Cisco Secure Malware Analytics Appliance Getting Started Guide Version 2.19

First Published: 2020-12-15

Last Modified: 2024-09-06

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 –2024 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Introduction** 1

About Cisco Secure Malware Analytics Appliance 1

Audience 2

Assumptions 2

Product Documentation 2

What's New In This Release 3

Supported Browsers 3

Updates 3

Support 3

Setup and Configuration Overview 6

CHAPTER 2 **Initial Network Configuration** 7

Power On and Boot Up Appliance 7

Configure Network Using Admin TUI 8

CHAPTER 3 **Admin UI Configuration** 11

Introduction 11

Log In to the Admin UI 12

Change Admin Password 13

Review End User License Agreement 13

Configuration Wizard 14

Home 15

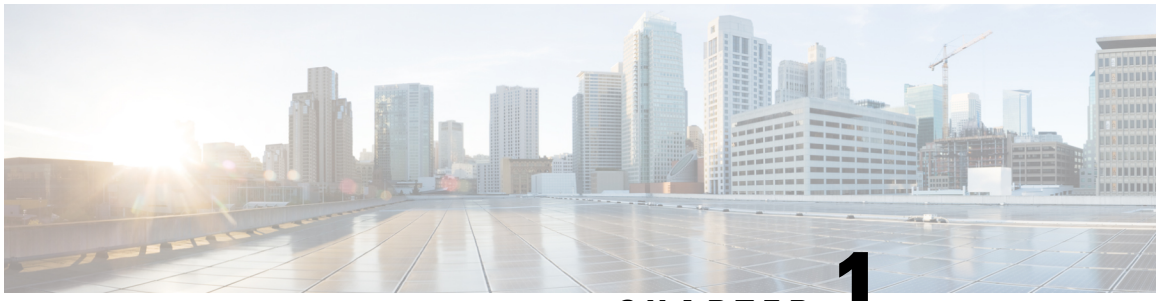
Configure Network Settings 15

Configure NFS 16

Configure Clustering 17

Configuring First Cluster Node 18

Joining Additional Cluster Nodes 18
Install License 19
Configure Email 20
Configure Notifications 21
Configure Date and Time 22
Configure System Log 23
Review and Install Configuration Settings 24
Install Secure Malware Analytics Appliance Updates 27
Test the Appliance Setup 28



CHAPTER 1

Introduction

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

- About Cisco Secure Malware Analytics Appliance, on page 1
- Audience, on page 2
- Assumptions, on page 2
- Product Documentation, on page 2
- What's New In This Release, on page 3
- Supported Browsers, on page 3
- Updates, on page 3
- Support, on page 3
- Setup and Configuration Overview, on page 6

About Cisco Secure Malware Analytics Appliance

The Cisco Secure Malware Analytics appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. A Secure Malware Analytics Appliance provides the complete malware analysis platform, installed on a Cisco Secure Malware Analytics M5 Appliance server (v2.7.2 and later). It empowers organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.

Note Cisco UCS C220 M4 (TG5400) servers are still supported for Secure Malware Analytics Appliance but the servers are end of life. See the Server Setup chapter in the *Cisco Secure Malware Analytics Appliance Setup and Configuration Guide* (v2.7 and earlier) for instructions.

Many organizations that handle sensitive data, such as banks and health services, must follow various regulatory rules and guidelines that do not allow certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Cisco Secure Malware Analytics Appliance on-premises, organizations can send suspicious documents and files to it to be analyzed without leaving the network.

With a Secure Malware Analytics Appliance, security teams can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. The appliance correlates the analysis results with hundreds of millions of previously analyzed malware artifacts, to provide a global view of malware attacks and campaigns, and their distributions. A single sample of observed activity and characteristics can quickly

be correlated against millions of other samples to fully understand its behaviors within an historical and global context. This ability helps security teams to effectively defend the organization against threats and attacks from advanced malware.

Audience

Before a new appliance can be used for malware analysis, it must be set up and configured for the organization's network. This guide is intended for the security team IT staff tasked with setting up and configuring a new Secure Malware Analytics Appliance.

This document describes how to complete the initial setup and configuration for a new Secure Malware Analytics Appliance, up to the point where malware samples can be submitted to it for analysis.

Assumptions

It is assumed that you have gathered the necessary information and completed the planning steps as described in the *Cisco Secure Malware Analytics Appliance Administration Guide*.

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

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

Product Documentation

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

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

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

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

Secure Malware Analytics Portal UI Online Help

Secure Malware Analytics Portal user documentation, including Release Notes, Secure Malware Analytics Online Help, API documentation, and other information is available from the **Help** menu located in the navigation bar at the top of the user interface.

What's New In This Release

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

Table 1: Changes in Version 2.19 Release

Feature or Update	Section
Enhanced dashboard in the Admin UI	Home, on page 15
In TGSH, you can now ping via a clean and dirtly interface	

Supported Browsers

Secure Malware Analytics supports the following browsers:

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

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

Updates

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

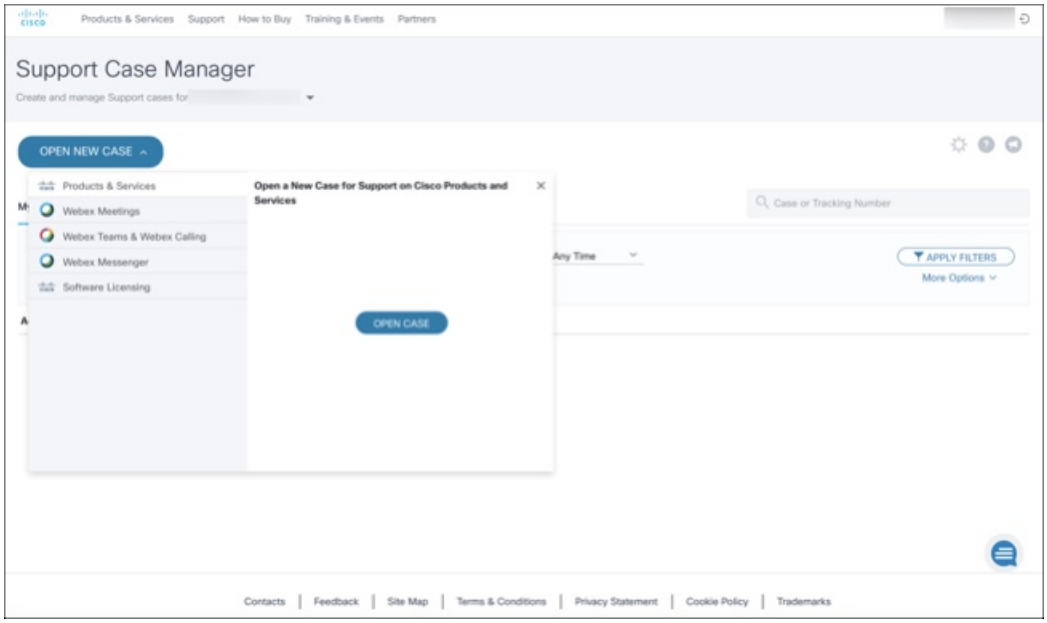
Secure Malware Analytics Appliance updates cannot be downloaded until the license is installed, and the update process requires that the initial appliance configuration is completed. Updates must be done in sequence.

Support

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

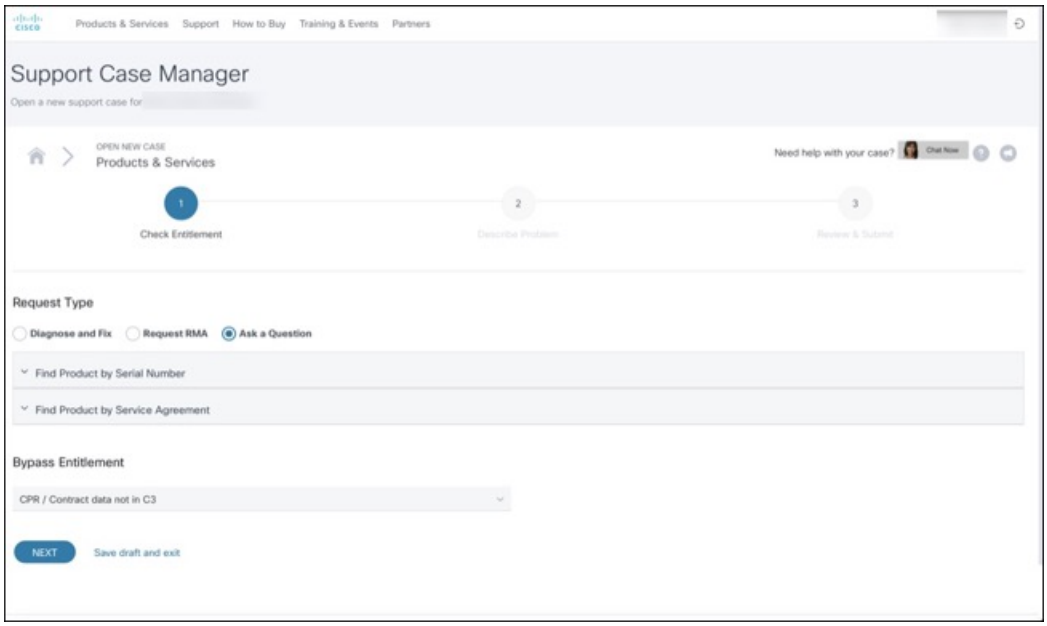
Step 1 In Support Case Manager, click **Open New Case > Open Case**.

