



## **Cisco Threat Grid Appliance Getting Started Guide Version 2.11**

**First Published:** 2020-05-08

### **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 NON-INFRINGEMENT 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](http://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 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### **Introduction 1**

- About Cisco Threat Grid Appliance 1
- Audience 2
- Assumptions 2
- Product Documentation 2
- What's New In This Release 3
- Supported Browsers 3
- Updates 4
- Threat Grid Support 4
- Setup and Configuration Overview 6

---

### CHAPTER 2

#### **Initial Network Configuration 9**

- Power On and Boot Up Appliance 9
- Configure Network Using TGSH Dialog 10

---

### CHAPTER 3

#### **Admin UI Configuration 17**

- Introduction 17
  - Log In to the Admin UI 18
  - Change Admin Password 19
  - Review End User License Agreement 19
- Configuration Wizard 20
  - Configure Network Settings 20
  - Install License 21
  - Configure NFS 22
  - Configure Clustering 24
  - Configure Email 24

Configure Notifications	25
Configure Date and Time	26
Configure System Log	27
Review and Install Configuration Settings	28
Install Threat Grid Appliance Updates	30
Test the Appliance Setup	31



# CHAPTER 1

## Introduction

---

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

- [About Cisco Threat Grid 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 4](#)
- [Threat Grid Support, on page 4](#)
- [Setup and Configuration Overview, on page 6](#)

## About Cisco Threat Grid Appliance

The Cisco Threat Grid appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. A Threat Grid Appliance provides the complete Threat Grid malware analysis platform, installed on a Cisco Threat Grid 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-M3 (TG5000) and Cisco UCS C220 M4 (TG5400) servers are still supported for Threat Grid Appliance but the servers are end of life. See the Server Setup chapter in the *Cisco Threat Grid 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 Threat Grid Appliance on-premises, organizations can send suspicious documents and files to it to be analyzed without leaving the network.

With a Threat Grid 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 Threat Grid Appliance.

This document describes how to complete the initial setup and configuration for a new Threat Grid 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 Threat Grid Appliance Administration Guide*.

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

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

## Product Documentation

The latest versions of Cisco Threat Grid Appliance product documentation can be found on Cisco.com:

- *Cisco Threat Grid Appliance Release Notes*
- *Cisco Threat Grid Version Lookup Table*
- *Cisco Threat Grid Appliance Administration Guide*
- *Cisco Threat Grid M5 Hardware Installation Guide*



---

**Note** The Cisco Threat Grid M5 Appliance is supported in Threat Grid Version 3.5.27 and later, and appliance version 2.7.2 and later.

---



---

**Note** Prior versions of Cisco Threat Grid Appliance product documentation can be found at [Threat Grid Install and Upgrade](#).

---

### Threat Grid Portal UI Online Help

Threat Grid Portal user documentation, including Release Notes, Threat Grid 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 2.11:

**Table 1: Changes in Version 2.11 - May 8, 2020**

Feature or Update	Section
Moved the following information to the <i>Cisco Threat Grid Appliance Administration Guide</i> : <ul style="list-style-type: none"> <li>• Enable Support Mode</li> <li>• Support Snapshots</li> <li>• Planning</li> </ul>	NA
Moved the following topics to the Introduction chapter in this guide: <ul style="list-style-type: none"> <li>• Supported Browsers</li> <li>• Updates</li> </ul>	<a href="#">Supported Browsers</a> <a href="#">Updates</a>
OpAdmin is replaced with a completely modernized Admin user interface.	NA
Updated Admin UI configuration and screenshots.	<a href="#">Admin UI Configuration</a>

## Supported Browsers

Threat Grid supports the following browsers:

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



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

# Updates

The initial Threat Grid Appliance setup and configuration steps **must be completed** before installing any Threat Grid Appliance updates. We recommend that you check for updates immediately after completing the initial configuration (see [Install Threat Grid Appliance Updates](#)).

Threat Grid 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.



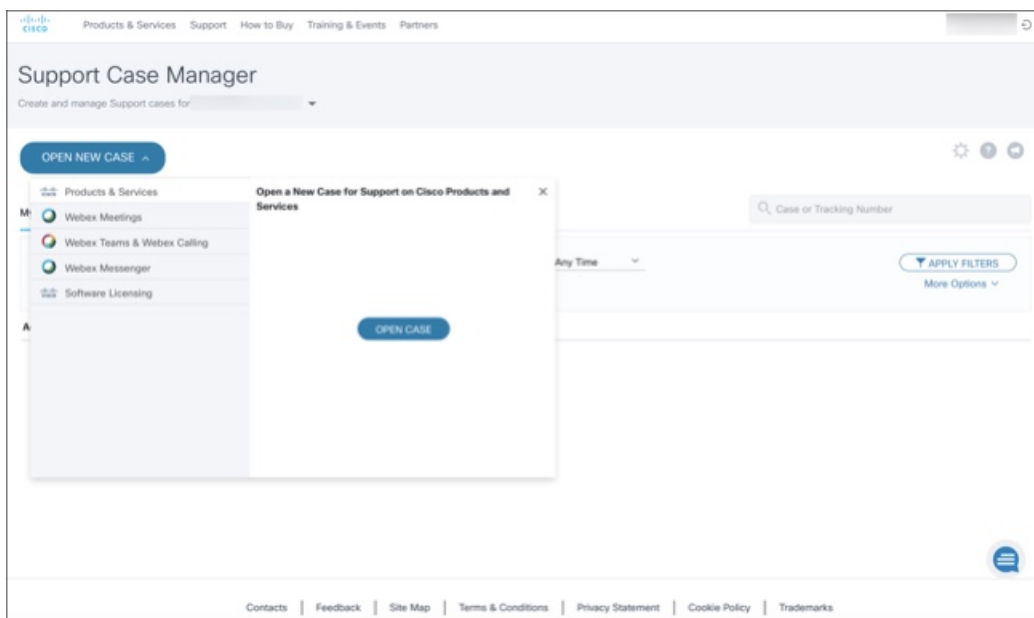
**Note** Verify that SSH is specified for updates.

## Threat Grid Support

If you have questions or require assistance with Threat Grid, 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 Threat Grid.

