Cisco Secure Malware Analytics Appliance Getting Started Guide Version 2.17

First Published: 2020-12-15

Last Modified: 2022-03-17

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.

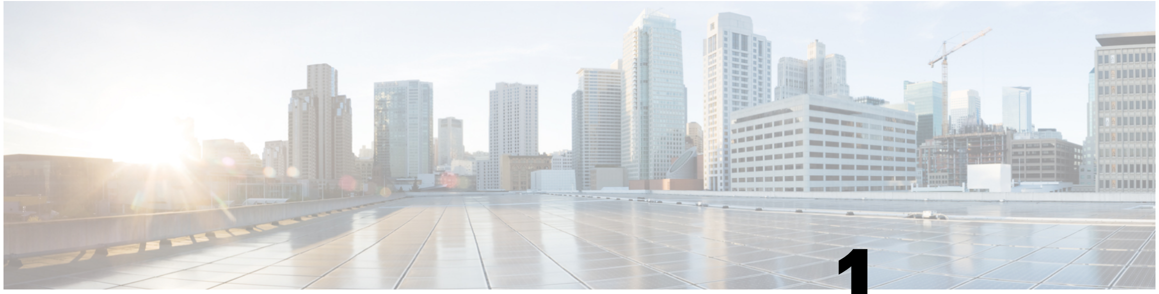
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS



CHAPTER 1

Introduction

This chapter provide 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

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 2.17:

Table 1: Changes in Version 2.17 Release - March 14, 2020

Feature or Update	Section
Updated screenshots and instructions.	Admin UI Configuration, on page 13
The legacy TGSH-dialog is replaced by a modern Admin TUI	Configure Network Using Admin TUI, on page 10

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.

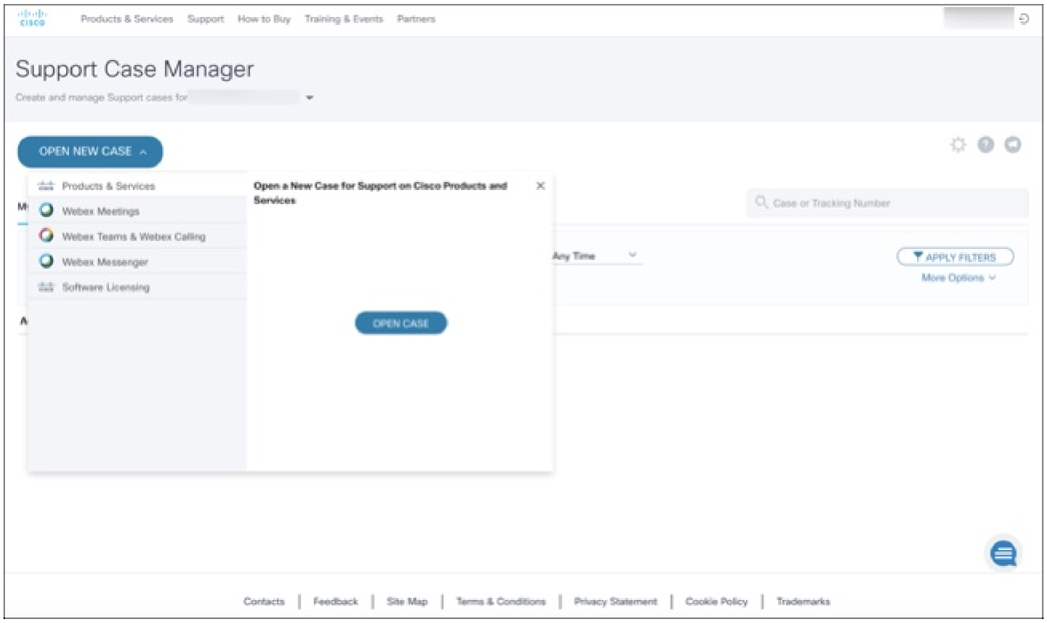
Note Verify that SSH is specified for updates.

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**.

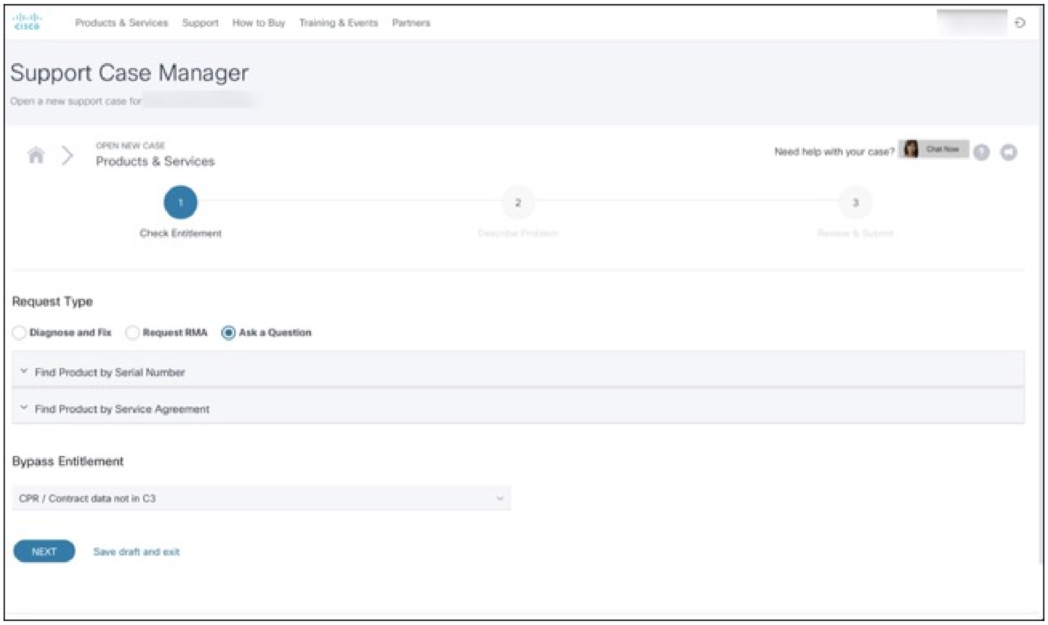
Figure 1: Open New Case



Open a New Case for Support on Cisco Products and Services

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



Support Case Manager

Open a new support case for [redacted]

OPEN NEW CASE

Products & Services

Request Type

○ Diagnose and Fix ○ Request RMA ● Ask a Question

Find Product by Serial Number

Find Product by Service Agreement

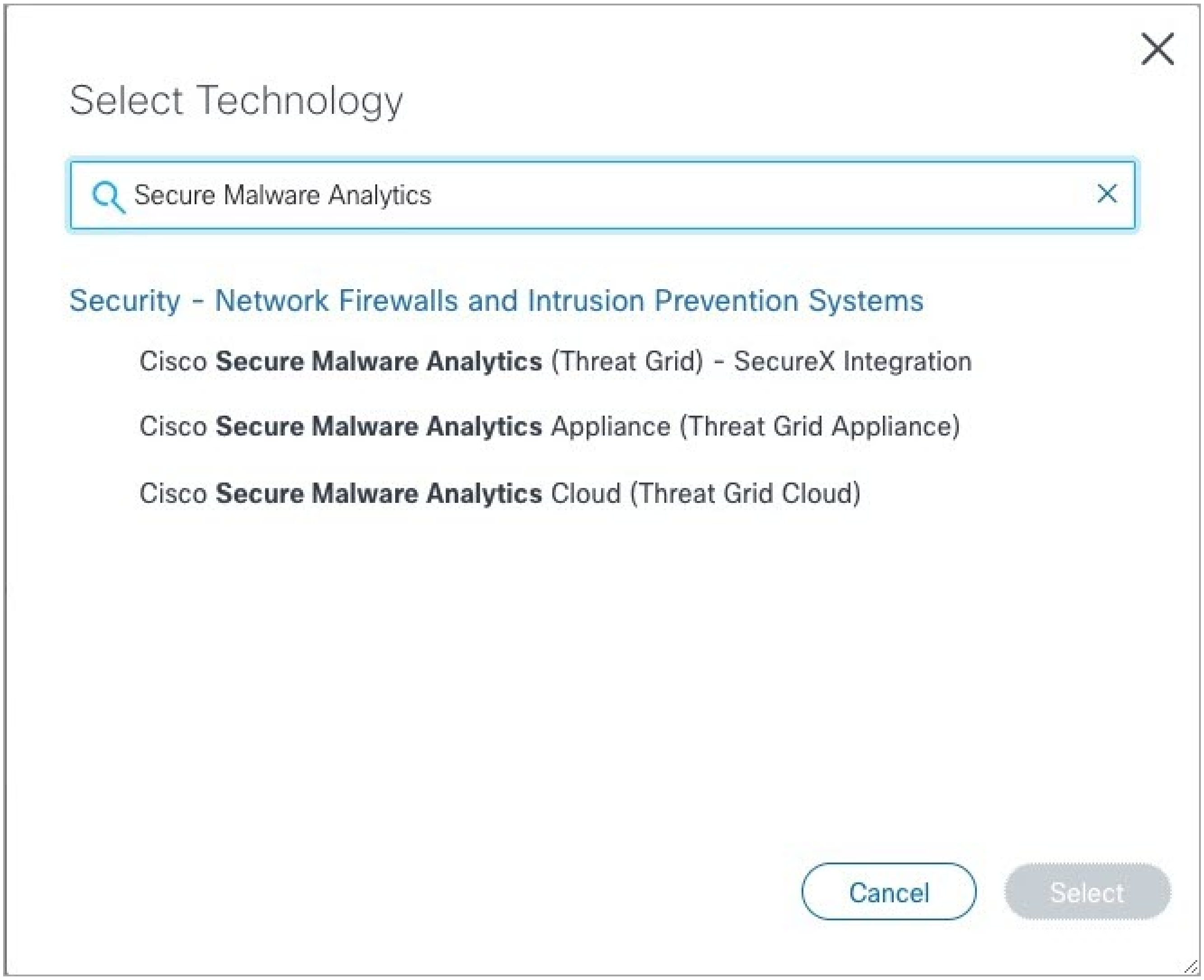
Bypass Entitlement

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 Appliance in the title).