Figure 1: Open New Case



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

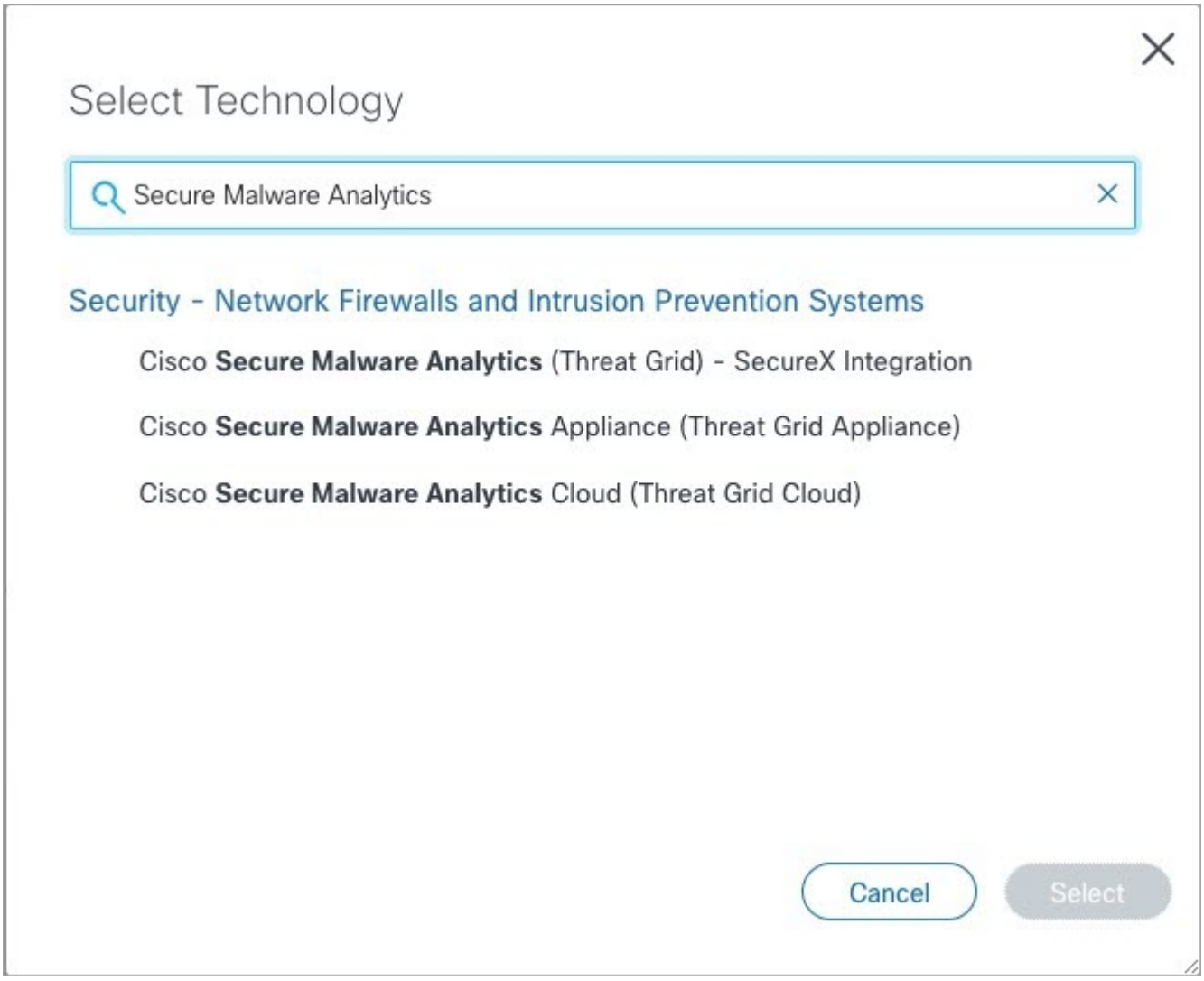
Figure 2: Check Entitlement



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

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

Figure 3: Select Technology



Step 5 Choose **Cisco Secure Malware Analytics Appliance** from the list and click **Select**.

Step 6 Complete the remainder of the form and click **Submit**.

If you are unable to open a case online, contact Cisco Support:

- **US and Canada**: 1-800-553-2447
- **Worldwide Contacts**: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

For additional information on how to request support:

- See Enable Support Mode and Support Snapshots in the *Secure Malware Analytics Appliance Administration Guide*.
- See the blog post: **Changes to the Cisco Secure Malware Analytics Support Experience** at https://community.cisco.com/t5/security-blogs/changes-to-the-cisco-threat-grid-support-experience/ba-p/3911407

- See the main **Cisco Support & Downloads** page at: https://www.cisco.com/c/en/us/support/index.html

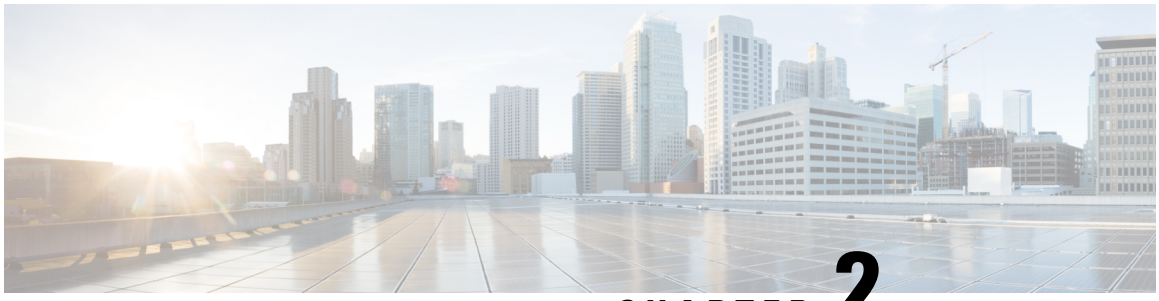
Setup and Configuration Overview

The following setup and initial configuration steps are described in this guide:

- Initial Network Configuration
- Admin UI Configuration
- Installing Updates
- Testing Appliance Setup

Note You should allow approximately 1 hour to complete the configuration.

Additional tasks that require administrator configuration (such as license installation, email server, and SSL certificates) are documented in the *Cisco Secure Malware Analytics Appliance Administration Guide*.



CHAPTER 2

Initial Network Configuration

This chapter provides instructions for completing the initial network configuration using the Admin TUI (Text-mode UI). It includes the following topics:

- Power On and Boot Up Appliance, on page 7
- Configure Network Using Admin TUI, on page 8

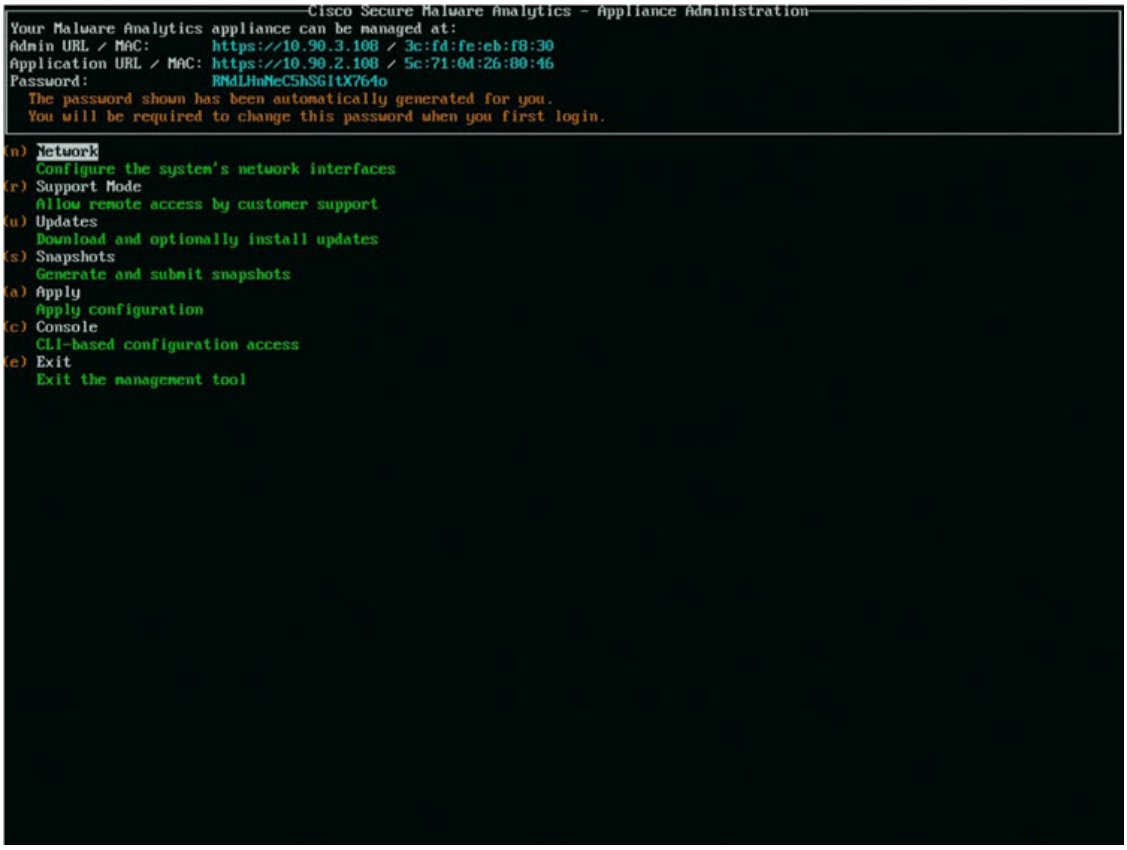
Power On and Boot Up Appliance

Once you have connected the server peripherals, network interfaces, and power cables, turn on the Secure Malware Analytics M5 Appliance and wait for it to boot up. The Cisco screen is briefly displayed.

Figure 4: Cisco Screen During Bootup

The **Admin TUI** is displayed on the console when the server has successfully booted up and connected.

Figure 5: Admin TUI



The Admin URL shows as unavailable because the network interface connections are not yet configured and the Admin UI cannot be reached yet to perform this task.

Important The **Admin TUI** displays the initial administrator Password, which will be needed to access and configure the Admin UI later in the configuration. Make a note of the Password in a separate text file (copy and paste).

