated. A Secure Malware Analytics Appliance administrator must manually activate the device user account before it can be used for submitting malware samples for analysis.

Configuring Inbound Connection

The connection between the ESA/WSA is incoming from the perspective of the Secure Malware Analytics Appliance, and uses the CSA API.

Note Refer to the ESA and WSA product documentation for more information about the tasks that must be performed.

Procedure

Step 1 Set up and configure the Secure Malware Analytics Appliance as normal (no integration yet).

Step 2 Check for updates and install, if necessary.

Step 3 Set up and configure the ESA/WSA as normal (no integration yet).

Step 4 The Secure Malware Analytics Appliance SSL certificate SAN or CN must match its current Hostname and ESA/WSA Expectations. If you are deploying a self-signed SSL certificate, generate a new SSL certificate (on the Secure Malware Analytics Application Clean interface), to replace the default if needed, and download it to install on the ESA/WSA (see Replacing SSL Certificates).

Note
Be sure to generate a certificate that has the hostname of your Secure Malware Analytics Appliance as the SAN or CN (the default certificate from the Secure Malware Analytics Appliance will not work). Use the hostname; not the IP address.

Step 5 Verify that the ESA/WSA can connect to the Clean interface of the Secure Malware Analytics Appliance over your network.

Step 6 Configure the ESA/WSA for Secure Malware Analytics Appliance integration. See the ESA/WSA product documentation for complete instructions.

Step 7 Submit and commit your changes.

Registration of your ESA/WSA with the Secure Malware Analytics Appliance occurs automatically when you submit the configuration for File Analysis.

Step 8 Activate the new device user account on the Secure Malware Analytics Appliance:

a) Log into the Secure Malware Analytics Portal UI as Admin.
b) Click the **Administration** tab and choose **Manage Users** to open the **Users** page.
c) Click the user name to open the **User Details** page for the device user account (you may need to use Search to find it).
d) The user status is currently **Inactive**. Click **Active** to activate th enew account.
e) On the confirmation dialog, confirm the action.

The ESA/WSA can now initiate connections with the Secure Malware Analytics Appliance.

Connecting Secure Endpoint Private Cloud to Secure Malware Analytics Appliance

The Secure Malware Analytics Appliance supports integration with Secure Endpoint Private Cloud for the Disposition Update Service as an outbound connection.

Note The Secure Malware Analytics Appliance Disposition Update Service and Secure Endpoint Private Cloud integration setup tasks must be performed on the devices in the specified order, particularly if you are setting up new appliances. If you are integrating appliances that are already set up and configured, the order is not as critical.

Refer to the Secure Endpoint Private Cloud documentation for more detailed information on the tasks that must be performed.

Procedure

Step 1 Set up and configure the Secure Malware Analytics Appliance as normal (no integration yet). Check for updates and install, if necessary.

Step 2 Set up and configure the Secure Endpoint Private Cloud as normal (no integration yet).

Step 3 In the Secure Malware Analytics Appliance Admin UI, click the **Configuration** tab and choose **SSL**.

Step 4 Regenerate the SSL certificate on the Clean interface to replace the default certificate, if needed, and make a copy of it to install on the Secure Endpoint Private Cloud device (see Regenerating SSL Certificates for more information).

Step 5 Obtain the following information, which is needed to configure the integration in Secure Endpoint Private Cloud device:

- **Hostname** - Click **Configuration** > **Hostname** and note the hostname.
- **API Key** - Copy the **API Key** from the **User Details** page in the Secure Malware Analytics portal (click the **Administration** tab and choose **Manage Users**, and then navigate to the integration user account to locate the API key on the **User Details** page).

  Note
  This does not need to be the Admin user; it can be a user that was specifically created for this purpose on the Secure Malware Analytics Appliance.

Step 6 Configure the Secure Endpoint Private Cloud device for Secure Malware Analytics Appliance integration. See the ESA/WSA product documentation for complete instructions. The configuration will allow AMP to talk to the Secure Malware Analytics Appliance; you can now submit samples to Secure Malware Analytics.

Step 7 Complete the remaining steps to set up the Disposition Update Service to communicate disposition results to the Secure Malware Analytics Appliance (for more information, see the user documentation for Secure Endpoint Private Cloud):

a) Configure DNS, if needed. See Configuring DNS.

b) Download or copy and paste the Secure Endpoint Private Cloud SSL certificate to the Secure Malware Analytics Appliance so it can trust the integrating device. See CA Certificates.

c) In the Secure Malware Analytics portal UI, specify the AMP Disposition Update Service URL and credentials and click **Add** (see Managing Disposition Update Syndication Services).