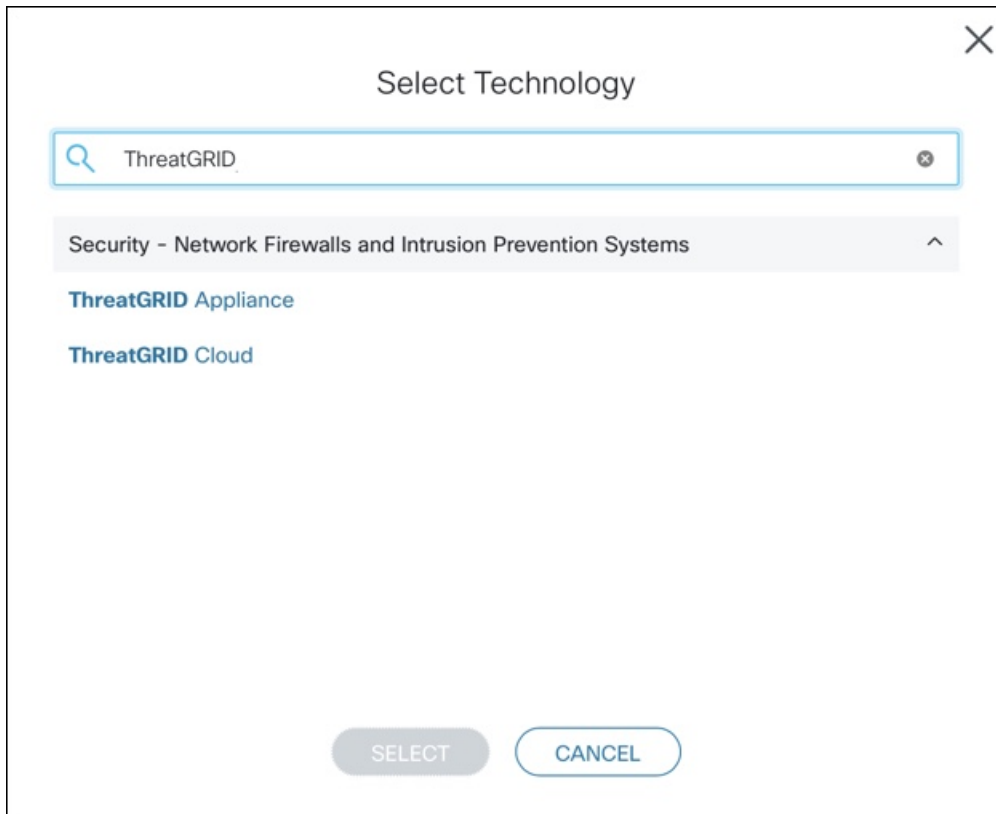


**Figure 2: Check Entitlement**

The screenshot shows the 'Support Case Manager' interface. At the top, there are navigation links: 'Products & Services', 'Support', 'How to Buy', 'Training & Events', and 'Partners'. Below the navigation is the title 'Support Case Manager' and a sub-header 'Open a new support case for'. A progress bar indicates three steps: 1. Check Entitlement (active), 2. Describe Problem, and 3. Review & Submit. Below the progress bar, there are radio buttons for 'Request Type': 'Diagnose and Fix', 'Request RMA', and 'Ask a Question' (selected). Under 'Ask a Question', there are two expandable sections: 'Find Product by Serial Number' and 'Find Product by Service Agreement'. Below these is a 'Bypass Entitlement' section with a dropdown menu showing 'CPR / Contract data not in C3'. At the bottom, there are two buttons: 'NEXT' and 'Save draft and exit'.

- Step 3** On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Threat Grid Appliance in the title).
- Step 4** Click **Manually select a Technology** and search for **ThreatGRID**.

Figure 3: Select Technology



The screenshot shows a 'Select Technology' dialog box. At the top right is a close button (X). Below the title is a search input field containing 'ThreatGRID'. A dropdown menu is open, showing a category 'Security - Network Firewalls and Intrusion Prevention Systems' with an upward arrow. Underneath are two search results: 'ThreatGRID Appliance' and 'ThreatGRID Cloud'. At the bottom of the dialog are two buttons: 'SELECT' and 'CANCEL'.

**Step 5** Choose **ThreatGRID 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 *Threat Grid Appliance Administration Guide*.
- See the blog post: **Changes to the Cisco Threat Grid 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 Threat Grid Appliance Administration Guide](#).





## CHAPTER 2

# Initial Network Configuration

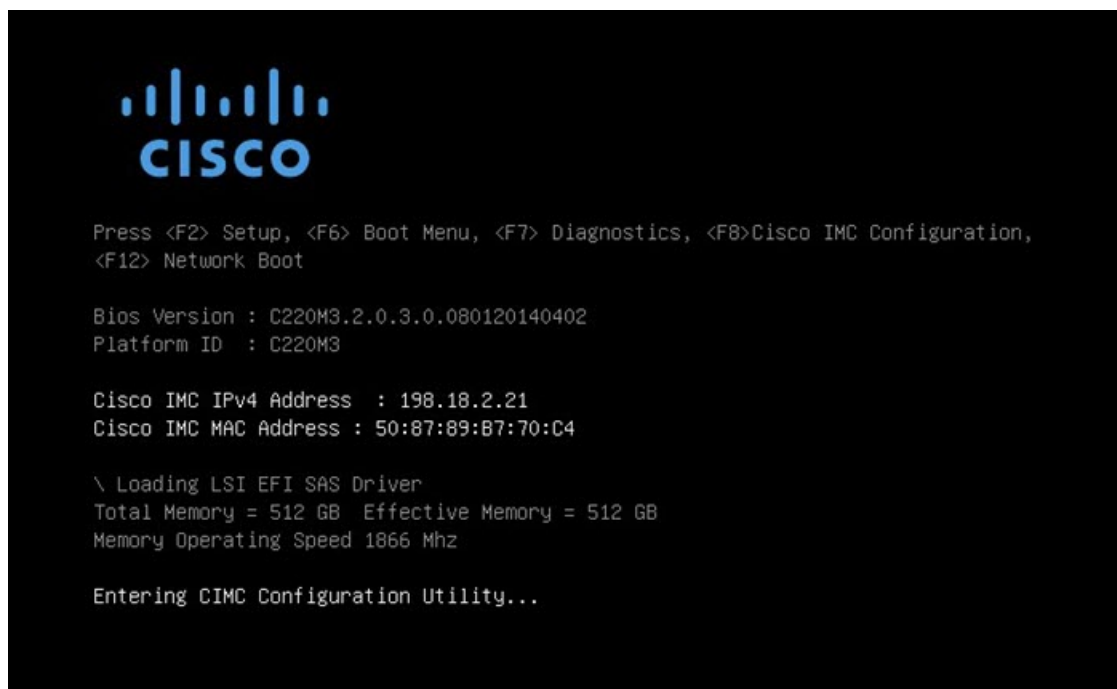
This chapter provides instructions for completing the initial network configuration using the TGS Dialog. It includes the following topics:

- [Power On and Boot Up Appliance, on page 9](#)
- [Configure Network Using TGS Dialog, on page 10](#)

## Power On and Boot Up Appliance

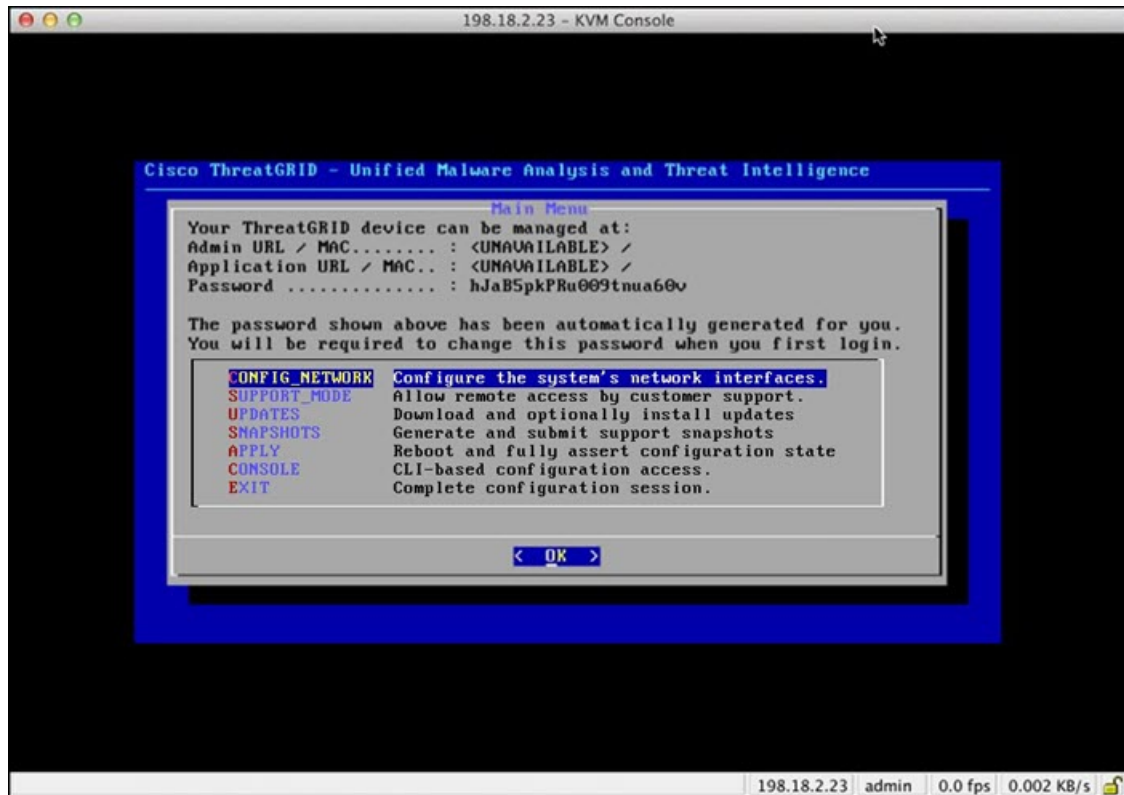
Once you have connected the server peripherals, network interfaces, and power cables, turn on the Threat Grid M5 Appliance and wait for it to boot up. The Cisco screen is briefly displayed.

*Figure 4: Cisco Screen During Bootup*



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

Figure 5: TGSH Dialog



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 **TGSH Dialog** 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 TGSH Dialog

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

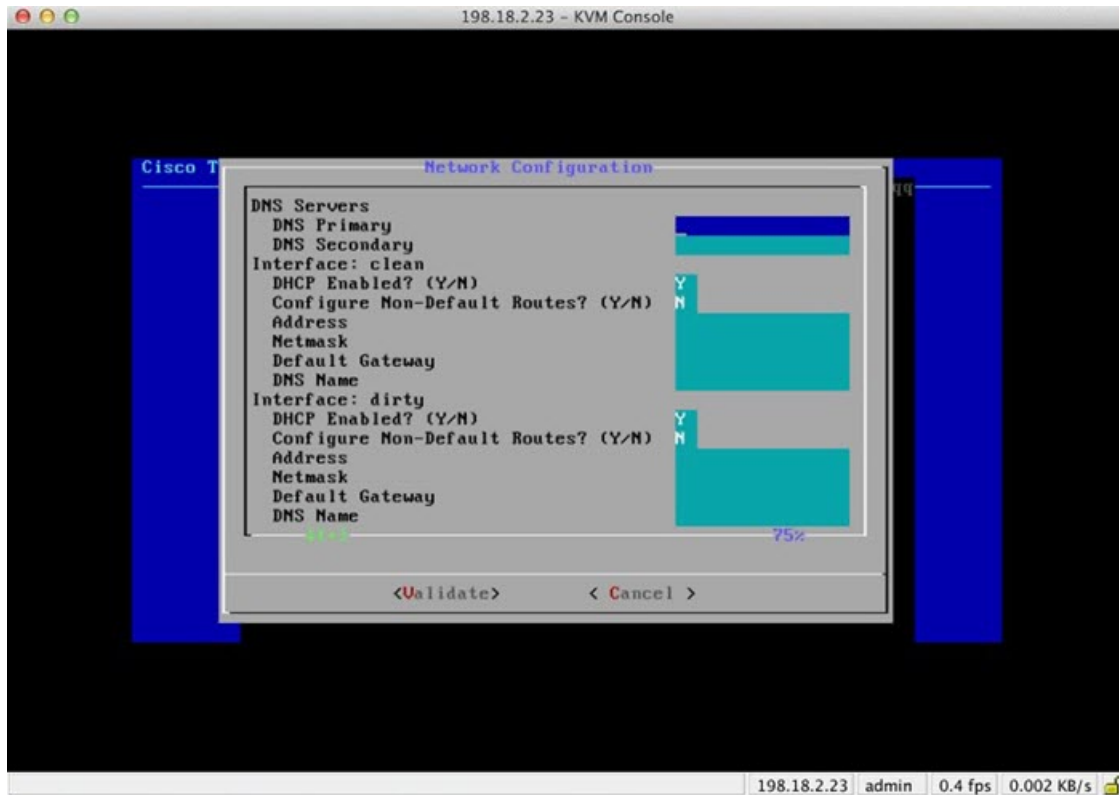


### Note

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 Threat Grid Appliance Administration Guide](#).