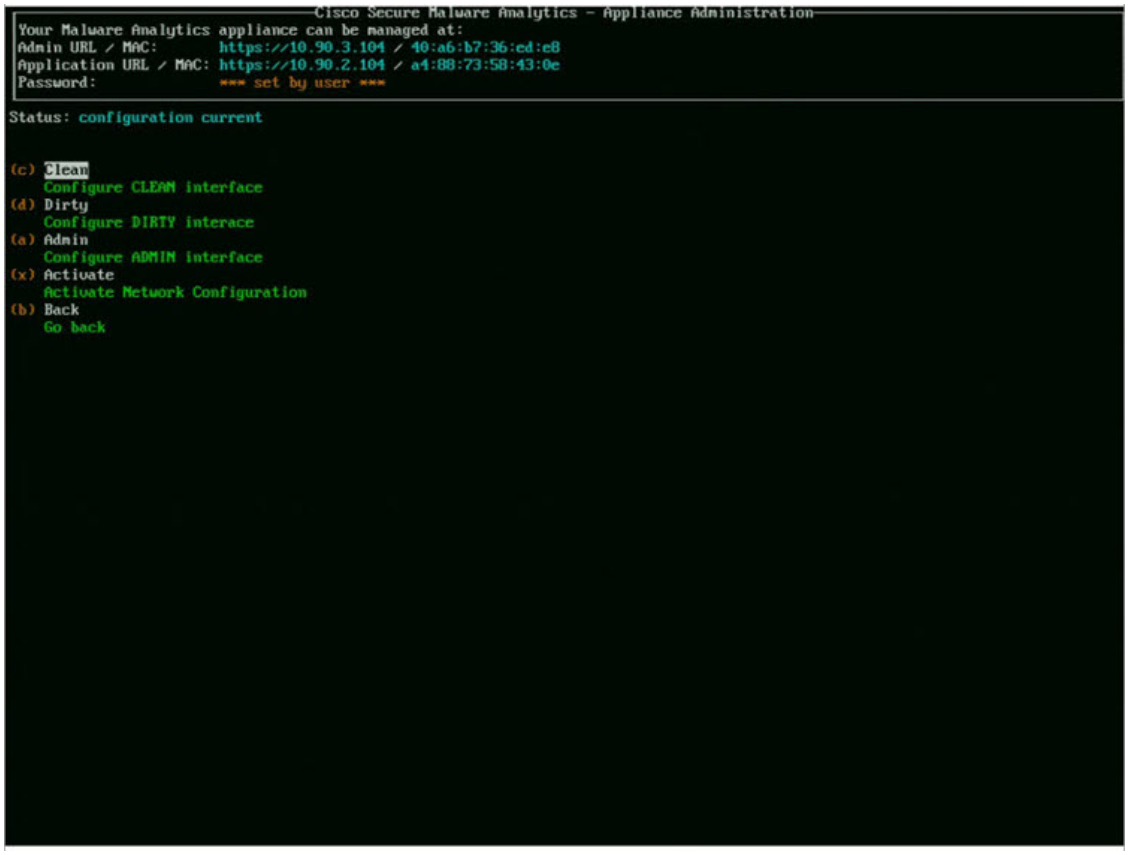
Configure Network Using Admin TUI

The initial network configuration is completed in the Admin TUI. The basic configuration, once completed, allows access to the Admin UI, where you can complete additional configuration tasks.

Note For DHCP users, the following steps assume that you are using static IP addresses. If you are using DHCP to obtain your IP addresses, see the *Cisco Secure Malware Analytics Appliance Administration Guide*.

Step 1 On the Admin TUI, select **NETWORK**. The **Status: configuration current** screen appears.

Figure 6: Admin TUI - Network Configuration Console



Step 2 Select **Clean**. The **Network Config - CLEAN Interface** screen appears.

Step 3 Complete the blank fields according to the settings provided by your network administrator.

Step 4 Select **Save**.

Step 5 Select **Dirty**. The **Network Config - Dirty Interface** Interface screen appears.

Step 6 Complete the blank fields according to the settings provided by your network administrator.

Step 7 Select **Save**.

Step 8 Select **Admin**. The **Network Config - ADMIN Interface** Interface screen appears.

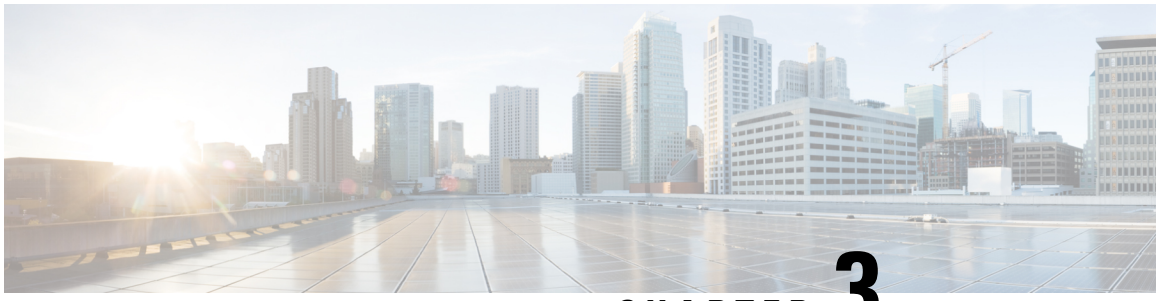
Step 9 Complete the blank fields according to the settings provided by your network administrator.

Step 10 Select **Save**.

Step 11 Select **Activate**. To activate the configuration.

What to do next

The next step in the Secure Malware Analytics Appliance setup is to complete the remaining configuration tasks using the Admin UI, as described in Admin UI Configuration.



CHAPTER 3

Admin UI Configuration

This chapter provides instructions for configuring your appliance using the Admin UI. It includes the following topics:

- Introduction, on page 11
- Configuration Wizard, on page 14
- Install Secure Malware Analytics Appliance Updates, on page 27
- Test the Appliance Setup, on page 28

Introduction

The Admin UI is the recommended tool for administrators to use to configure the Secure Malware Analytics Appliance. It is a Web user interface that can be used once an IP address has been configured on the Admin interface.

The configuration includes the following steps:

- Change Admin UI Admin Password
- Review End User License Agreement
- Configure Network Settings
- Install License
- Configure NFS
- Configure Clustering
- Configure Email
- Configure Notifications
- Configure Date and Time
- Configure System Log
- Review and Install Configuration Settings

Note Not all configuration steps are completed using the configuration wizard. See the *Cisco Secure Malware Analytics Appliance Administration Guide* for configuring settings not included in the wizard, such as SSL Certificates and Backups.

Important The steps in the following sections should be completed in one session to reduce the chance of an interruption to the IP address during configuration.

Log In to the Admin UI

Perform the following steps to log in to the Secure Malware Analytics Admin UI.

Step 1 In a browser, enter the URL for the Admin UI (**https://<adminIP>/** or **https://<adminHostname>/**) to open the Secure Malware Analytics Admin UI login screen.

Note The Hostname is the appliance serial number.

Figure 7: Admin UI Login Screen

Step 2 Enter the initial **Admin Password** that you copied from the Admin TUI and click **Log In**.

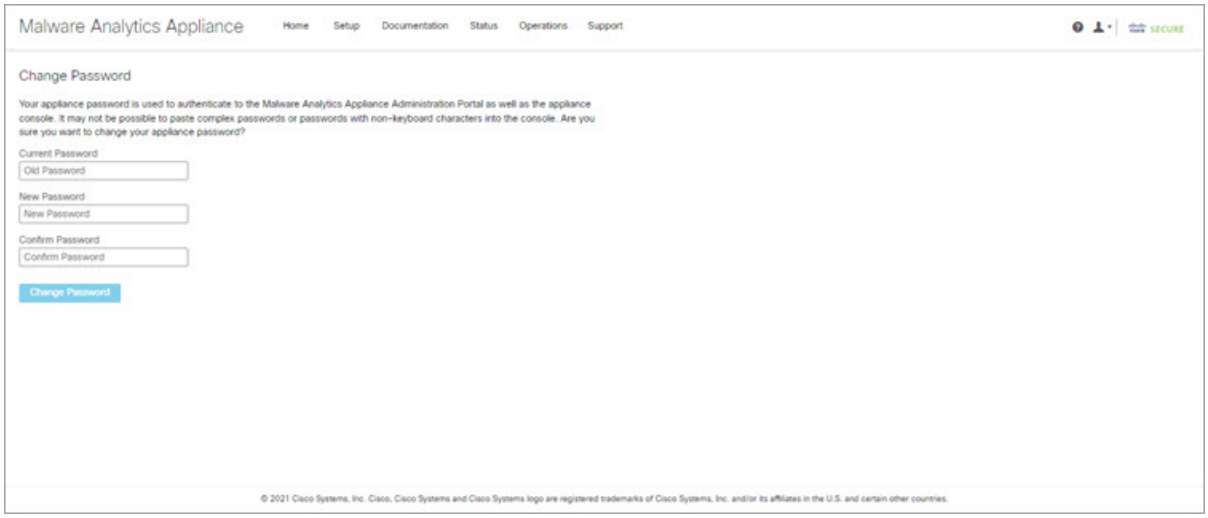
What to do next

Proceed to Change Admin Password.

Change Admin Password

The initial Admin password was generated randomly during the pre-ship Secure Malware Analytics installation and is visible as plain text in the Admin TUI. You must change the initial Admin password before continuing with the configuration.

Figure 8: Change Admin Password



Step 1 Enter the old password from the Admin TUI in the **Current Password** field. (You should have this password saved in a text file.)

Step 2 Enter a **New Password** and re-enter it in the **Confirm New Password** field.

The new password must contain the following: 8 characters minimum, one number, one special character, at least one uppercase and one lowercase character.

Step 3 Click **Change Password**. The password is updated.

Note The new password will not be displayed in visible text in the Admin TUI so be sure to save it somewhere.

What to do next

Proceed to Review End User License Agreement.

Review End User License Agreement

Review the license agreement and confirm that you agree to it.

Step 1 Review the End User License Agreement.

Step 2 Scroll to the end and click **I HAVE READ AND AGREE**.

Note We recommend that you follow the configuration workflow and configure the networks before you install the license.

What to do next

Proceed to Configure Network Settings.