Managing Disposition Update Syndication Services

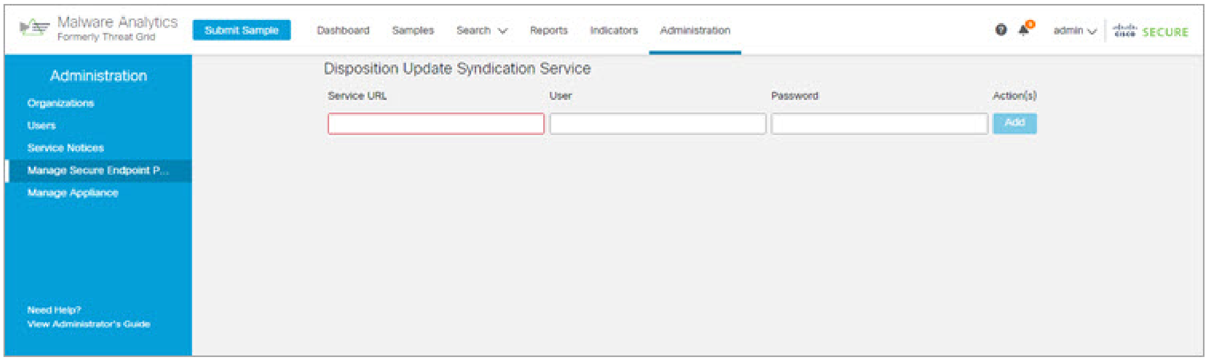
You can manage the Disposition Update Syndication Service for Secure Endpoint Private Cloud appliance integrations in the Secure Malware Analytics portal. URLs can be added, edited, and deleted from the **Disposition Update Syndication Service** page.

Note For more information about Secure Endpoint Private Cloud appliance integrations, see Connecting Secure Endpoint Private Cloud to Secure Malware Analytics Appliance.

Procedure

Step 1 In the Secure Malware Analytics portal, click the **Administration** tab and choose **Manage Secure Endpoint Private Cloud Integration** to open the **Disposition Update Syndication Service** page.

Figure 60: Disposition Update Syndication Service



Step 2 Enter the following information:

- **Service URL** - The Secure Endpoint Private Cloud URL.
- **User** - The admin user name.
- **Password** - The password provided by the Secure Endpoint configuration portal.

Step 3 Click **Add**.

APPENDIX B

Removing All Data with the Wipe Appliance Operation

This appendix describes how to use the Wipe Appliance operation to remove all data from the Secure Malware Analytics Appliance. It includes the following topics:

About Wipe Appliance

The Wipe Appliance boot option enables you to wipe the disks on a Secure Malware Analytics Appliance to remove all data prior to decommissioning or returning it to the Cisco Demo Loan Program.

Note The Wipe Appliance boot option should not be confused with Data Reset, which prepares an appliance to restore a backup by clearing operating system logs and other state with the `destroy-data` command.

Important After performing the wipe appliance procedure, the Secure Malware Analytics Appliance will no longer operate without being returned to Cisco for reimaging.

Wipe Appliance Procedure

This operation is only available in recover-mode tgsh, not tgsh as started from Admin TUI. Perform the following steps to wipe all data from the appliance:

Procedure

Step 1 Reboot the appliance (click the **Operations** tab, choose **Power**, and then click the **Reboot** button).

Step 2 Press **F6** at the BIOS window for a list of possible boot targets, and choose **Recovery**.

The Secure Malware Analytics Shell opens in Recovery Mode. (See Figure 6 in Resetting the Administrator Password)