**Step 1** On the TGSH Dialog, select **CONFIG\_NETWORK**. The **Network Configuration** console opens.

Figure 6: TGSH Dialog - Network Configuration Console



**Step 2** Complete the blank fields according to the settings provided by your network administrator for the Clean, Dirty, and Admin interfaces.

**Step 3** Change **DHCP Enabled** to N.

**Note** You need to backspace over the old character before you can enter the new one.

**Step 4** Leave the **Configure Non-Default Routes** field set to the default N (unless additional routes are needed).

**Step 5** If your network is using a DNS name for the Clean network, enter the name in the **DNS Name** field.

**Step 6** Leave the Dirty network **DNS Name** field blank.

Figure 7: Network Configuration In-Progress (Clean and Dirty)

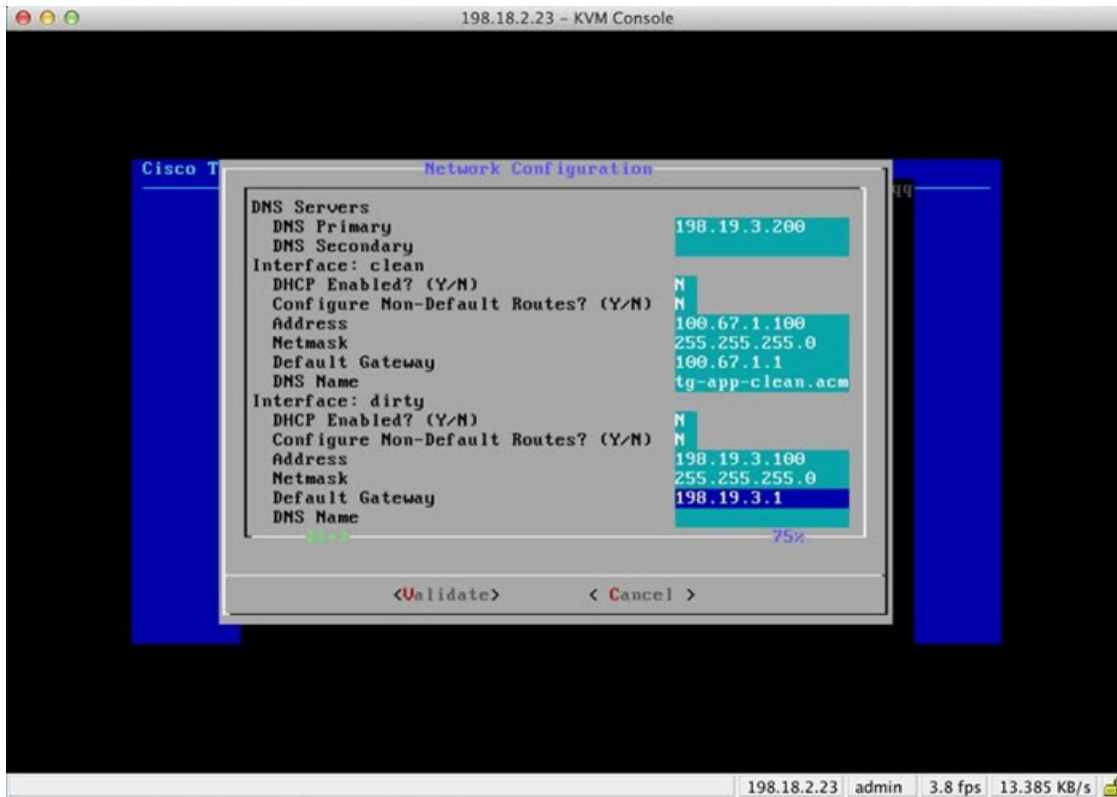
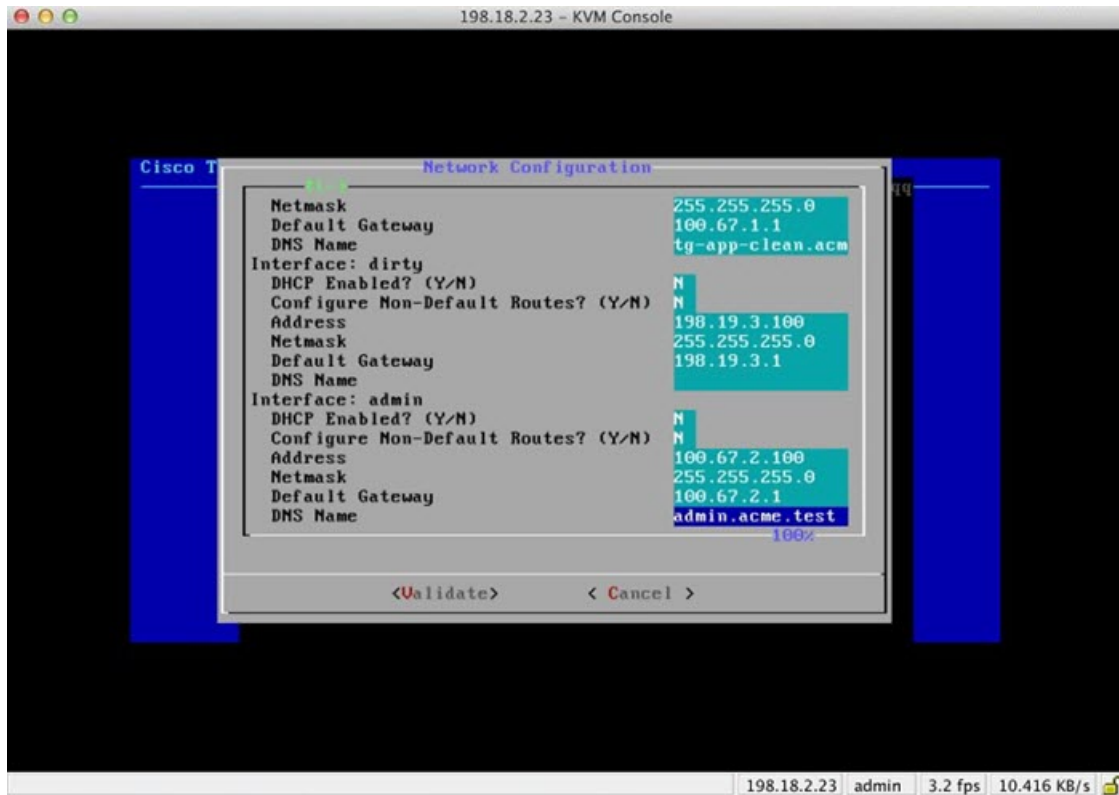