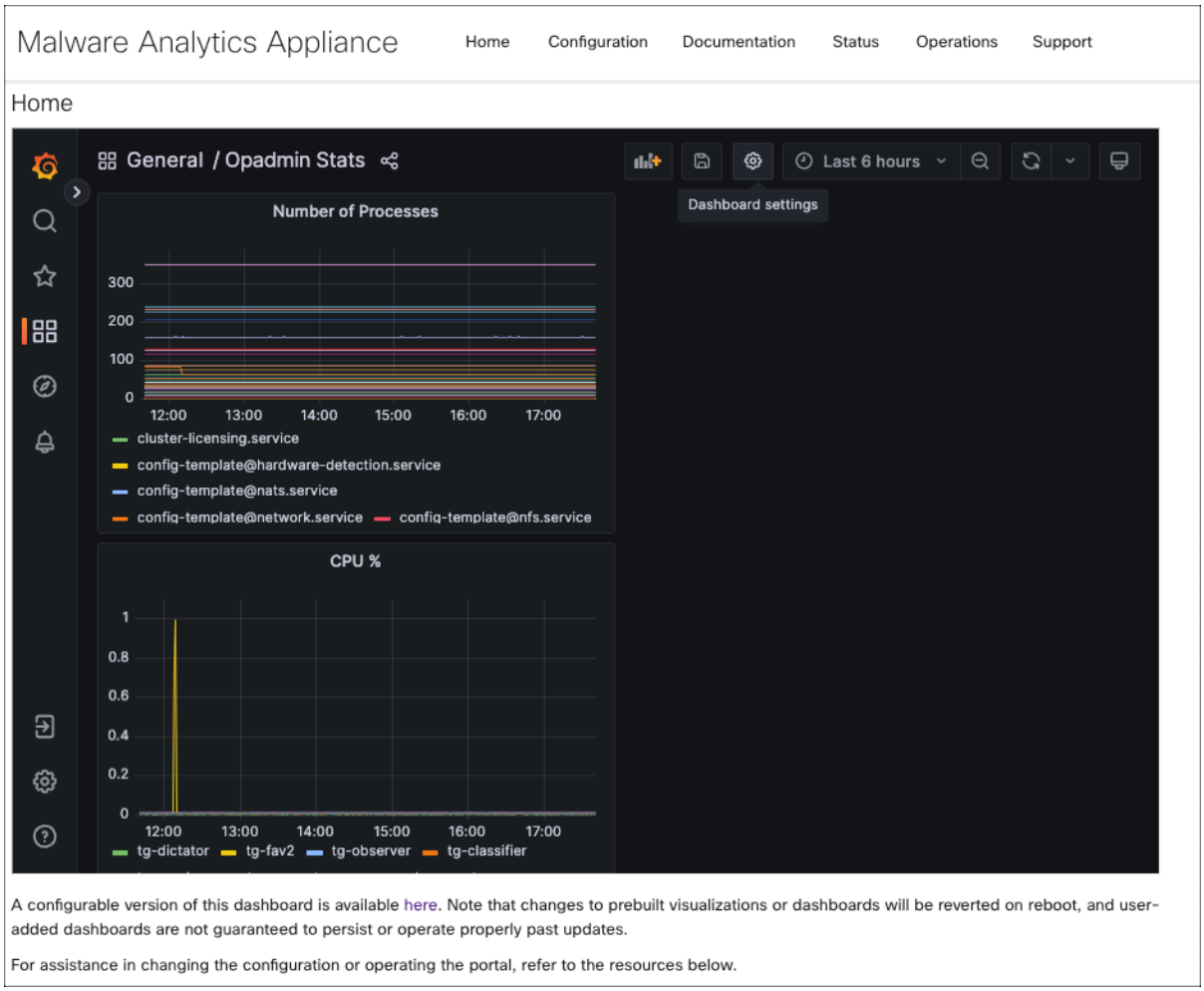
Configuration Wizard

The Configuration wizard takes you through configuring your Secure Malware Analytics Appliance.

If you need to make changes after you have completed the wizard configuration, you can access the settings from the **Configuration** tab in the Admin UI.

Home

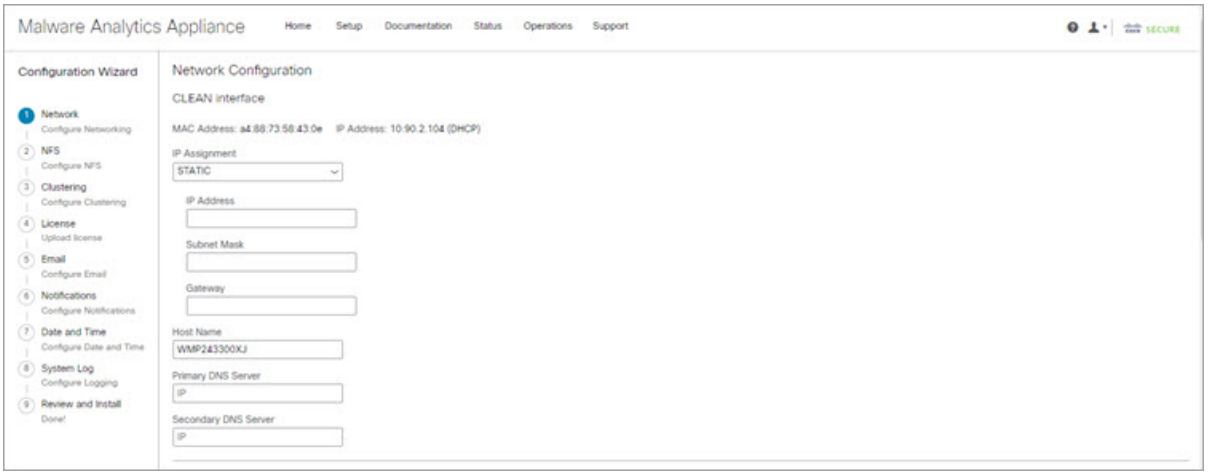
Figure 9: Home



Configure Network Settings

If you configured static network settings in the Admin TUI, the IP addresses displayed on the **Network Configuration** page reflect the values you entered in the Admin TUI during the Secure Malware Analytics Appliance network configuration.

Figure 10: Network Configuration



Step 1 Review the IP addresses and confirm they are accurate.

Step 2 If you used DHCP for your initial connection and now need to change the Clean and Dirty IP networks to static IP addresses, follow the steps in the Using DHCP section of the Cisco Secure Malware Analytics Appliance Administration Guide.

What to do next

Proceed to Configure NFS, on page 16.

Configure NFS

The next step in the workflow is NFS configuration. This task is required for backups and for clustering. See the NFS Requirements section in the *Cisco Secure Malware Analytics Appliance Administration Guide* for more information.

The configuration process includes mounting the NFS store, mounting the encrypted data, and initializing the Secure Malware Analytics Appliance local datastores from the contents of the NFS store.

If you would like to skip this step or continue and return later, click **Continue without NFS**.

Step 1 Click **NFS** in the navigation pane to open the **NFS Configuration** page.

Step 2 Enter the following information. Appliances in a cluster should share the same Host and Path as those set in the first cluster node.

- **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. 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. 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.)

The **Status** is **Enabled_Pending Key**.

Step 3 Click **Save**. The page refreshes and the **Generate Key** and **Activate** buttons become available.

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. 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.

Step 4 Click **Generate Key** to generate a new NFS encryption key.

Step 5 Click **Activate**. The **State** changes to **Active**. The **Upload** button changes to **Download.**

Step 6 Click **Download** to download a copy of the encryption key for safekeeping.

If this appliance is the first node in a cluster, you will need the key for joining additional nodes to the cluster. If the first node has already been configured, then click **Upload** and choose the NFS encryption key you downloaded from the first node when you started the new cluster.

Step 7 Click **Save**.

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

Step 8 Click**Activate**.

The **Status** changes to **Active** after a few seconds (lower left corner).

Step 9 When activation has succeeded, click **Continue**.

What to do next

Proceed to Configuring First Cluster Node.

Configure Clustering

The next step in the wizard workflow is to configure clustering. If the appliance being configured is not going to be part of a cluster, then skip to the next configuration step, Install License, on page 19.

The main goal of clustering is to increase the sample analysis capacity of a single system. Each appliance in a cluster saves data in the shared file system, and has the same data as the other nodes in the cluster. Clustering does not increase storage capacity, and it does not increase the *speed* of sample analysis. Instead, clustering makes it possible to analyze more samples in the same amount of time that you can achieve with a single appliance. Because the data is the same on all nodes, sample analysis can be passed from the submitting node to another cluster node that is not as busy. Clusters can include 2-7 appliances.

Clustering also helps support recovery from failure of one or more appliances in the cluster, depending on the cluster size.

You can create a cluster with new appliances, with appliances that have had their data removed (not Wiped), or a combination of new and existing appliances. When joining a Secure Malware Analytics Appliance to a cluster, it's convenient if the NFS and clustering are configured during the initial setup. You can start a cluster

post-installation from the **Cluster Configuration** page, but you can't join an installed appliance into an existing cluster.

For more information about clustering, see the *Secure Malware Analytics Appliance Administrator Guide v2.17*.

If you have questions about installing or reconfiguring clusters, contact Support for assistance.

Note If you are joining an existing appliance to a cluster, remove existing data with the `destroy-data`command, as documented in Reset Appliance as Backup Restore Target section in the *Secure Malware Analytics Appliance Administrator Guide v2.17*. Do not use the Wipe Appliance feature.

Configuring First Cluster Node

Begin a cluster by configuring the first node, and then configure each additional node and join them to the cluster using the NFS key that you downloaded when you configured the first node.

If you've already configured the first node, go to Joining Additional Cluster Nodes.

Clusters are configured and managed in the Admin UI on the **Cluster Configuration** page . 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).

Step 1 Click **Clustering** in the navigation pane to open the **Cluster Configuration** page.

Step 2 Click **Start Cluster** and then click **OK** on the confirmation dialog.

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

Step 3 Complete the remaining steps in the wizard and click **Start Installation**. This initiates a restore of the data in cluster mode.

Step 4 Check the health of the newcluster on the **Clustering** page.

What to do next

Proceed to Joining Additional Cluster Nodes

Joining Additional Cluster Nodes

This section describes how to join additional appliances to a cluster. It assumes that the first appliance in the cluster is configured as described in Configuring First Cluster Node. You can now start the configuration steps for the next node.

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

Step 2 Specify the **Host** and **Path** to match what was set in the first node in the cluster.

Step 3 Click **Save**. The page refreshes and the **Upload** button becomes available.

Step 4 In the **Configuration** menu, choose **Clustering** to open the **Cluster Configuration** page.

Step 5 Click **Join Cluster** and then click **OK** on the confirmation dialog.

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

Step 6 Finish the installation. This will initiate a restore of the data in cluster mode.

Step 7 Repeat the procedure for each node you want to join to the cluster.

What to do next

Proceed to Install License, on page 19.

Install License

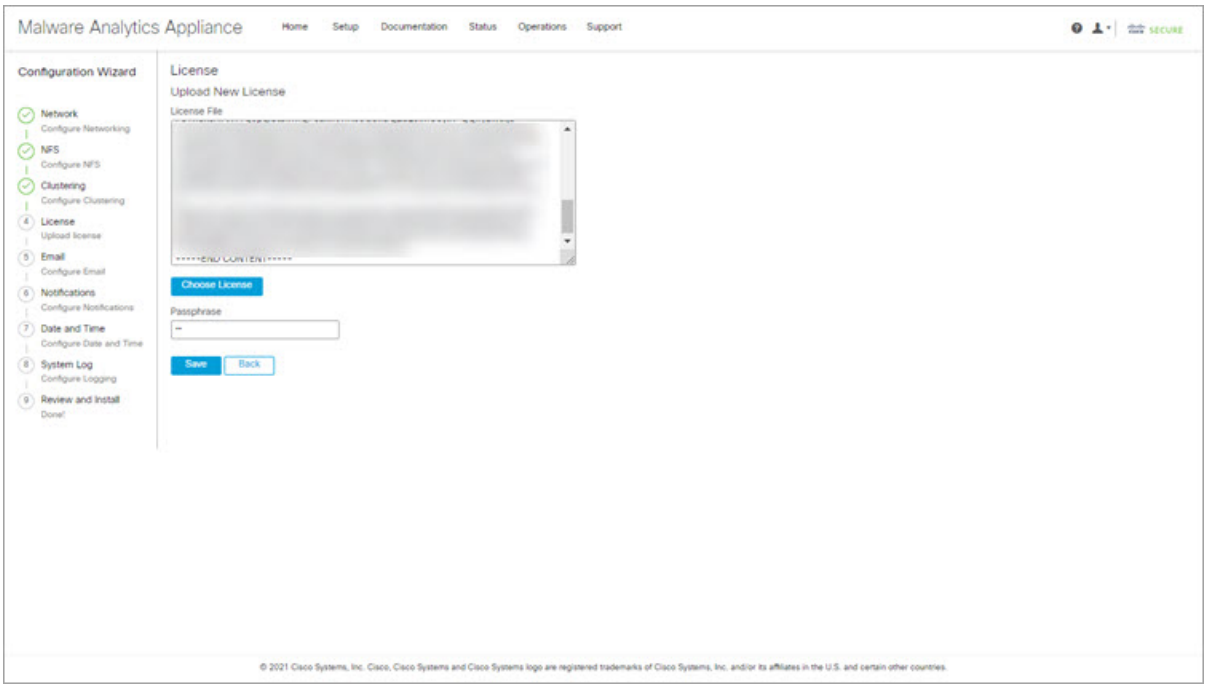
After the clustering, you are ready to install the Secure Malware Analytics license.