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

Figure 3: 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)

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

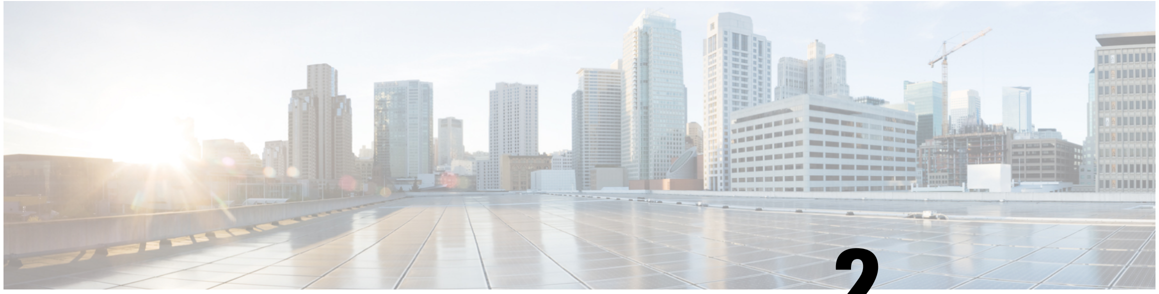
Setup and Configuration Overview

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

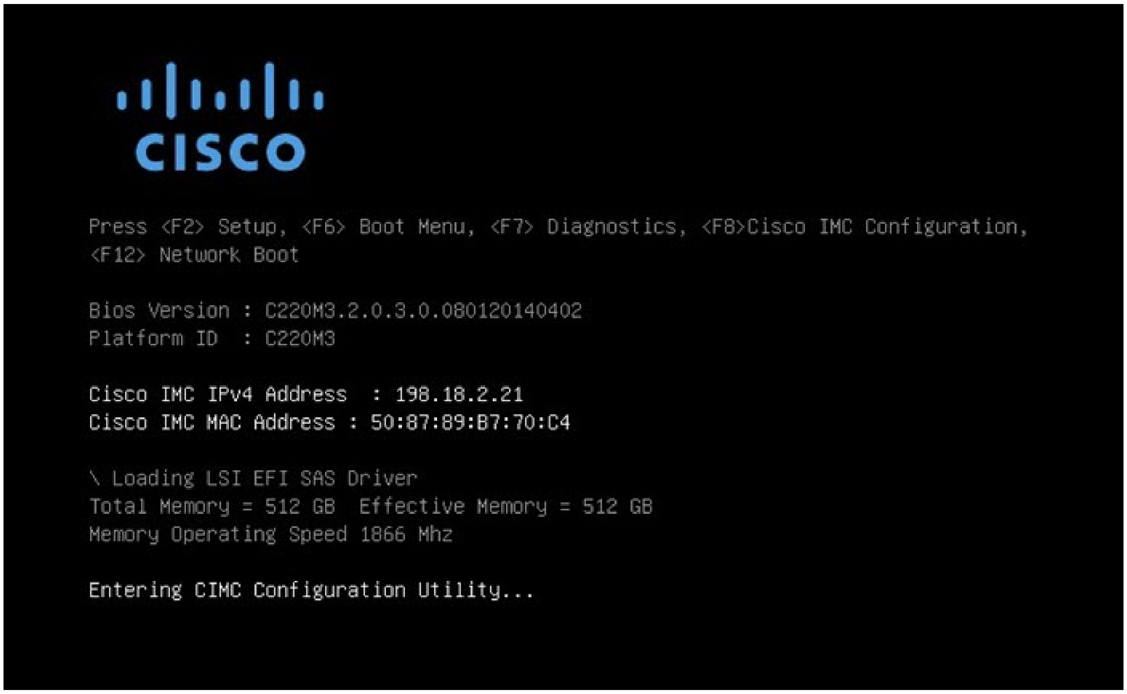
Initial Network Configuration

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

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.

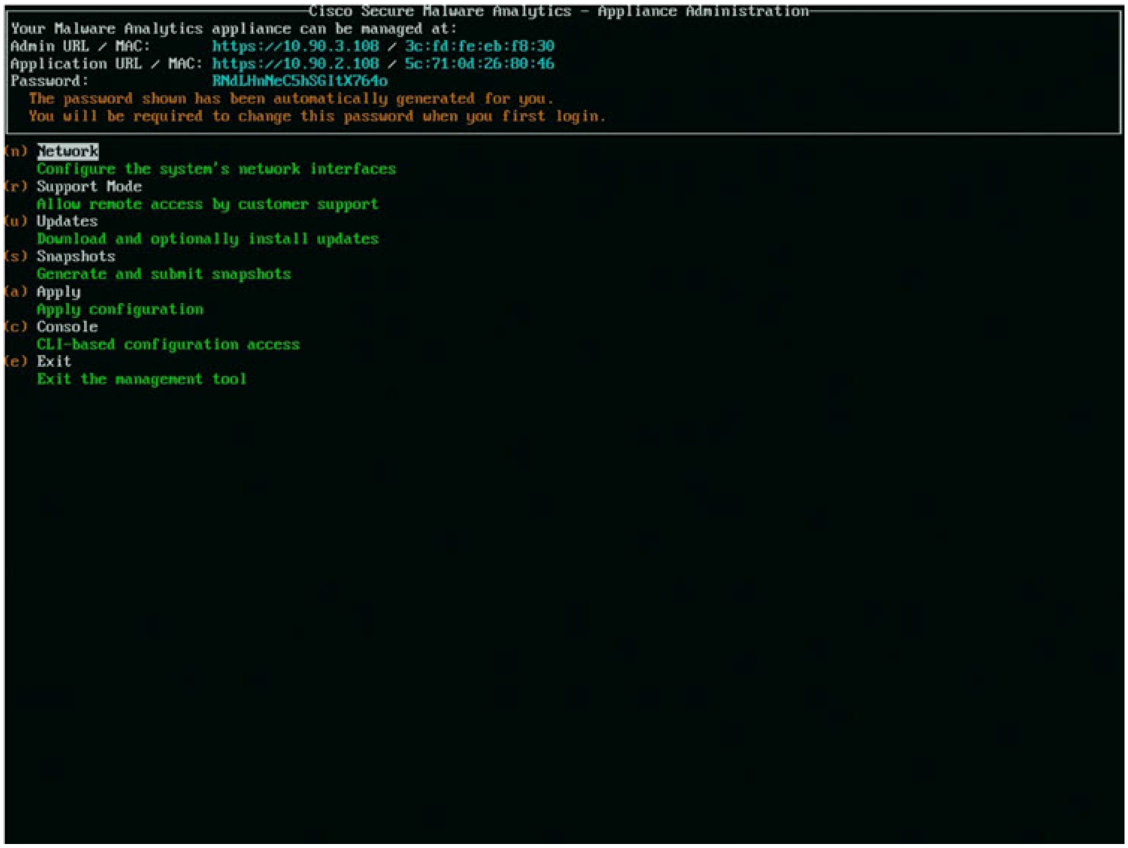
Figure 4: Cisco Screen During Bootup



```
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...
```

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

Figure 5: Admin TUI



```
                    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:              RNdLHnMeC5hSGltX764o
  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
```

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).