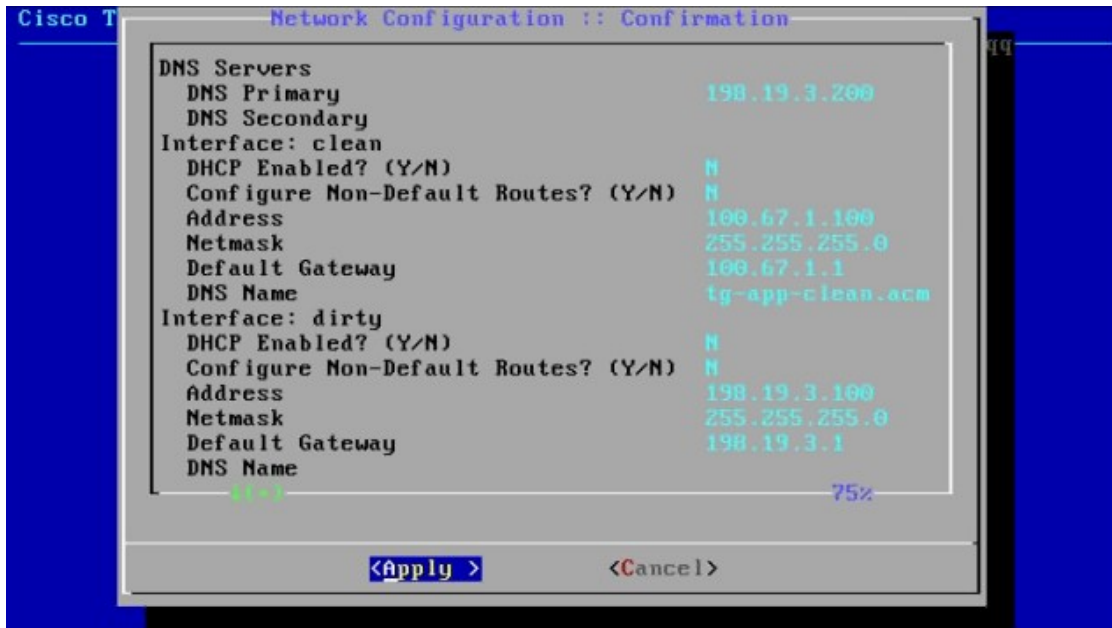


Figure 8: Network Configuration In-Progress (Admin)



- Step 7** After you finish entering all the network settings, tab down and select **Validate** to verify your entries. If errors occur, fix the invalid values and select **Validate** again. After validation, the **Network Configuration Confirmation** page displays the entered values.

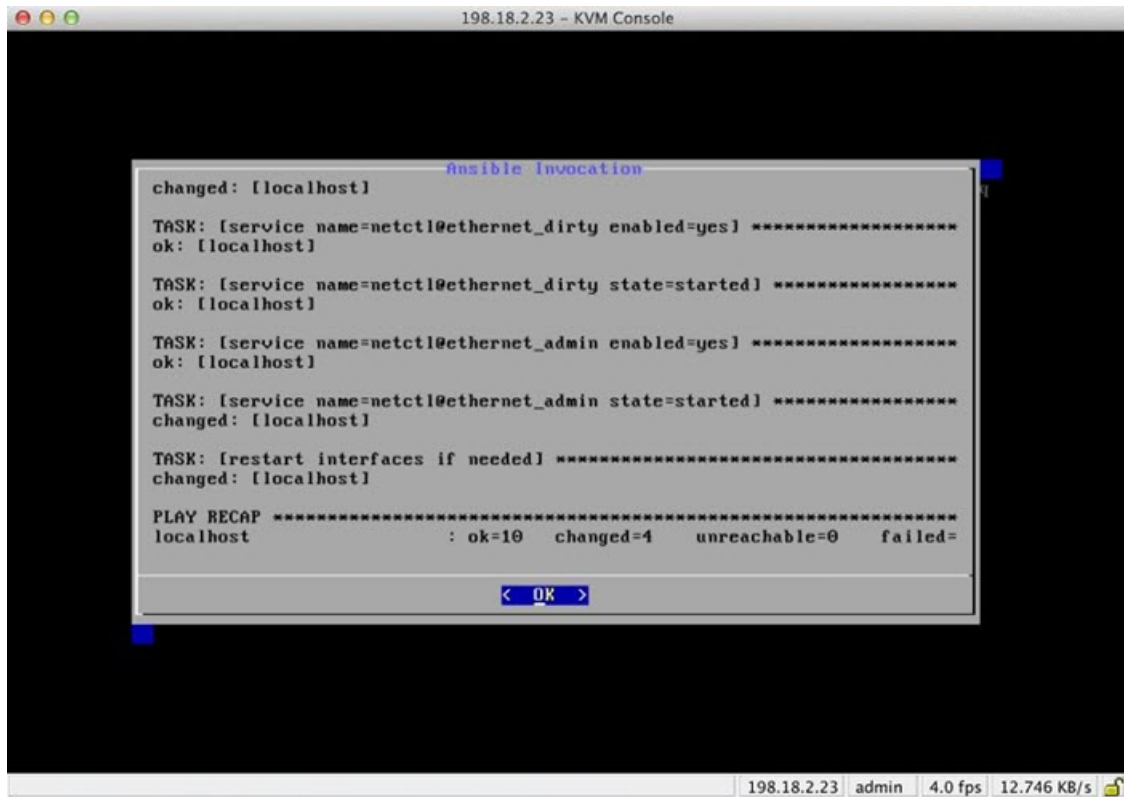
Figure 9: Network Configuration Confirmation



**Step 8** Select **Apply** to apply your configuration settings.

After the configuration settings are applied (it may take 10 minutes or more to complete), details about the changes are displayed.