Step 1 Click **Upload License** and select the license file from your file manager.

Alternatively, you can retrieve the license from the server. If the appliance has network access when being installed, click **Retrieve License From Server** to get the license over the network.

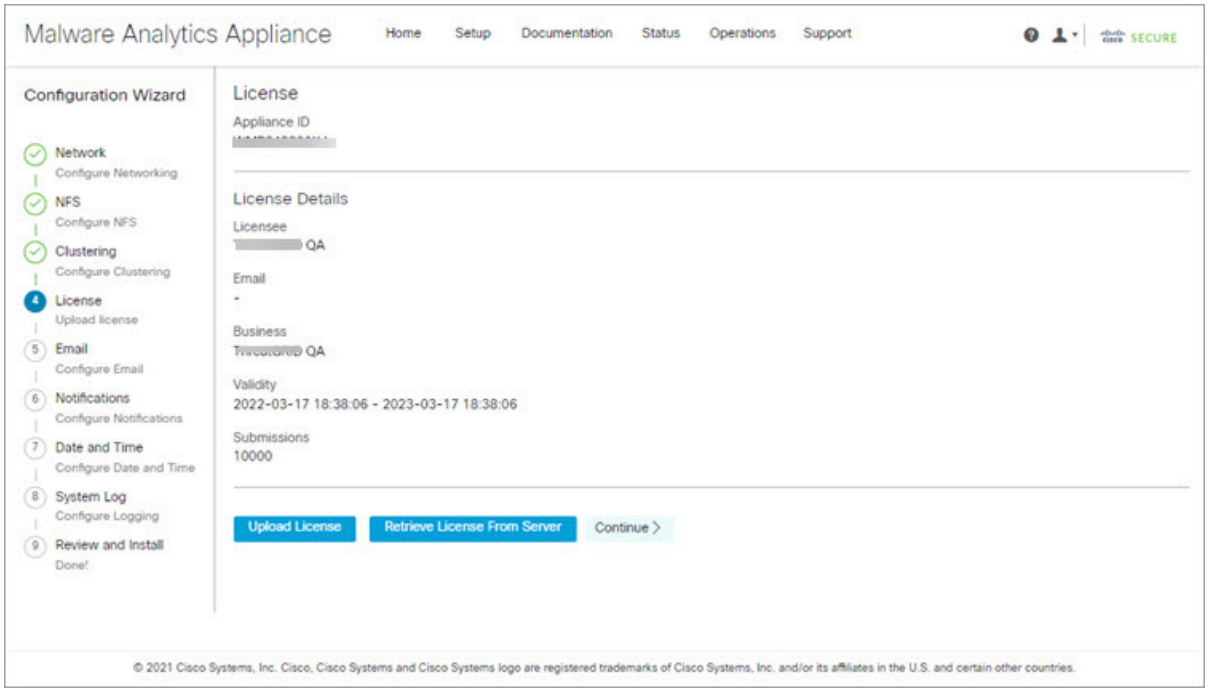
Step 2 Enter your license password in the **Passphrase** field.

Figure 11: Upload New License



Step 3 Click **Save** to install the license. The page refreshes and your license information is displayed.

Figure 12: License Information After Successful Installation



Step 4 Click **Continue**.

What to do next

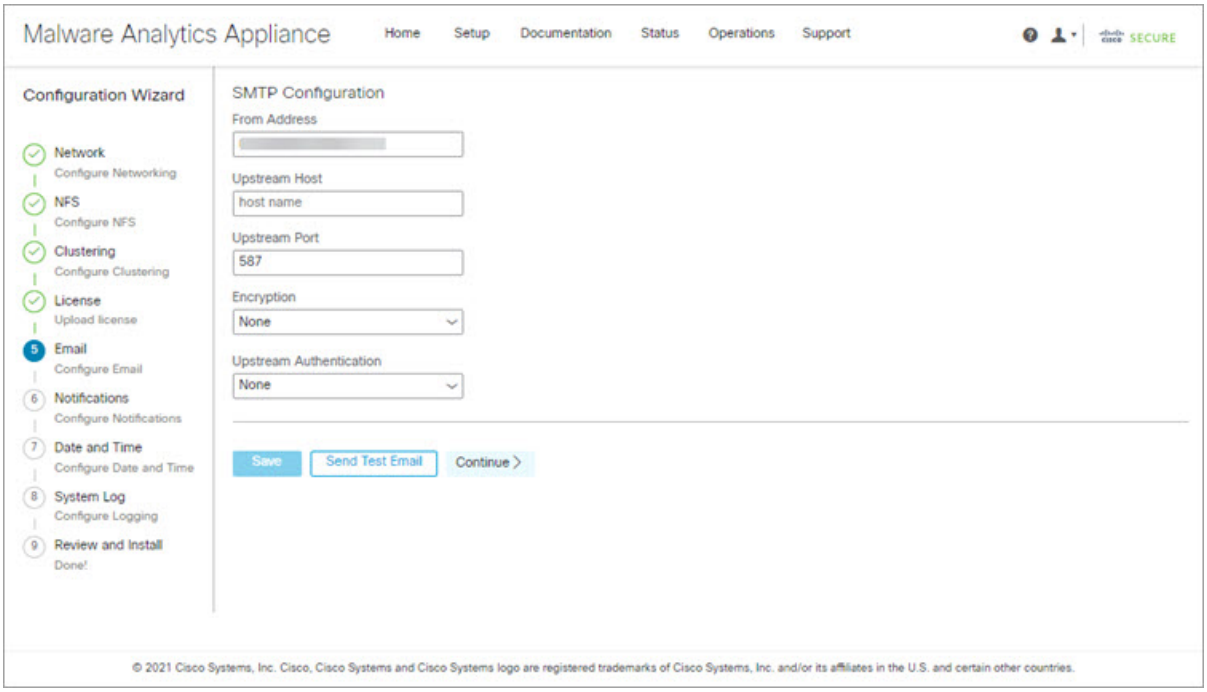
Proceed to Configure Email, on page 20.

Configure Email

The next step in the workflow is to configure the email host in the **SMTP Configuration** page.

Step 1 Enter the email **From Address**.

Figure 13: SMTP Configuration



Step 2 Enter the name of the **Upstream Host** (email host).

Step 3 Change the port from **587** to **25**.

Step 4 Keep the defaults for the other settings.

Step 5 Click **Save** to save your settings.

Step 6 Click **Continue** to move to the next step in the workflow.

What to do next

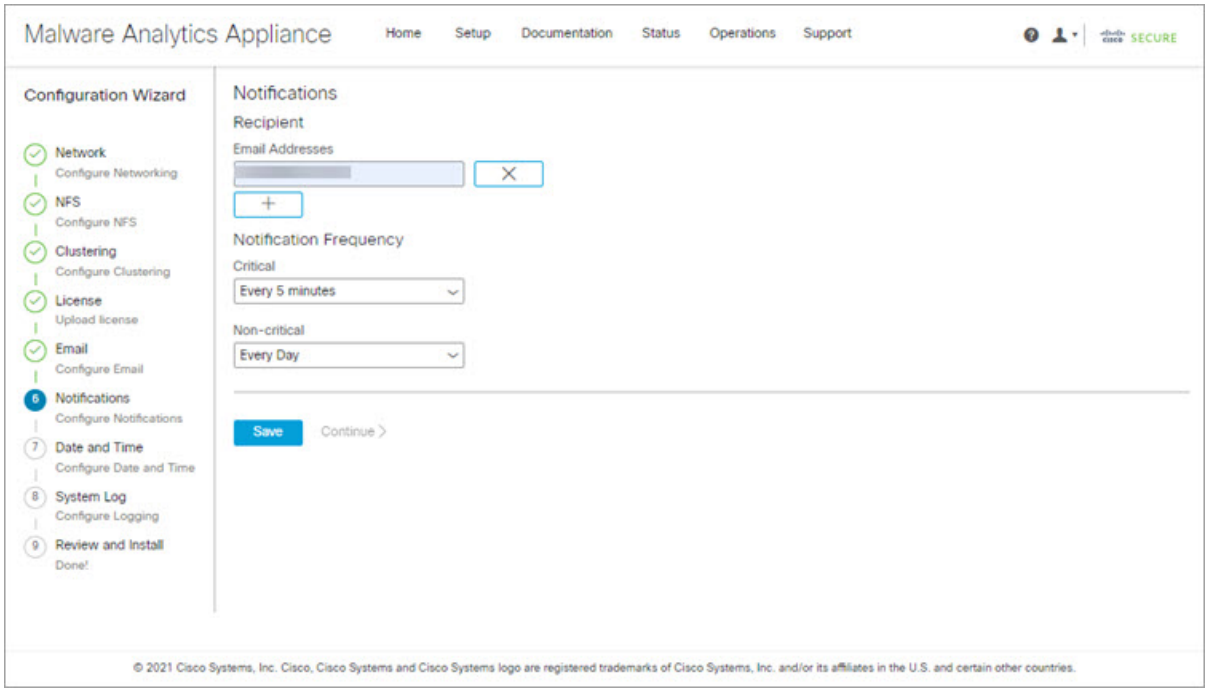
Proceed to Configure Notifications.

Configure Notifications

The next step in the workflow is to configure notifications that can be delivered periodically to one or more email addresses. System notifications are displayed in the Secure Malware Analytics portal interface, but this page allows you to set up **Notifications** that are also sent via email.

Step 1 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.

Figure 14: Notifications



Step 2 Under **Notification Frequency**, choose the settings for **Critical** and **Non-critical** from the drop-down lists.

Step 3 Click **Save**.

Step 4 Click **Continue** to move to the next step in the workflow.