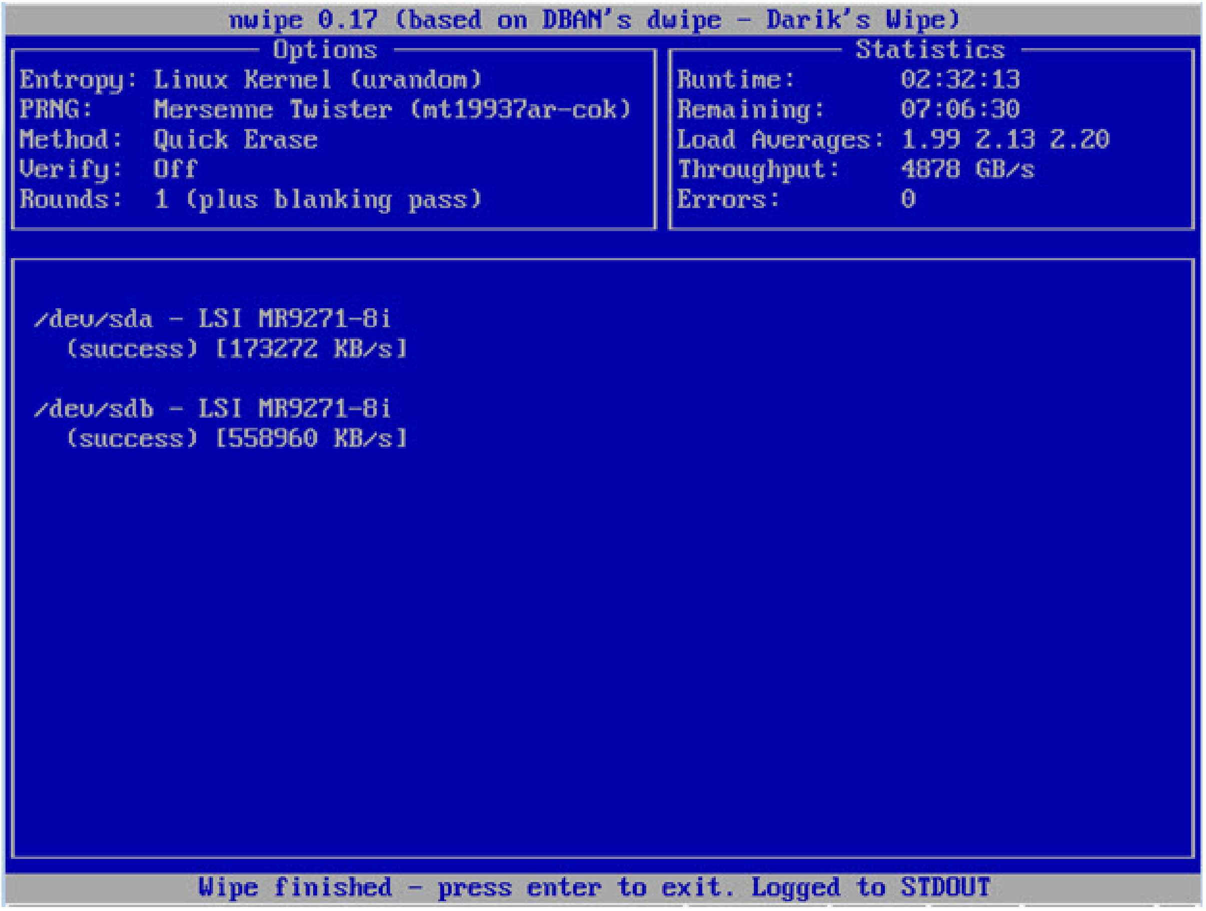
Step 3 Run one of the following commands in recovery-mode tgsh. These vary only in performance and (theoretically) level of security (although with modern drives, even the fast mechanism is likely to provide very good security).

- service start wipe-fast
- service start wipe-random
- service start wipe-3pass

Immediately after running any of these commands, the Wipe process will start.

The **Wipe Finished** window is displayed when the wipe operation is complete.

Figure 61: Wipe Finished



```
              nwipe 0.17 (based on DBAN's dwipe - Darik's Wipe)
 --------------- Options ---------------   ----------- Statistics -----------
 Entropy: Linux Kernel (urandom)           Runtime:        02:32:13
 PRNG:    Mersenne Twister (mt19937ar-cok) Remaining:      07:06:30
 Method:  Quick Erase                      Load Averages: 1.99 2.13 2.20
 Verify:  Off                              Throughput:     4878 GB/s
 Rounds:  1 (plus blanking pass)           Errors:         0

  /dev/sda - LSI MR9271-8i
    (success) [173272 KB/s]

  /dev/sdb - LSI MR9271-8i
    (success) [558960 KB/s]

           Wipe finished - press enter to exit. Logged to STDOUT
```

Step 4 Press **Enter** to exit.

Wipe Appliance and Clusters

After performing a wipe operation, the Secure Malware Analytics Appliance will no longer operate unless it is returned to Cisco for reimaging. Wipe should only be used on a cluster node after that node has been flagged in the Admin UI as permanently removed.