Figure 10: Network Configuration - List of Changes Made



```
198.18.2.23 - KVM Console

changed: [localhost]
Ansible Invocation
TASK: [service name=netctl@ethernet_dirty enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_dirty state=started] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin state=started] *****
changed: [localhost]
TASK: [restart interfaces if needed] *****
changed: [localhost]
PLAY RECAP *****
localhost : ok=10  changed=4  unreachable=0  failed=

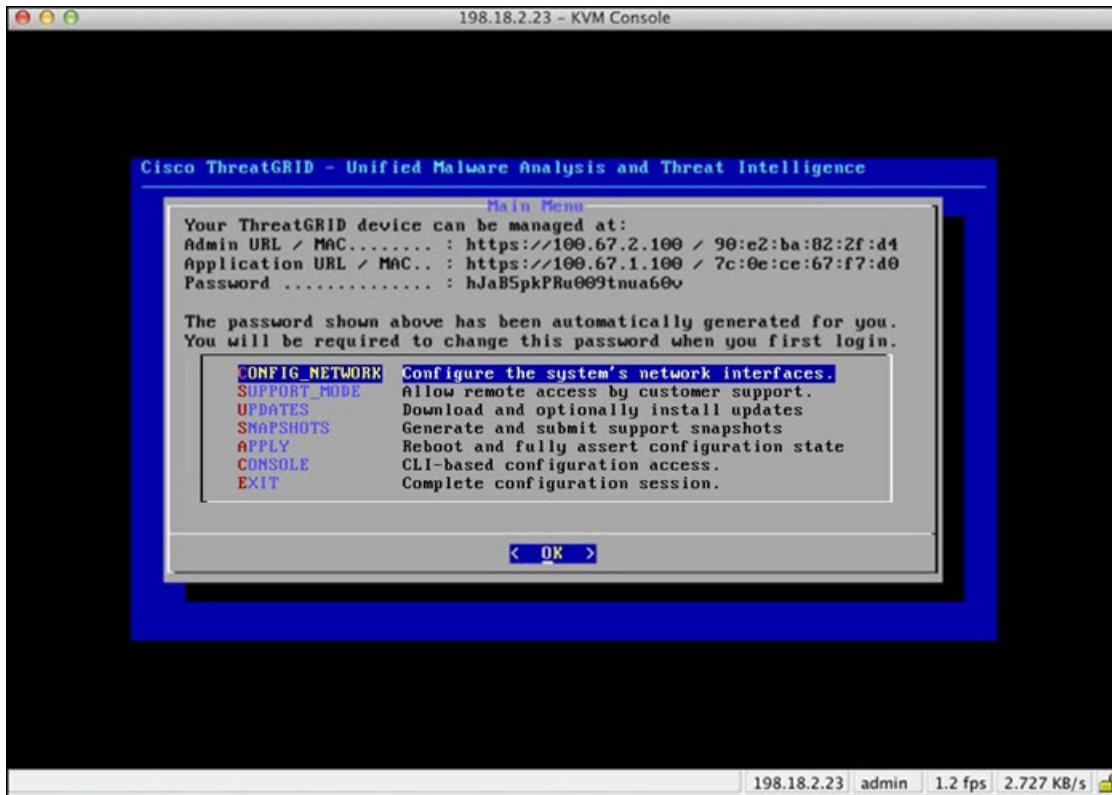
< OK >
```

198.18.2.23 | admin | 4.0 fps | 12.746 KB/s

**Step 9** Select **OK**.

The **Network Configuration** console refreshes again and displays the entered IP addresses.

Figure 11: IP Addresses



You have completed the network configuration of your Threat Grid Appliance.

**Note** The URL for the Clean interface is not active until the Admin UI configuration is complete.

### What to do next

The next step in the Threat Grid 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 17](#)
- [Configuration Wizard, on page 20](#)
- [Install Threat Grid Appliance Updates, on page 30](#)
- [Test the Appliance Setup, on page 31](#)

## Introduction

The Admin UI is the recommended tool for administrators to use to configure the Threat Grid 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 Threat Grid Appliance Administration Guide](#) for configuring settings not included in the wizard, such as SSL Certificates and Clustering.



**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 Threat Grid Admin UI.

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

**Note** The Hostname is the appliance serial number.

*Figure 12: Admin UI Login Screen*



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

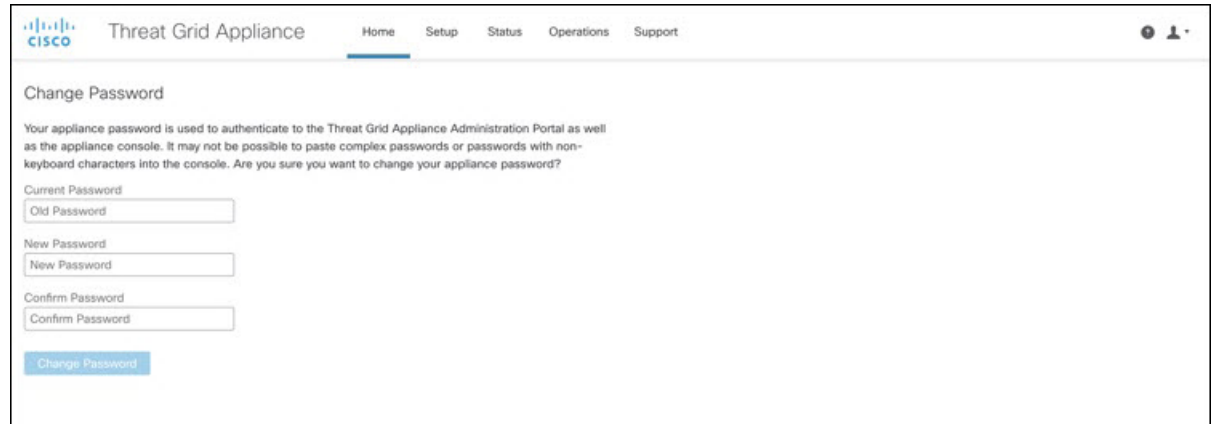
### What to do next

Proceed to [Change Admin Password](#).

## Change Admin Password

The initial Admin password was generated randomly during the pre-ship Threat Grid installation and is visible as plain text in the TGS Dialog. You must change the initial Admin password before continuing with the configuration.

**Figure 13: Change Admin Password**



The screenshot shows the 'Change Password' page in the Threat Grid Appliance administration portal. The page has a header with the Cisco logo and navigation links for Home, Setup, Status, Operations, and Support. The main content area is titled 'Change Password' and contains a warning message: 'Your appliance password is used to authenticate to the Threat Grid 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?'. Below the warning are three input fields: 'Current Password' (with a sub-label 'Old Password'), 'New Password' (with a sub-label 'New Password'), and 'Confirm Password' (with a sub-label 'Confirm Password'). A blue 'Change Password' button is located at the bottom of the form.