What to do next

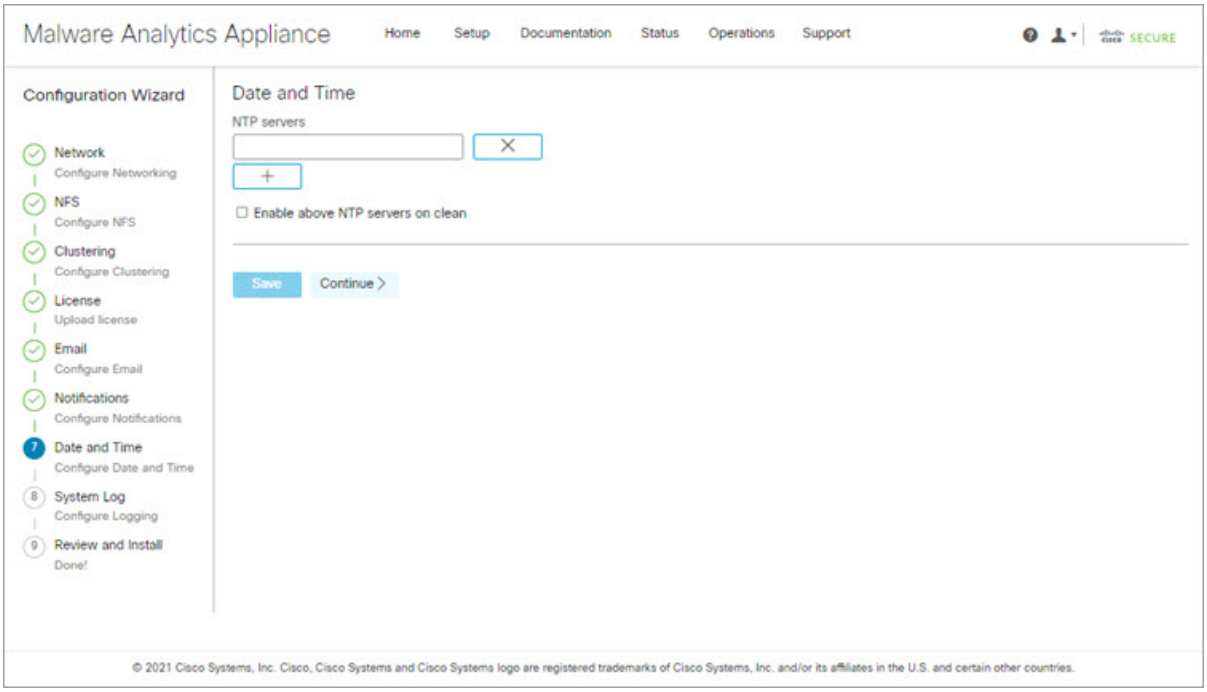
Proceed to Configure Date and Time.

Configure Date and Time

The next step is to specify the Network Time Protocol (NTP) servers to configure the date and time.

Step 1 Enter the **NTP Server(s)** IP or NTP name.

Figure 15: Date and Time



If there are multiple NTP servers, click the + icon to add another field; repeat as needed.

Step 2 Click **Save**.

Step 3 Click **Continue** to move to the next step in the workflow.

What to do next

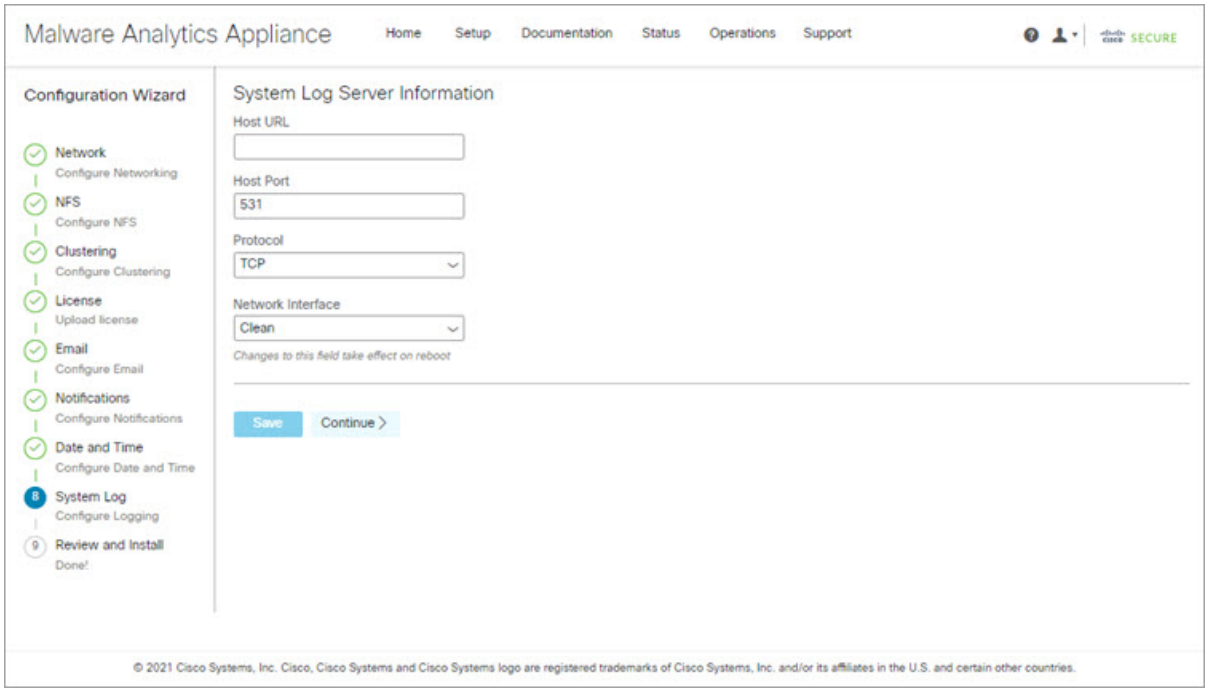
Proceed to Configure System Log.

Configure System Log

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

Step 1 Complete the Host URL, Host Port, and Protocol fields and click **Save**.

Figure 16: System Log Server Information



Step 2 Click **Continue** to move to the final step in the workflow.

See the *Cisco Threat Grid Appliance Administration Guide* for more information.

What to do next

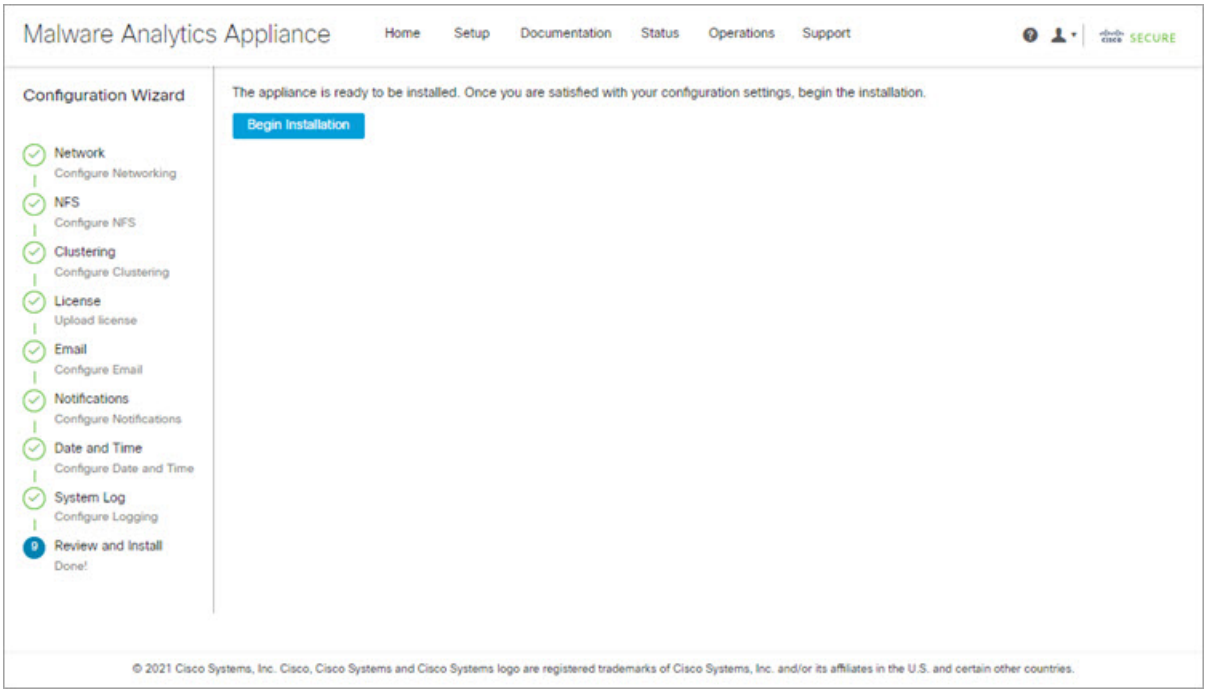
Proceed to Review and Install Configuration Settings.

Review and Install Configuration Settings

The final step in the workflow is to review and install your network configuration settings.

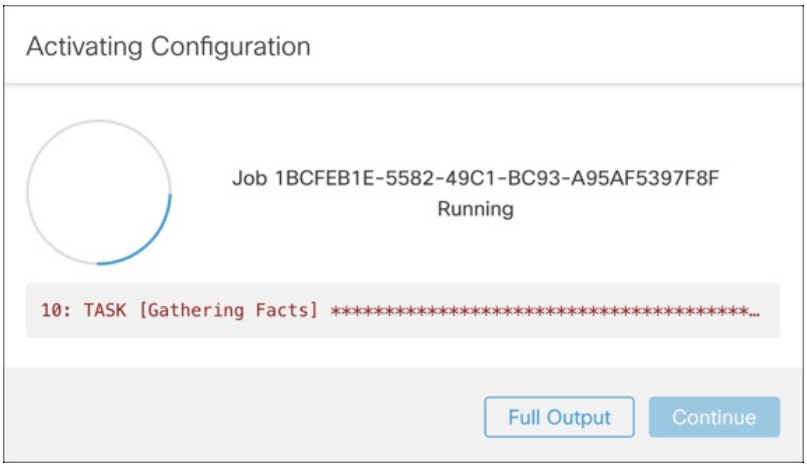
Step 1 Click **Review and Install** in the navigation pane and then click **Begin Installation** to begin installing the configuration scripts.