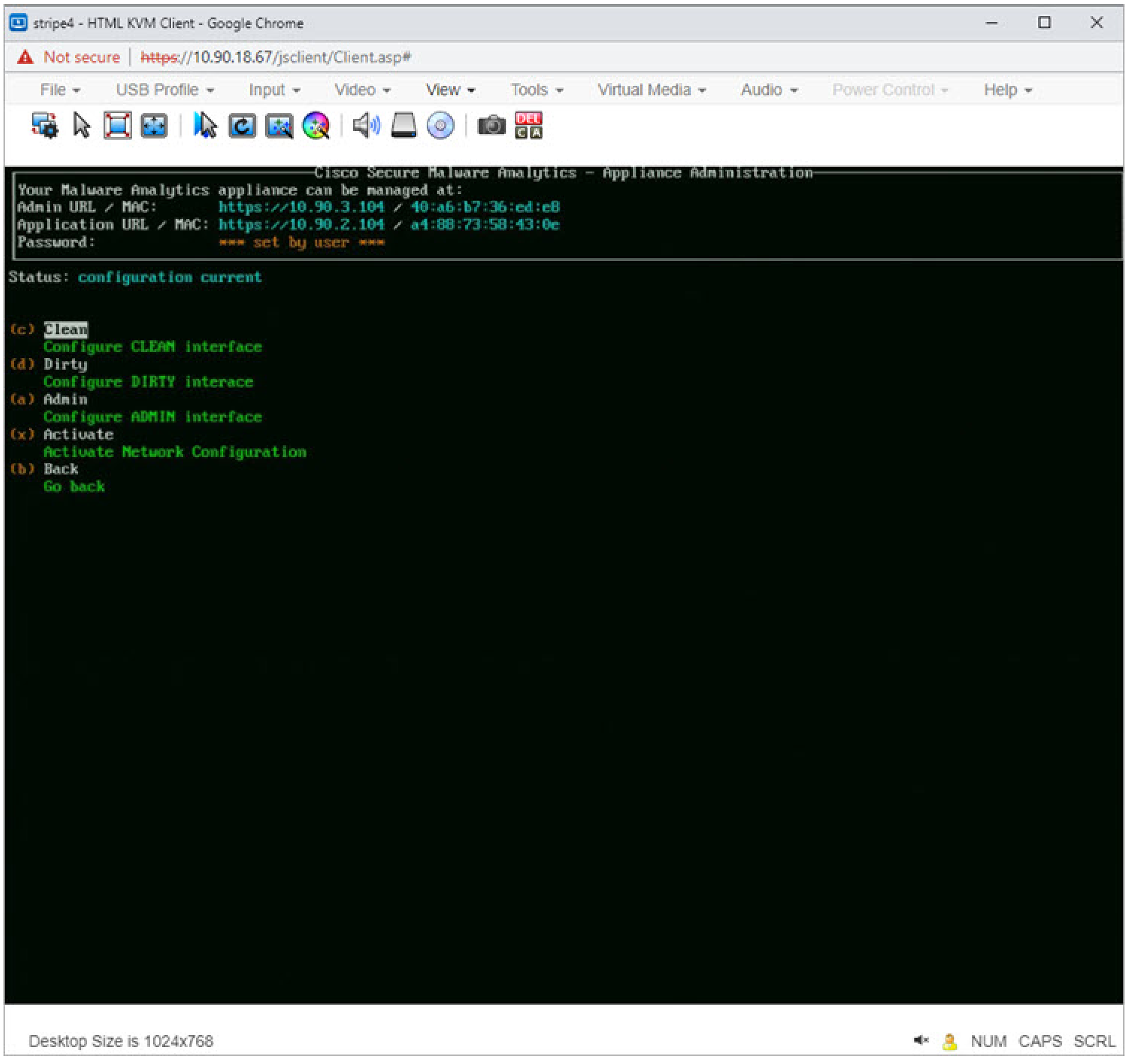
Configure Network Using Admin TUI

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



```
                              Cisco Secure Malware Analytics - Appliance Administration
 Your Malware Analytics appliance can be managed at:
 Admin URL / MAC:        https://10.90.3.104 / 40:a6:b7:36:ed:e8
 Application URL / MAC:  https://10.90.2.104 / a4:88:73:58:43:0e
 Password:               *** set by user ***

Status: configuration current


(c) Clean
    Configure CLEAN interface
(d) Dirty
    Configure DIRTY interace
(a) Admin
    Configure ADMIN interface
(x) Activate
    Activate Network Configuration
(b) Back
    Go back
```

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

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.

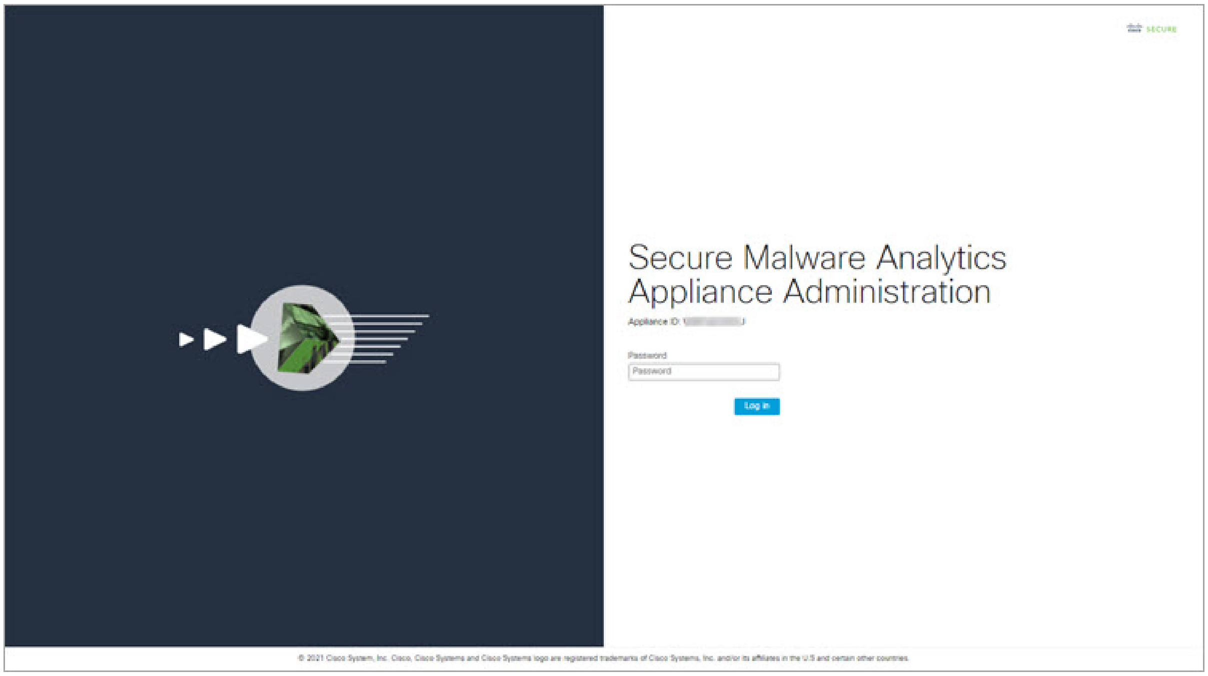
Log In to the Admin UI

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



Secure Malware Analytics Appliance Administration

Appliance ID: [redacted]

Password

Password

© 2021 Cisco System, 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 Enter the initial **Admin Password** that you copied from the Admin TUI and click **Log In**.

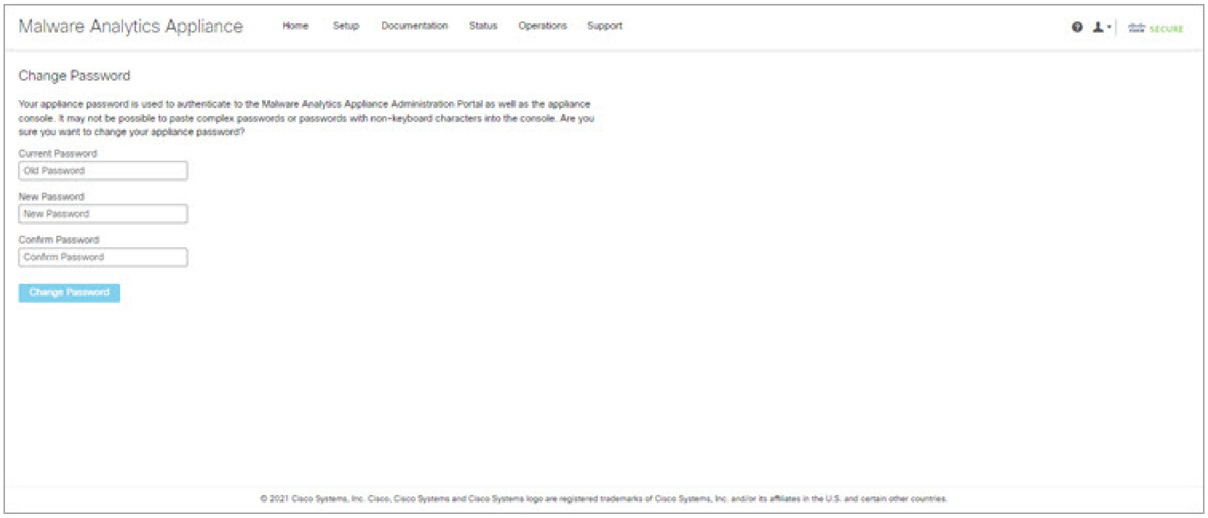
What to do next

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



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: Old Password

New Password: New Password

Confirm 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 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

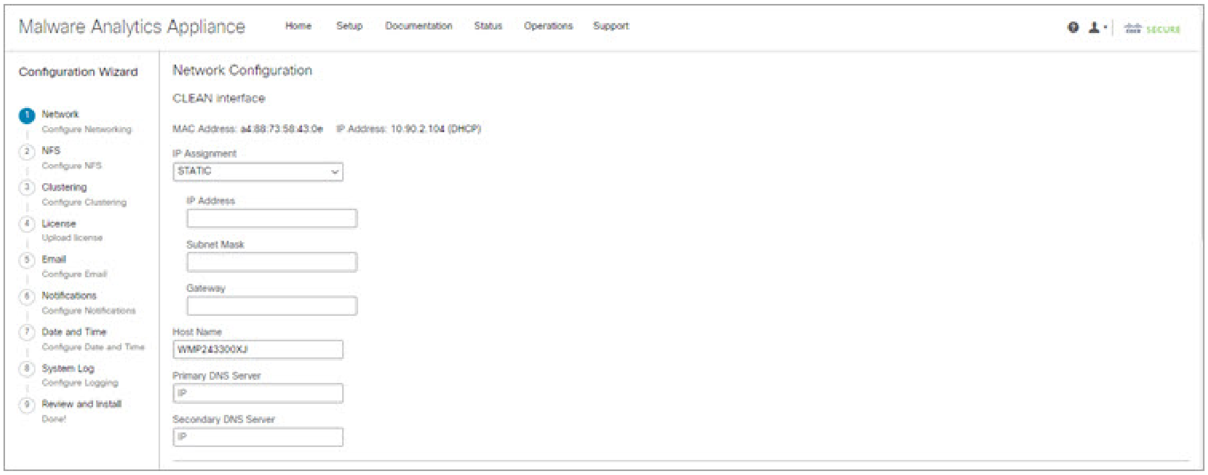
The Configuration wizard takes you through configuring your Secure Malware Analytics Appliance.