**Step 1** Enter the old password from the TGS Dialog 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 TGS Dialog 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 Threat Grid Appliance.

### Configure Network Settings

If you configured static network settings in the TGS Dialog, the IP addresses displayed on the **Network Configuration** page reflect the values you entered in the TGS Dialog during the Threat Grid Appliance network configuration.

**Figure 14: Network Configuration**

The screenshot displays the 'Network Configuration' page in the Threat Grid Appliance admin UI. On the left, a 'Configuration Wizard' sidebar lists steps: 1. Network (Configure Networking), 2. License (Upload license), 3. NFS (Configure NFS), 4. Clustering (Configure Clustering), 5. Email (Configure Email), 6. Notifications (Configure Notifications), 7. Date and Time (Configure Date and Time), 8. System Log (Configure Logging), and 9. Review and Install (Done!). The main content area is titled 'Network Configuration' and is divided into two sections: 'CLEAN interface' and 'DIRTY interface'. For the 'CLEAN interface', the MAC Address is shown as '00:0c:29:00:00:00' and the IP Address is '10.10.10.10 (DHCP)'. Below this, there is a dropdown menu for 'IP Assignment' set to 'DHCP', a text input for 'Host Name' containing 'tgs-000000000000', and text inputs for 'Primary DNS Server' (IP) and 'Secondary DNS Server' (IP). The 'DIRTY interface' section shows a MAC Address of '00:0c:29:00:00:00' and an IP Address of 'Unassigned (DHCP)'. It also has a dropdown for 'IP Assignment' set to 'DHCP', and text inputs for 'Primary DNS Server' (IP) and '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 Threat Grid Appliance Administration Guide](#).

### What to do next

Proceed to [Install License](#).

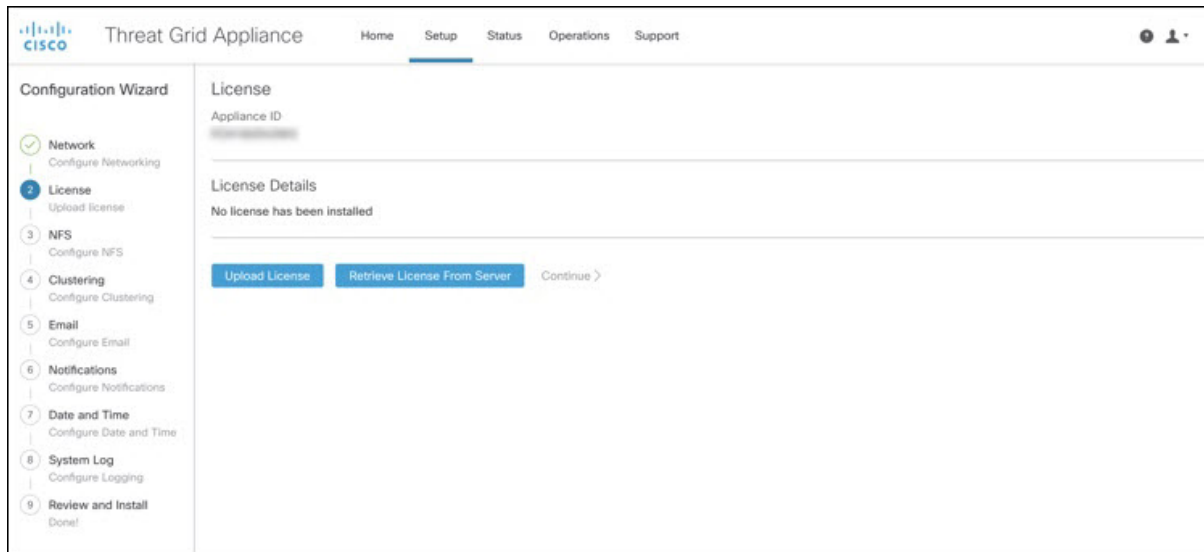


# Install License

After the networks are configured, you are ready to install the Threat Grid license.

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

*Figure 15: License Page Prior to Installation*



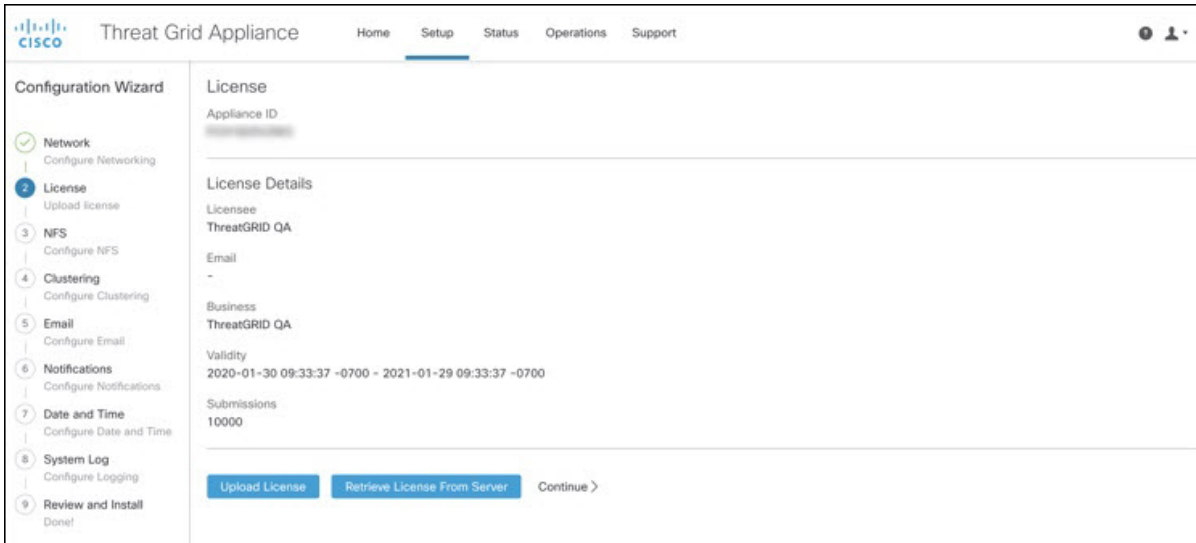
**Step 2** Click **Upload License** and select the license file from your file manager.

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 3** Enter your license password in the **Passphrase** field.