Figure 17: Begin Installation



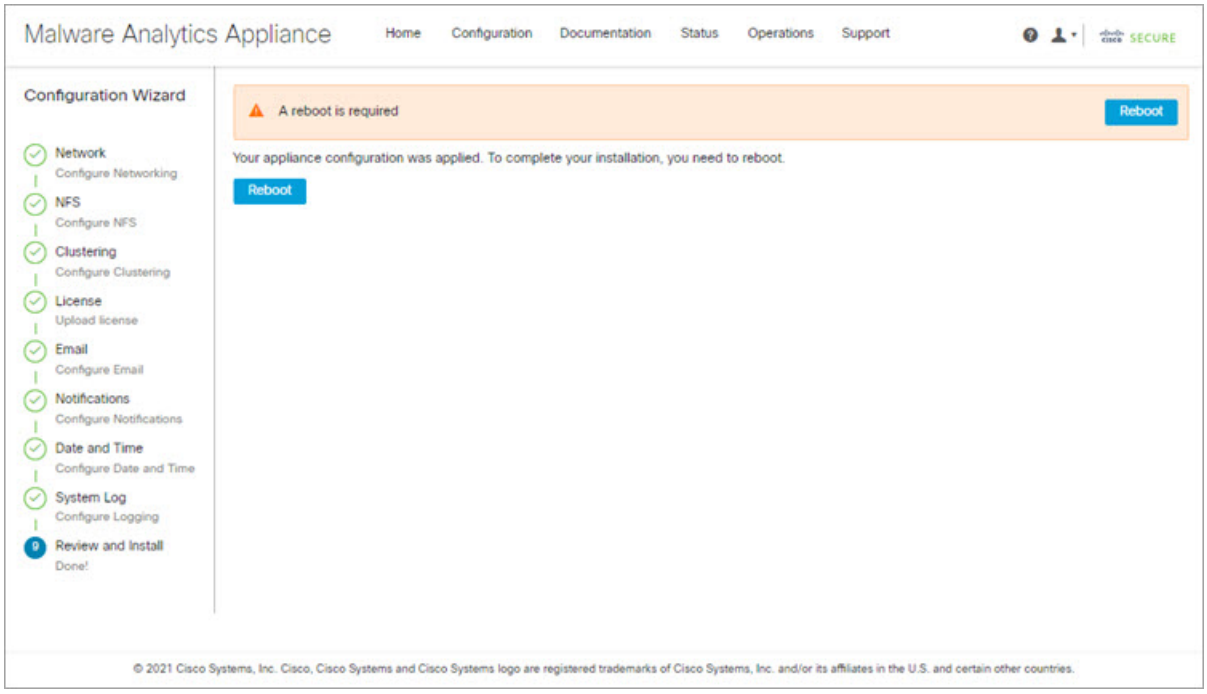
Note The screen displays configuration information as it is applied.

Figure 18: Activating Configuration



After successful installation, the **State** changes from **Running** to **Successful**, and the **Reboot** button becomes enabled (green). The configuration output is also displayed.

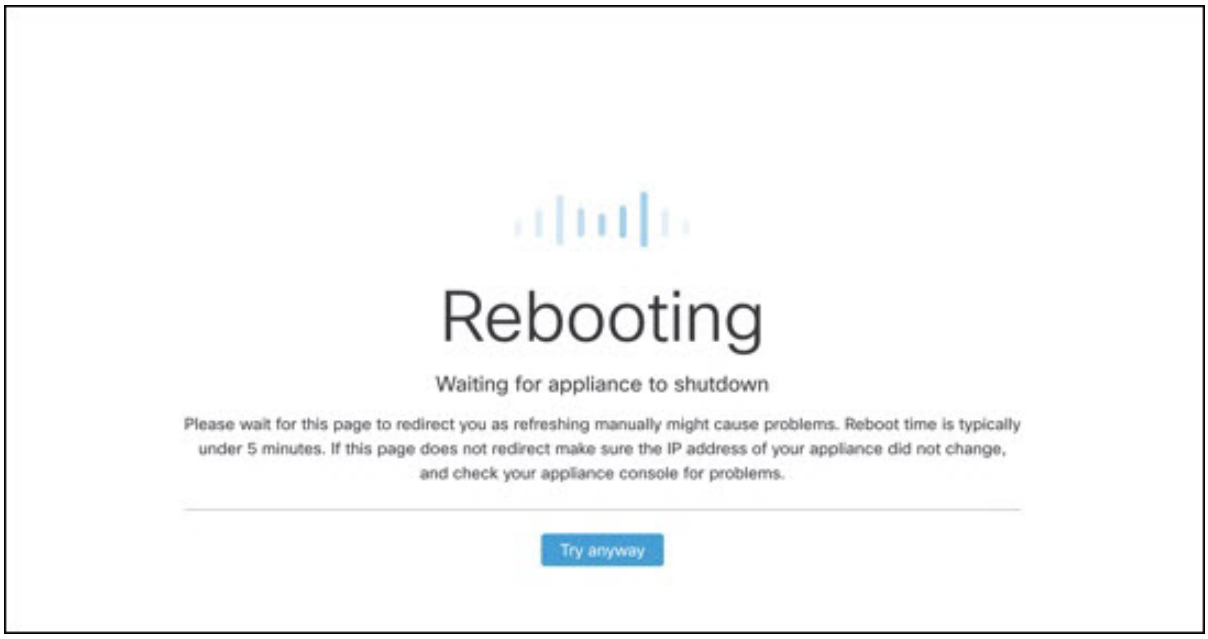
Figure 19: Successful Appliance Installation



Step 2 Click **Reboot**.

Note Rebooting may take up to 5 minutes. Do not make any changes while the Threat Grid Appliance is rebooting.

Figure 20: Appliance is Rebooting



After reboot, the appliance opens to the Admin UI **Home** page. This completes the configuration process.

Install Secure Malware Analytics Appliance Updates

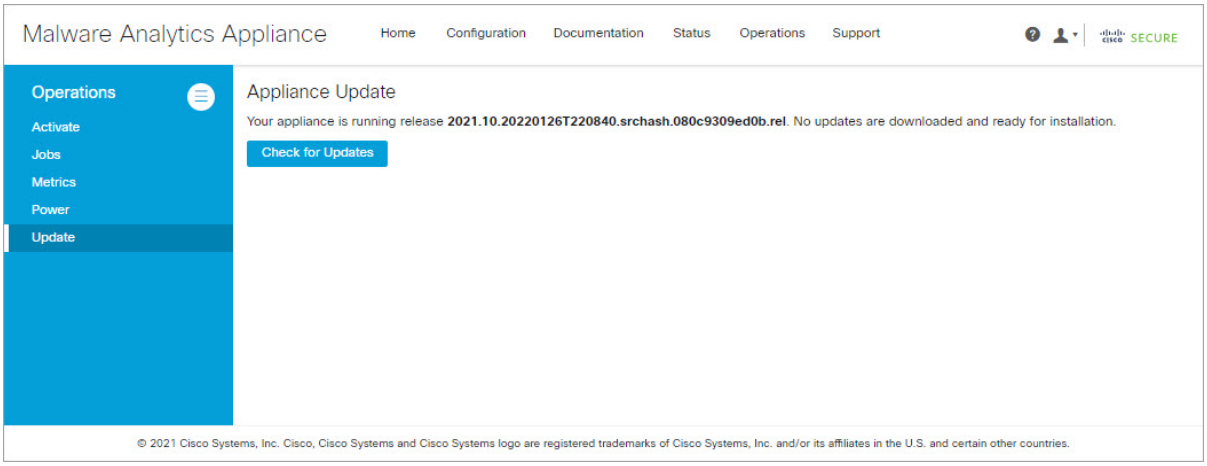
After you complete the initial Secure Malware Analytics Appliance setup, we recommend that you install any available updates before continuing. Secure Malware Analytics Appliance updates are applied through the Admin UI.

Users with air-gapped implementations may contact Support and request a downloadable update boot image.

Note For more information about installing updates, see the *Cisco Secure Malware Analytics Appliance Administration Guide*.

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

Figure 21: Appliance Updates Page



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.

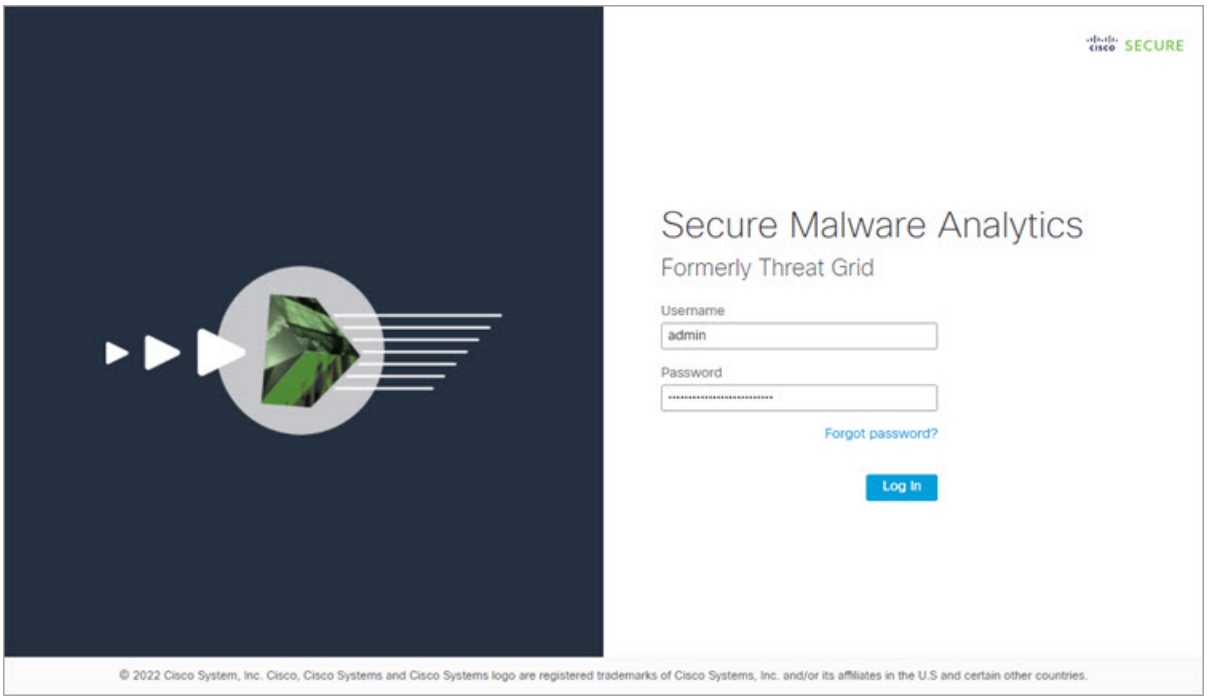
Test the Appliance Setup

Once the Secure Malware Analytics Appliance is updated to the current version, you should test that it has been configured properly by submitting a malware sample to Secure Malware Analytics.

Step 1 In a browser, open Secure Malware Analytics using the address you configured as the Clean interface.

The Secure Malware Analytics login page opens.