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.

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 9: 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:

Subnet Mask:

Gateway:

Host Name: WMP243300XJ

Primary DNS Server: IP

Secondary DNS Server: IP

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 17.

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

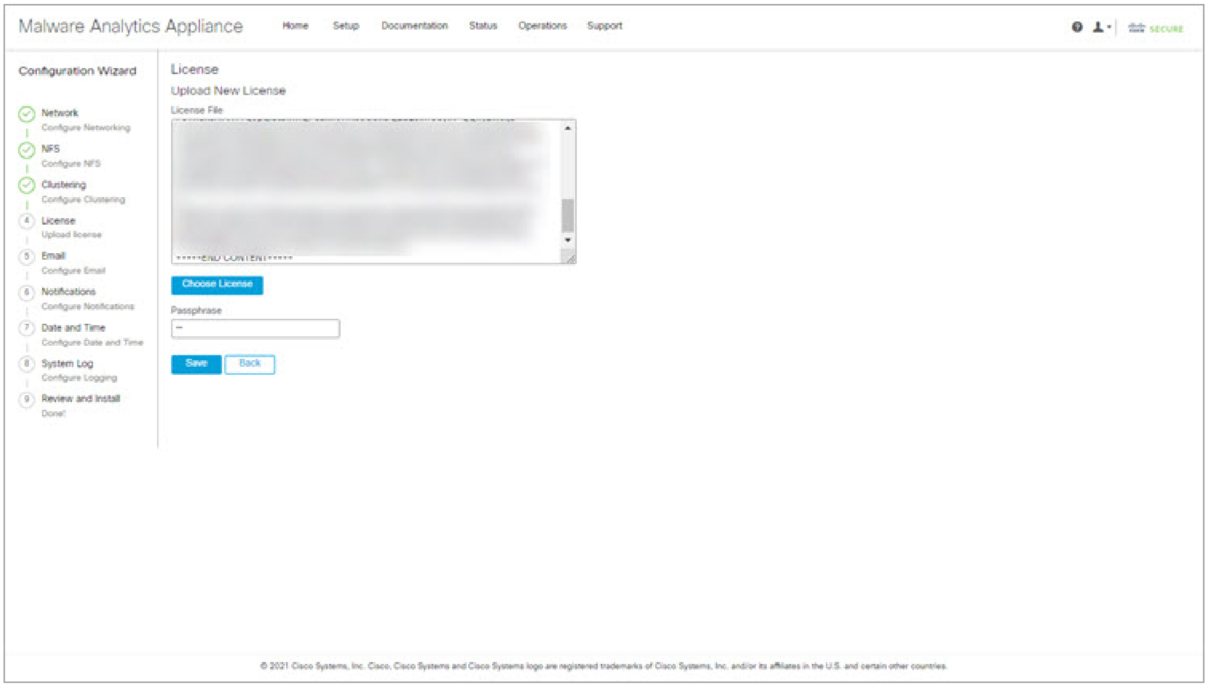
After the clustering, you are ready to install the Secure Malware Analytics license.

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 10: Upload New License



License

Upload New License

License File

[redacted]

*****END CONTENT*****

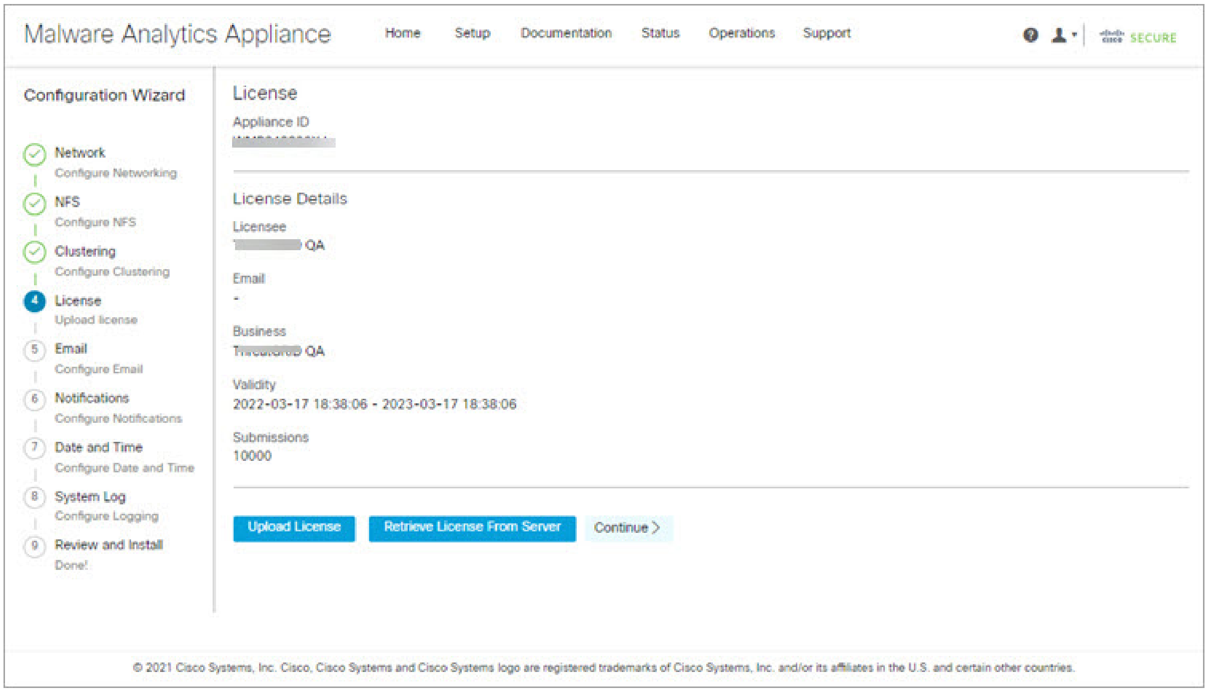
Passphrase

--

© 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 **Save** to install the license. The page refreshes and your license information is displayed.

Figure 11: License Information After Successful Installation



License

Appliance ID

[redacted]

License Details

Licensee

[redacted] QA

Email

-

Business

[redacted] QA

Validity

2022-03-17 18:38:06 - 2023-03-17 18:38:06

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 4 Click **Continue**.

What to do next

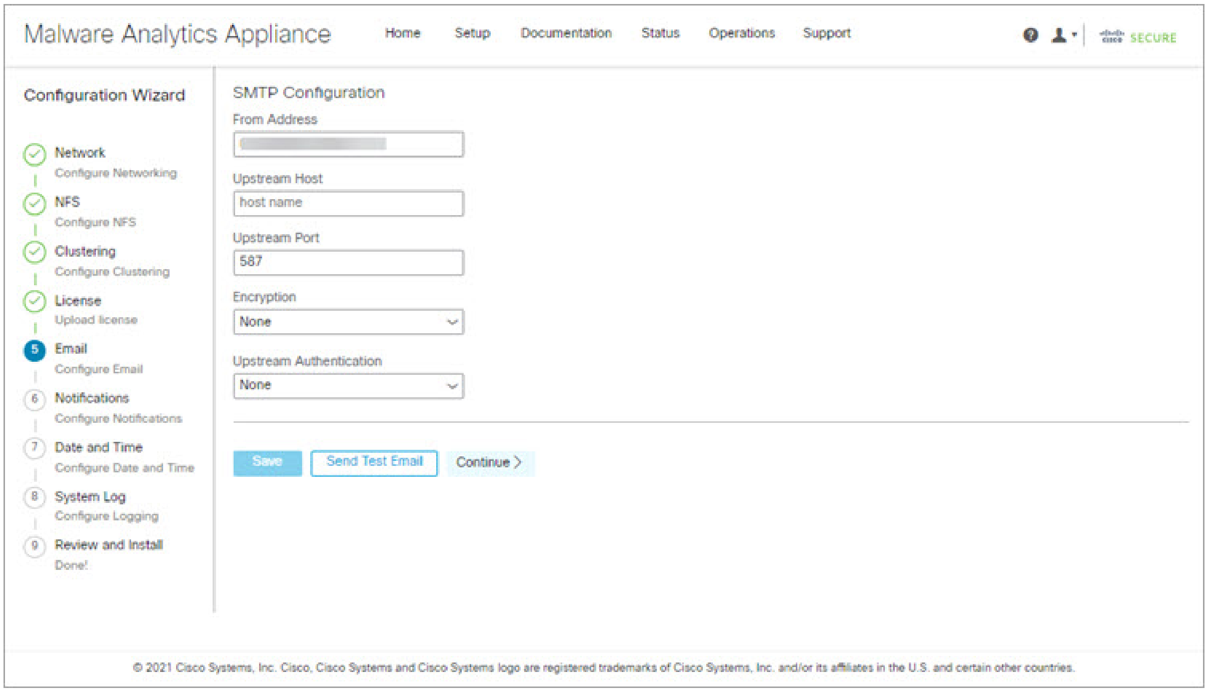
Proceed to Configure Email, on page 21.