APPENDIX C

CIMC Configuration

The Cisco Integrated Management Controller (CIMC) Configuration is the user interface used to manage the server. This appendix includes the following information about using the CIMC Utility to set up remote server management:

Using CIMC Configuration Utility

After booting the server, the Cisco screen is displayed, which allows you to enter the Cisco Integrated Management Controller (CIMC) Configuration Utility. The CIMC interface can be used for remote server management.

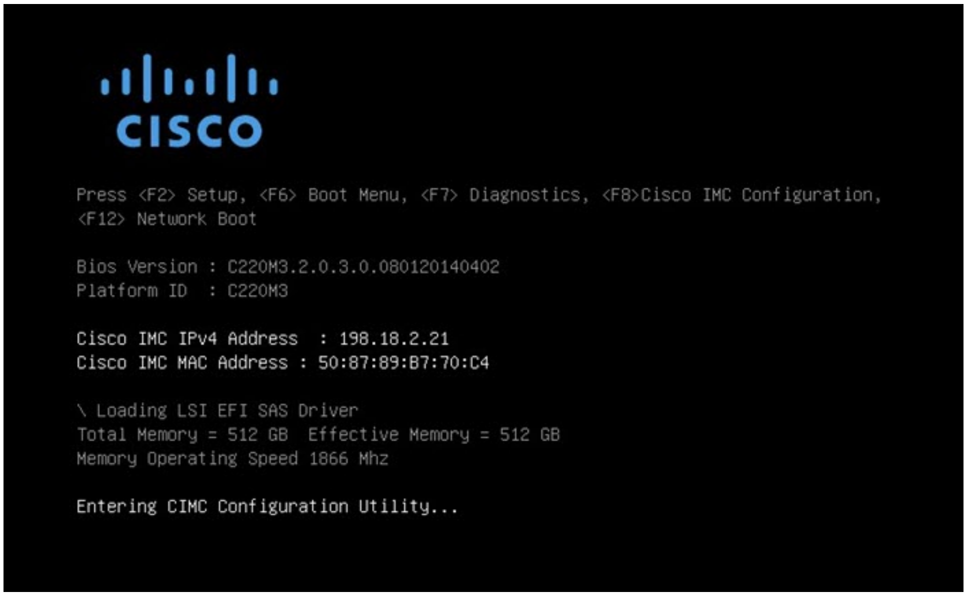
A monitor and keyboard must be attached directly to the Secure Malware Analytics Appliance to use this utility.

Note CIMC is not supported on Secure Malware Analytics M5 Appliance servers.

Procedure

Step 1 Power on the server.

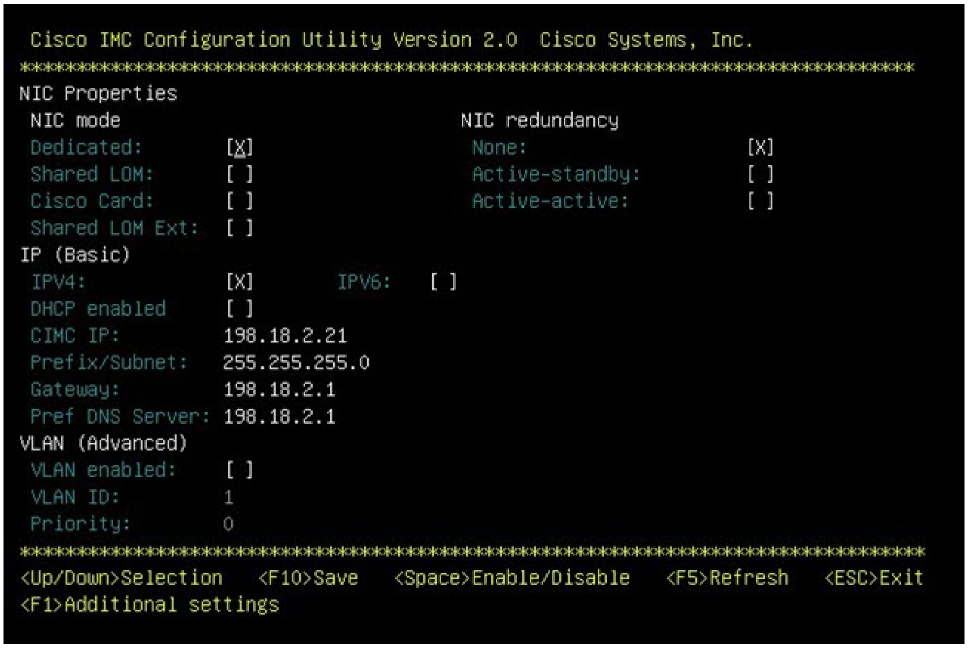
Figure 62: Cisco Screen



```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M3.2.0.3.0.080120140402
Platform ID  : C220M3

Cisco IMC IPv4 Address  : 198.18.2.21
Cisco IMC MAC Address : 50:87:89:B7:70:C4

\ Loading LSI EFI SAS Driver
Total Memory = 512 GB  Effective Memory = 512 GB
Memory Operating Speed 1866 Mhz

Entering CIMC Configuration Utility...
```

Step 2 After the memory check is completed, press **F8** to enter the CIMC Configuration Utility.