Figure 22: Secure Malware Analytics Login

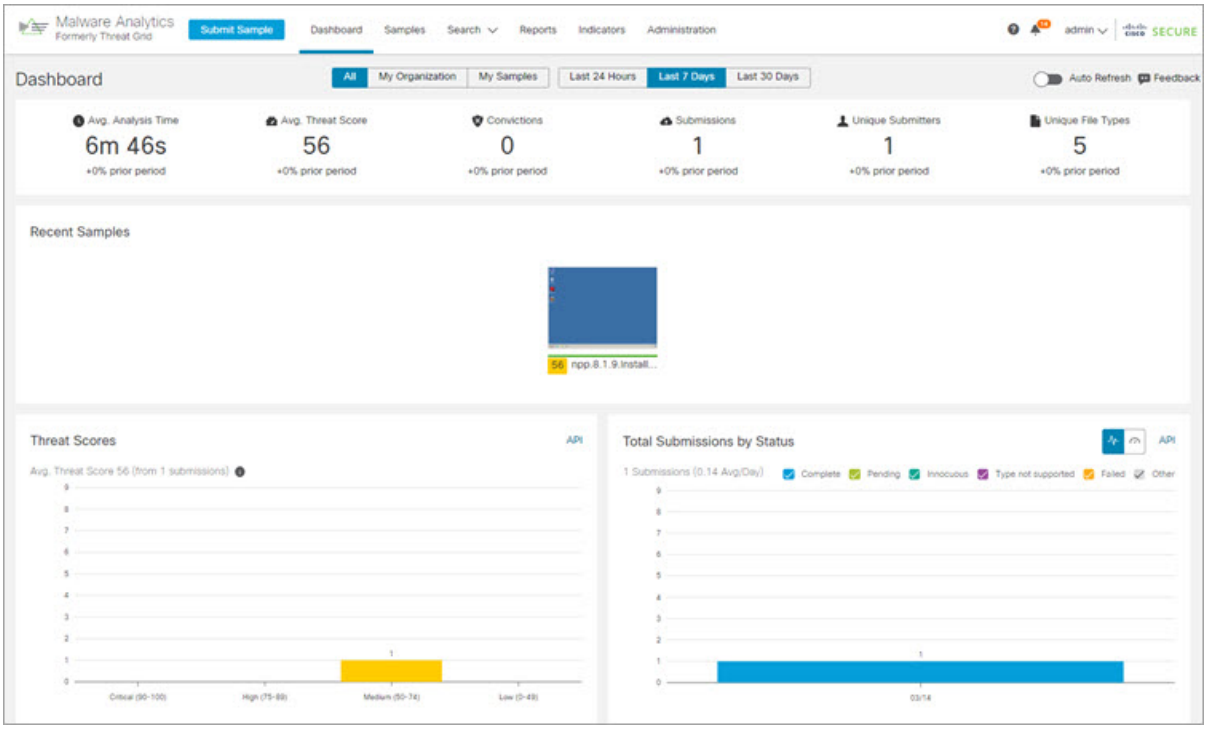


Step 2 Enter the default credentials:

- **Login** - admin
- **Password** - Use the new password entered during the first step of the Admin UI configuation workflow. We encourage you to change it for the portal when you have a chance.

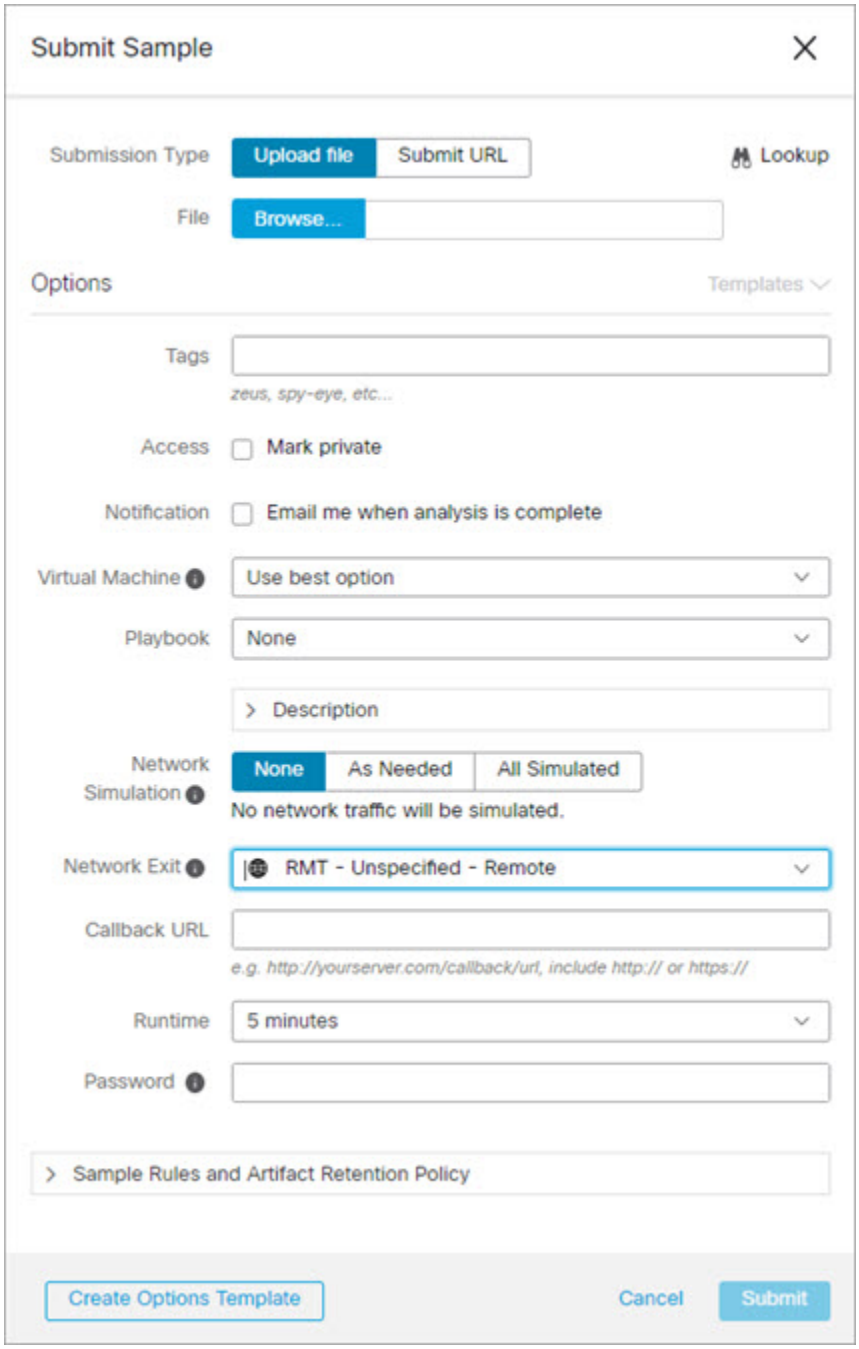
Step 3 Click **Log In** to open the main **Secure Malware Analytics** dashboard. There will be no sample data available yet.

Figure 23: Secure Malware Analytics Dashboard



Step 4 Click **Submit a Sample** to open the sample submission dialog.

Figure 24: Submit Sample



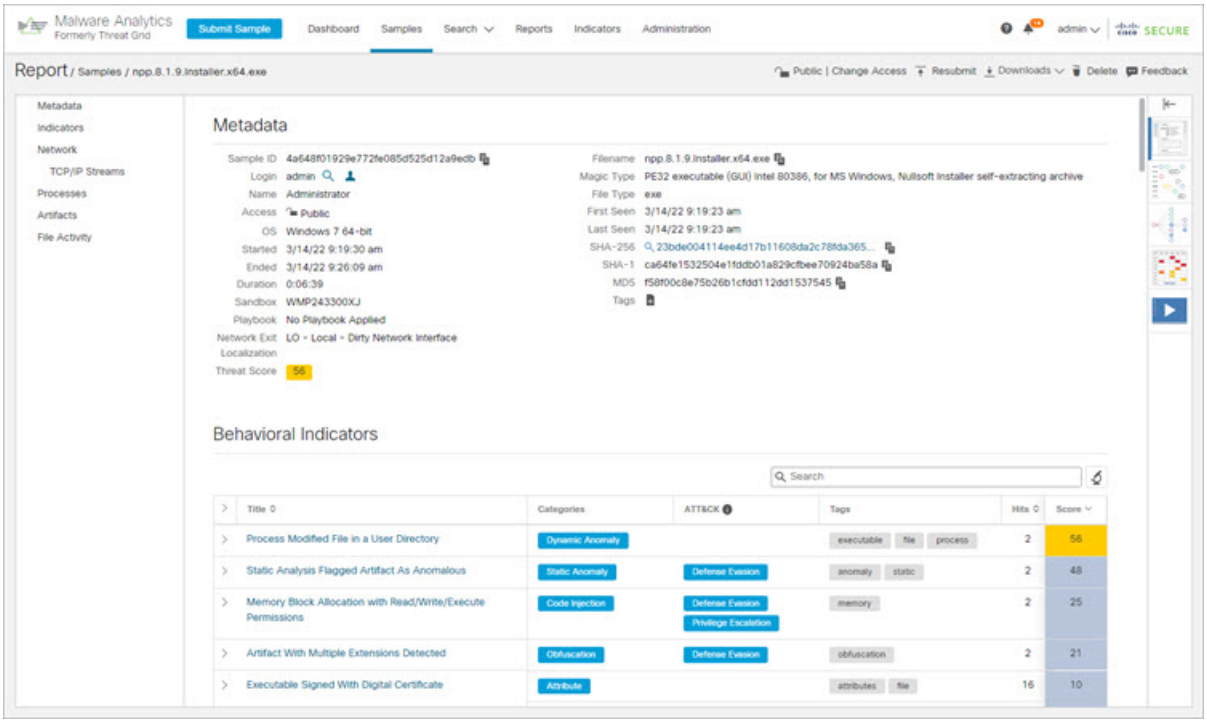
Note There is help available at the bottom of this form, describing sample submission file types, size, and other information. You can also click the **?** icon located in the upper-right corner to view the Secure Malware Analytics Release Notes and online help, including complete documentation on how to submit a sample and review the analysis results.

Step 5 Upload a file or enter a URL to submit for malware analysis. Leave the other options set at the defaults if you are not yet sure what they mean.

Step 6 Click **Submit**.

The Secure Malware Analytics sample analysis process is launched. You should see your sample going through several stages of analysis. During analysis, the sample is listed in the **Samples** page. Once analysis is completed, the results should be available in the Analysis Report.

Figure 25: Analysis Report



What to do next

Once the Secure Malware Analytics Appliance has been set up and initial configuration is completed, additional tasks can be performed by the appliance administrator, such as managing SSL certificates and adding users. See the *Cisco Secure Malware Analytics Appliance Administration Guide* for information about administrator tasks.