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 12: SMTP Configuration



SMTP Configuration

From Address: [redacted]

Upstream Host: host name

Upstream Port: 587

Encryption: None

Upstream Authentication: None

© 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 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

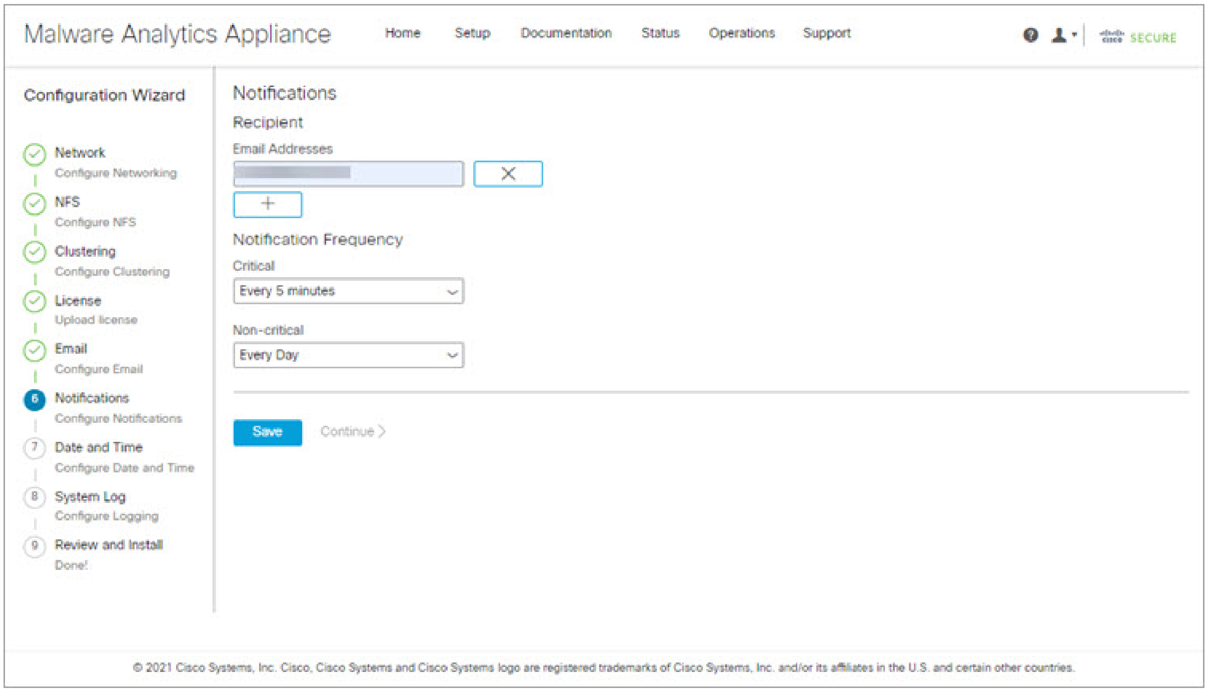
Proceed to Configure Notifications.

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 13: Notifications



Notifications

Recipient

Email Addresses: [redacted]

Notification Frequency

Critical: Every 5 minutes

Non-critical: Every Day

© 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 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

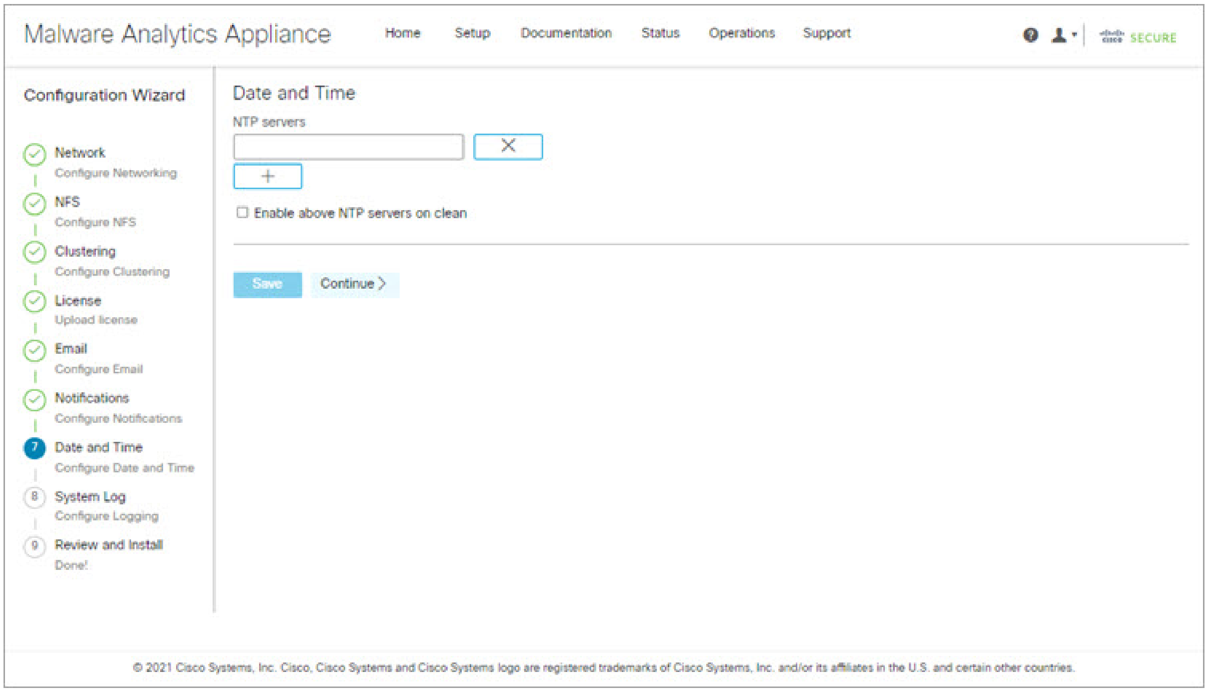
Proceed to Configure Date and Time.

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 14: 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

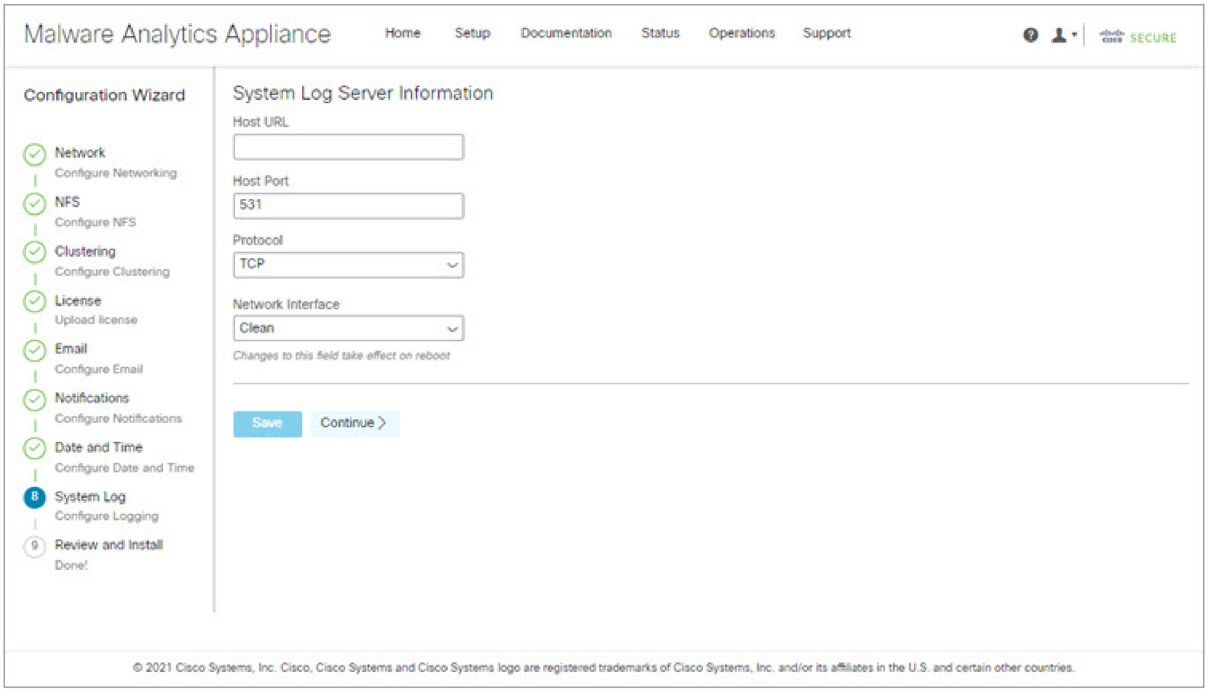
Proceed to Configure System Log.