Figure 63: CIMC Configuration Utility



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
********************************************************************************
NIC Properties
 NIC mode                              NIC redundancy
 Dedicated:         [X]                 None:                   [X]
 Shared LOM:        [ ]                 Active-standby:         [ ]
 Cisco Card:        [ ]                 Active-active:          [ ]
 Shared LOM Ext:    [ ]
IP (Basic)
 IPV4:              [X]         IPV6:    [ ]
 DHCP enabled       [ ]
 CIMC IP:           198.18.2.21
 Prefix/Subnet:     255.255.255.0
 Gateway:           198.18.2.1
 Pref DNS Server:   198.18.2.1
VLAN (Advanced)
 VLAN enabled:      [ ]
 VLAN ID:           1
 Priority:          0
********************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F1>Additional settings
```

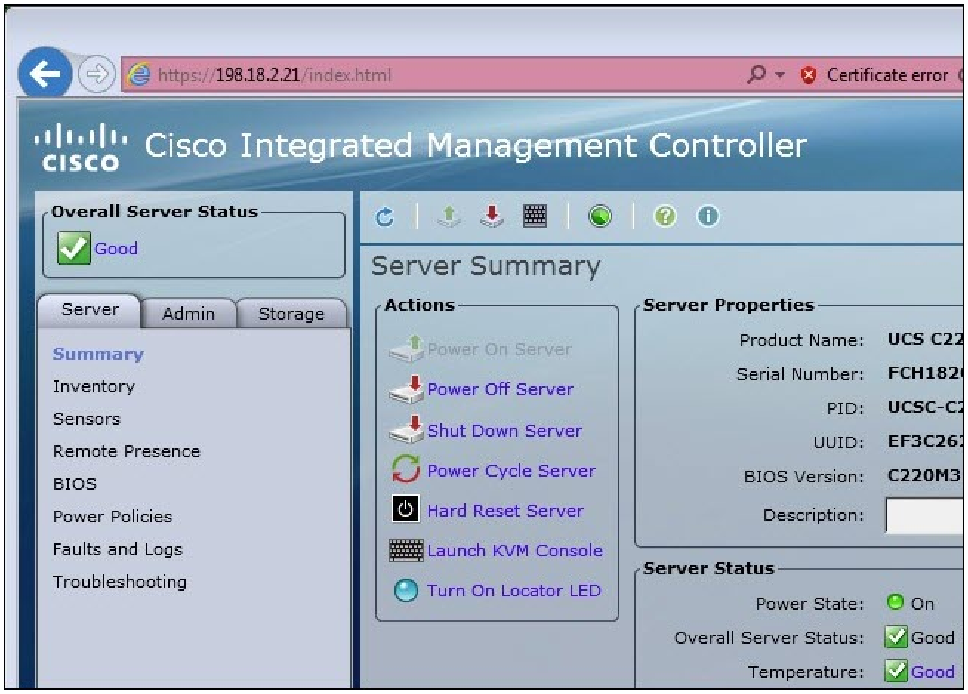
Step 3 In the CIMC configuration utility, set up an IP address that can be used for remote server management.

Step 4 Save the configuration and exit the utility.

Step 5 In a web browser, enter **https://<CIMC-IP address>/** to open the CIMC interface.

Step 6 Enter the initial **User Name** (admin) and **Password** (password).

Figure 64: Cisco Integrated Management Controller (CIMC) Interface



https://198.18.2.21/index.html

Certificate error

Cisco Integrated Management Controller

Overall Server Status: Good

Server Summary

Server Properties

Product Name: UCS C22

Serial Number: FCH182

PID: UCSC-C2

UUID: EF3C26

BIOS Version: C220M3

Description:

Server Status

Power State: On

Overall Server Status: Good

Temperature: Good

The CIMC interface can now be used to view the server health and open a KVM to complete the remaining setup steps remotely.