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 15: System Log Server Information



System Log Server Information

Host URL

Host Port: 531

Protocol: TCP

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 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

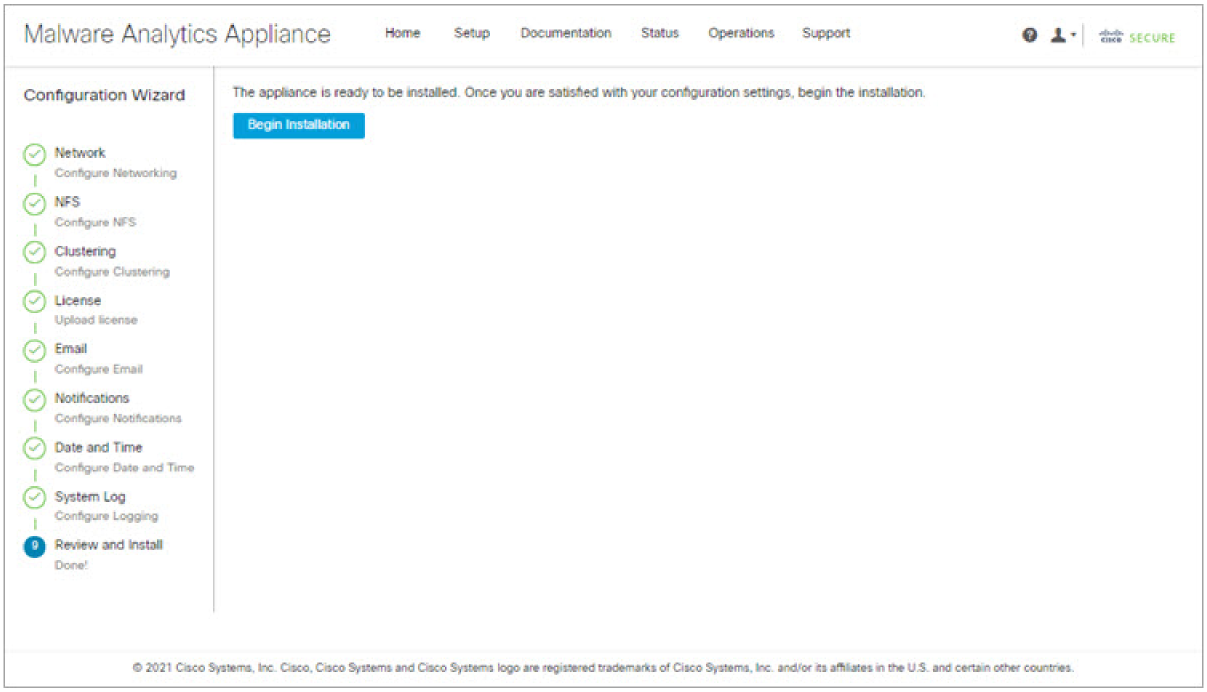
Proceed to Review and Install Configuration Settings.

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 16: Begin Installation



Malware Analytics Appliance

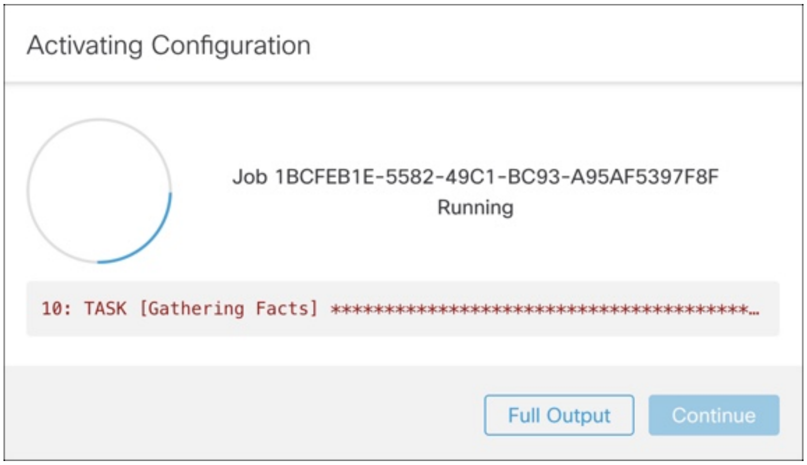
Configuration Wizard

The appliance is ready to be installed. Once you are satisfied with your configuration settings, begin the 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.

Note The screen displays configuration information as it is applied.

Figure 17: Activating Configuration



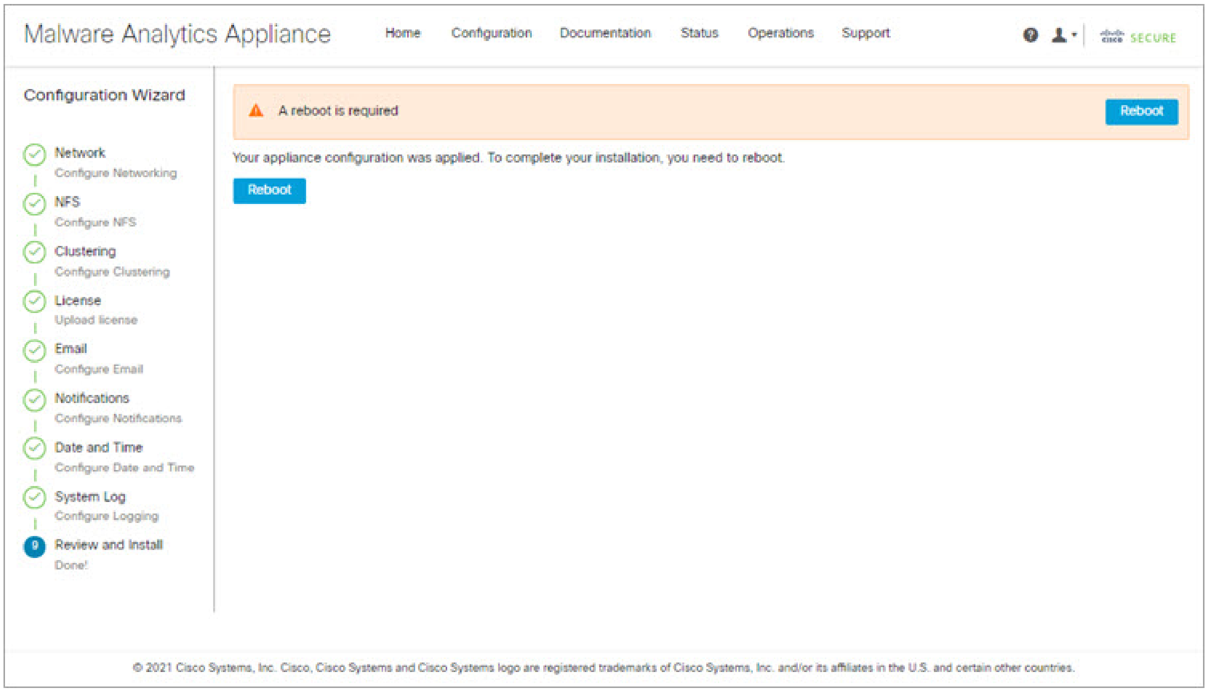
Activating Configuration

Job 1BCFEB1E-5582-49C1-BC93-A95AF5397F8F
Running

```
10: TASK [Gathering Facts] *****************************************…
```

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

Figure 18: Successful Appliance Installation



A reboot is required

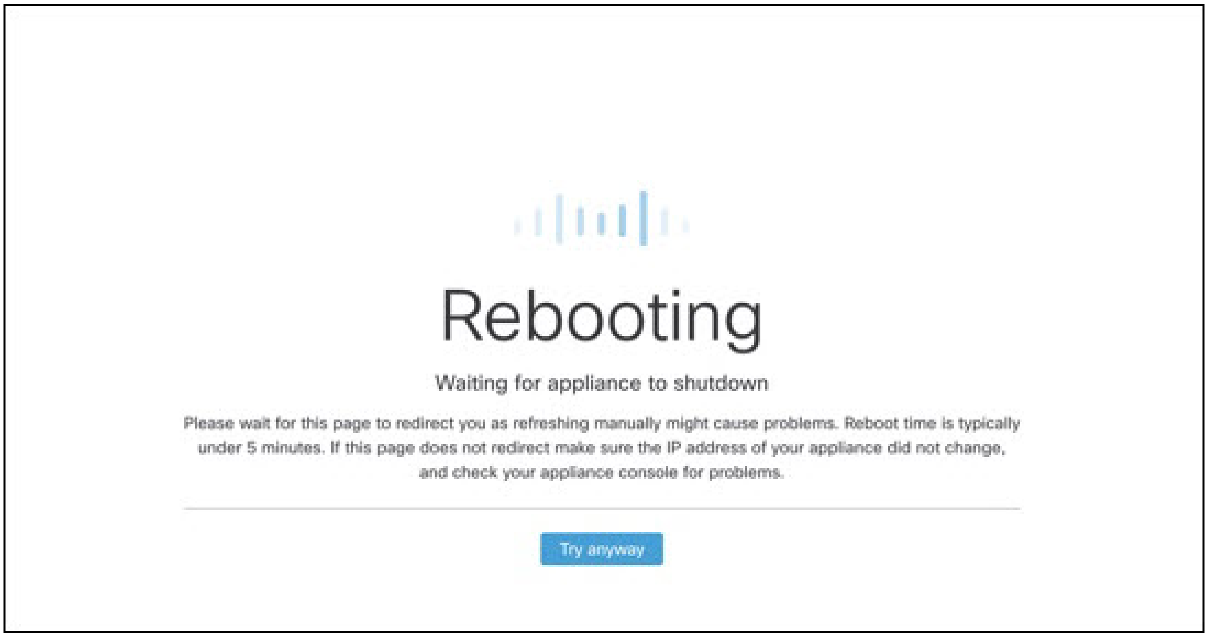
Your appliance configuration was applied. To complete your installation, you need to reboot.

© 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 2 Click **Reboot**.

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

Figure 19: Appliance is Rebooting



Rebooting

Waiting for appliance to shutdown

Please wait for this page to redirect you as refreshing manually might cause problems. Reboot time is typically under 5 minutes. If this page does not redirect make sure the IP address of your appliance did not change, and check your appliance console for problems.

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

Install Secure Malware Analytics Appliance Updates

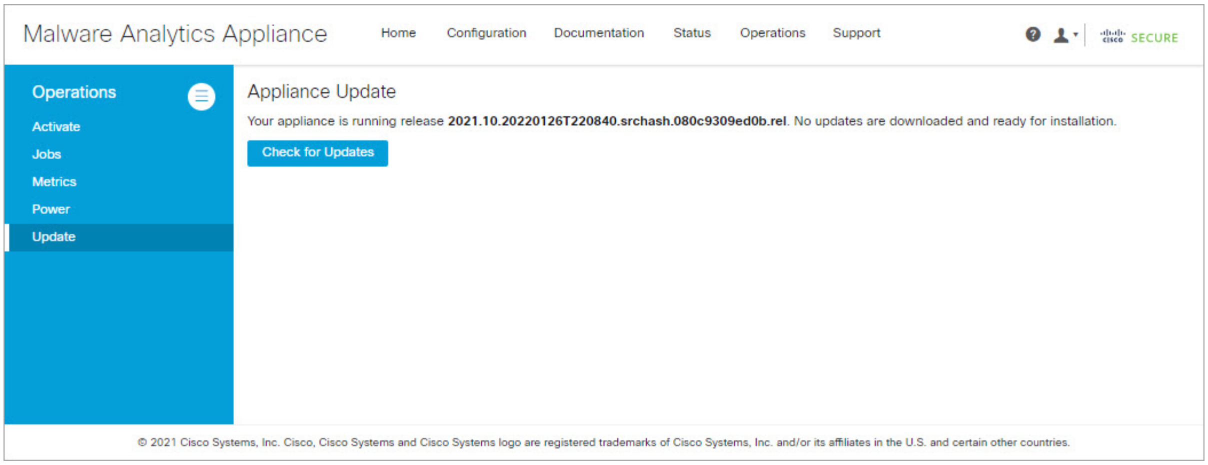
After you complete the initial Secure Malware Analytics Appliance setup, we recommend that you install any available updates before continuing. Secure Malware Analytics Appliance updates are applied through the Admin UI.

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 20: 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.

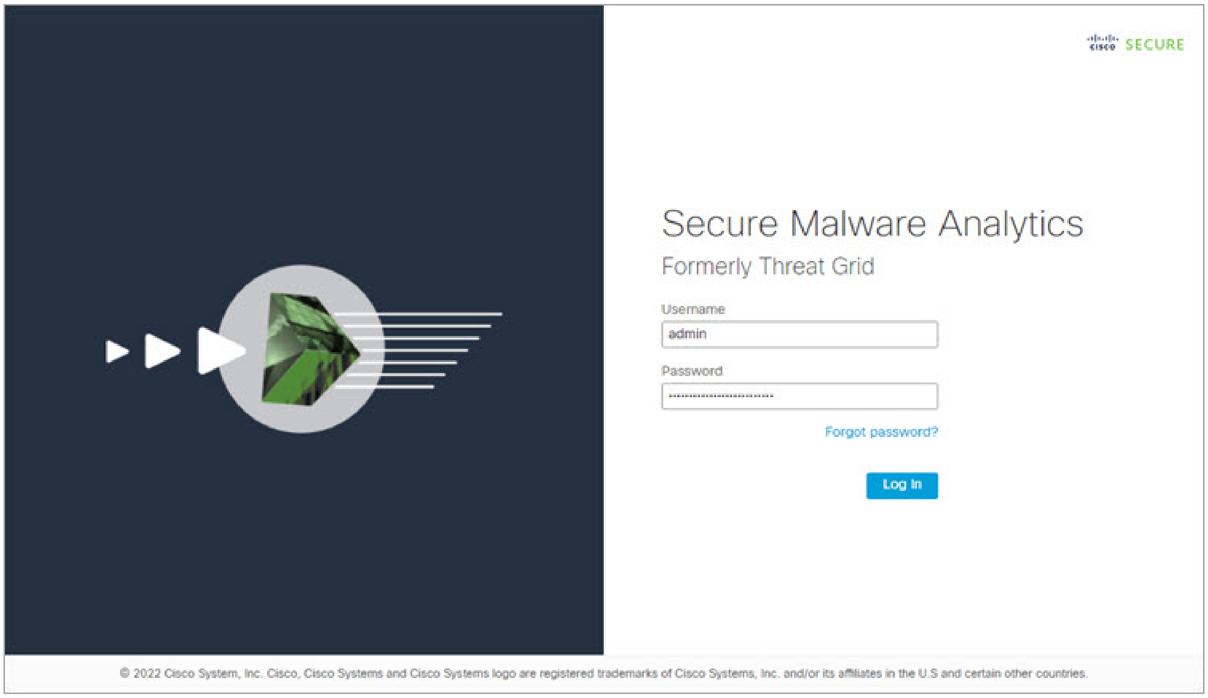
Test the Appliance Setup

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 21: Secure Malware Analytics Login



Secure Malware Analytics

Formerly Threat Grid

Username: admin

Password: ••••••••••••••••••••••••

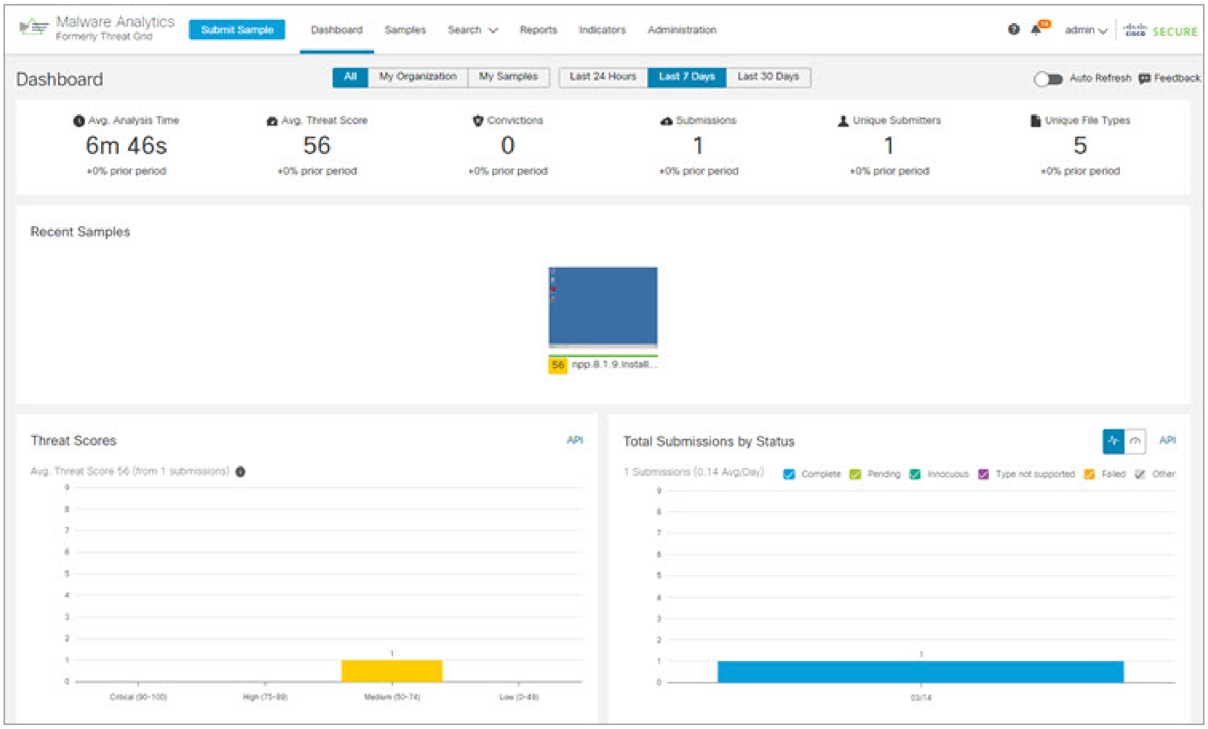
© 2022 Cisco System, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries.

Step 2 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 22: Secure Malware Analytics Dashboard



Avg. Analysis Time 6m 46s +0% prior period

Avg. Threat Score 56 +0% prior period

Convictions 0 +0% prior period

Submissions 1 +0% prior period

Unique Submitters 1 +0% prior period

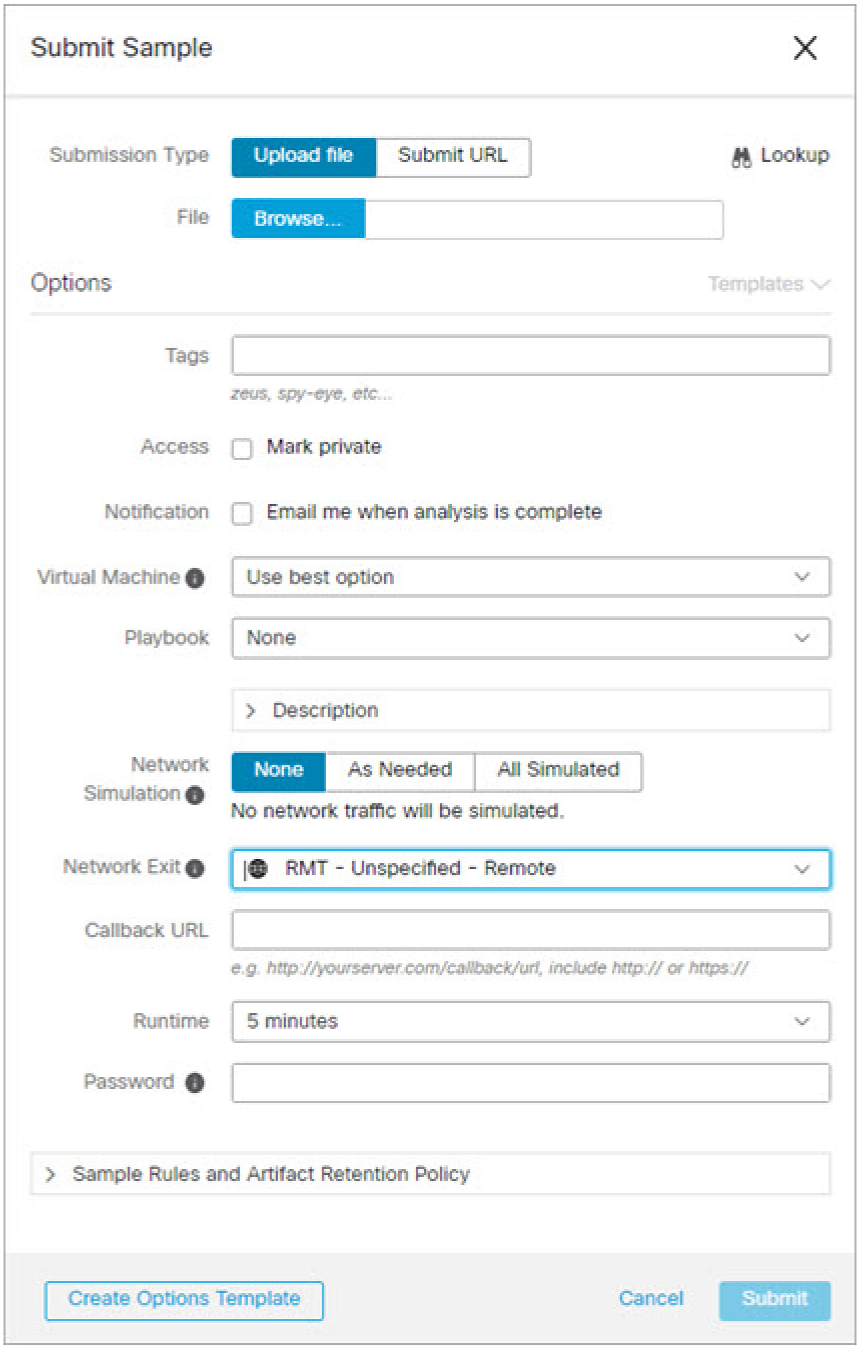
Unique File Types 5 +0% prior period

Avg. Threat Score 56 (from 1 submissions)

1 Submissions (0.14 Avg/Day)

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

Figure 23: Submit Sample



Submit Sample

Submission Type: Upload file | Submit URL

File: Browse...

Options

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

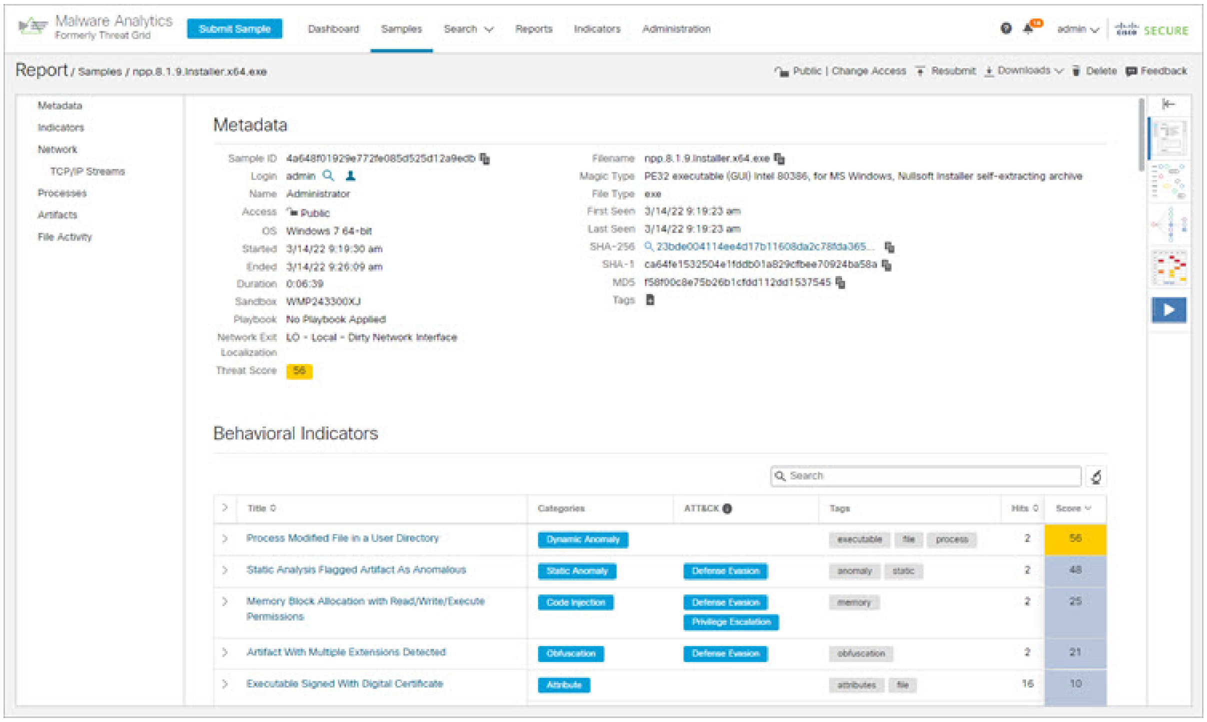
Note There is help available at the bottom of this form, describing sample submission file types, size, and other information. You can also click the **?** icon located in the upper-right corner to view the Secure Malware Analytics Release Notes and online help, including complete documentation on how 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 24: Analysis Report



Report / Samples / npp.8.1.9.Installer.x64.exe

Metadata

Sample ID	4a648f01929e772fe085d525d12a9edb	Filename	npp.8.1.9.Installer.x64.exe
Login	admin	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Name	Administrator	File Type	exe
Access	Public	First Seen	3/14/22 9:19:23 am
OS	Windows 7 64-bit	Last Seen	3/14/22 9:19:23 am
Started	3/14/22 9:19:30 am	SHA-256	23bde004114ee4d17b11608da2c78fda365...
Ended	3/14/22 9:26:09 am	SHA-1	ca64fe1532504e1fddb01a829cfbee70924ba58a
Duration	0:06:39	MD5	f58f00c8e75b26b1cfdd112dd1537545
Sandbox	WMP243300XJ	Tags	
Playbook	No Playbook Applied		
Network Exit Localization	LO - Local - Dirty Network Interface		
Threat Score	56		

Behavioral Indicators

Title	Categories	ATT&CK	Tags	Hits	Score
Process Modified File in a User Directory	Dynamic Anomaly		executable file process	2	56
Static Analysis Flagged Artifact As Anomalous	Static Anomaly	Defense Evasion	anomaly static	2	48
Memory Block Allocation with Read/Write/Execute Permissions	Code Injection	Defense Evasion Privilege Escalation	memory	2	25
Artifact With Multiple Extensions Detected	Obfuscation	Defense Evasion	obfuscation	2	21
Executable Signed With Digital Certificate	Attribute		attributes file	16	10

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.