**Step 4** Click **Save** to install the license. The page refreshes and your license information is displayed.

Figure 16: License Information After Successful Installation



**Step 5** Click **Continue**.

### What to do next

Proceed to [Configure NFS](#).

## Configure NFS

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

The configuration process includes mounting the NFS store, mounting the encrypted data, and initializing the Threat Grid 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.

Figure 17: NFS Configuration

**Step 2** 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 3** 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 4** Click **Activate** to activate the key. The Activating Key dialog is displayed.

**Step 5** When activation has succeeded, click **Continue**.

### What to do next

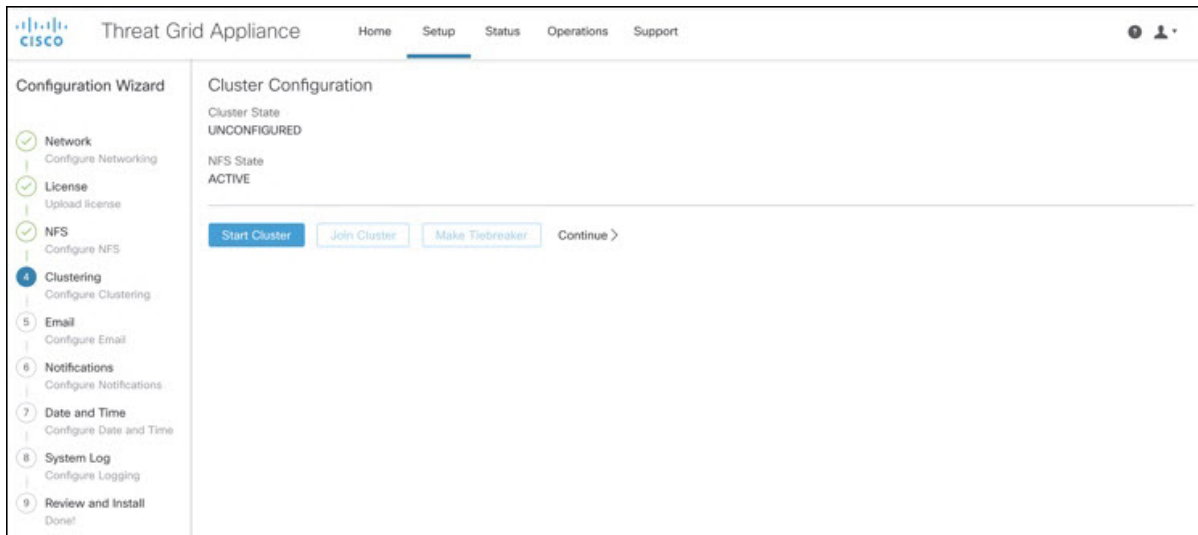
Proceed to [Configure Clustering](#).

## Configure Clustering

The next step in the wizard workflow is to configure clustering.

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

**Figure 18: Cluster Configuration**



**Step 2** See Clustering in the *Threat Grid Appliance Administration Guide* for more information. We recommend that you skip this step during the initial configuration, and return once configuration is completed.

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

### What to do next

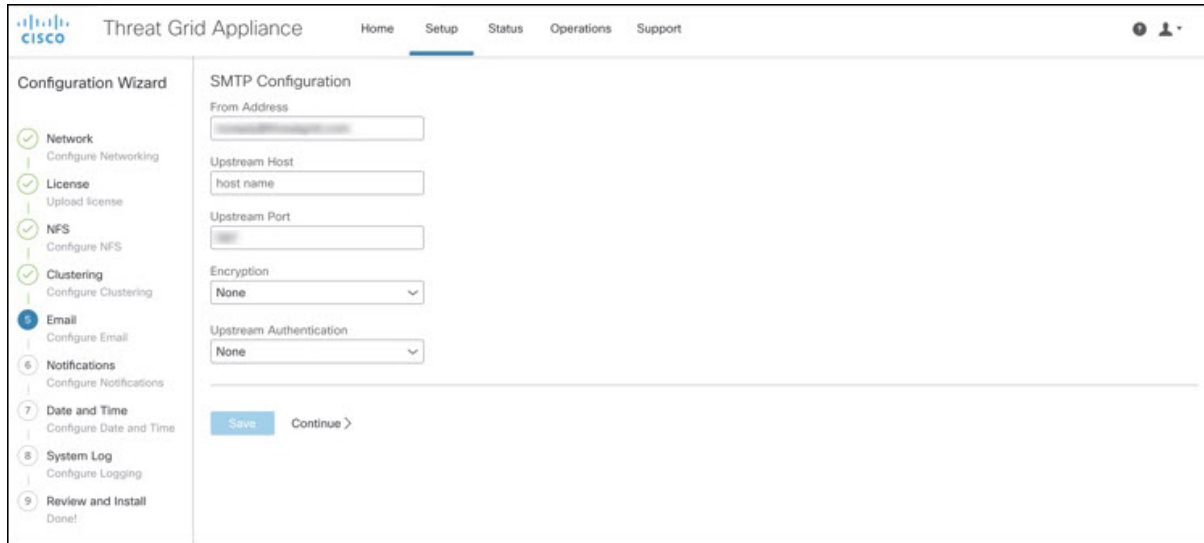
Proceed to [Configure Email](#).

## Configure Email

The next step in the workflow is to configure the email host.

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

Figure 19: SMTP Configuration



The screenshot shows the Threat Grid Appliance Configuration Wizard. The left sidebar lists the steps: Network, License, NFS, Clustering, Email, Notifications, Date and Time, System Log, and Review and Install. The main panel is titled "SMTP Configuration" and contains the following fields:

- From Address:
- Upstream Host:
- Upstream Port:
- Encryption:
- Upstream Authentication:

At the bottom of the main panel, there are two buttons: "Save" and "Continue >".

- Step 2** Enter the email From Address.
- Step 3** Enter the name of the Upstream Host (email host).
- Step 4** Change the port from **587** to **25**.
- Step 5** Keep the defaults for the other settings.
- Step 6** Click **Save** to save your settings.
- Step 7** 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 Threat Grid portal interface, but this page allows you to set up notifications that are also sent via email.

- Step 1** Click **Notifications** in the navigation pane to open the **Notifications** page.

Figure 20: Notifications

The screenshot shows the Cisco Threat Grid Appliance Admin UI. The top navigation bar includes Home, Setup, Status, Operations, and Support. The left sidebar shows the Configuration Wizard steps: Network, License, NFS, Clustering, Email, Notifications (highlighted), Date and Time, System Log, and Review and Install. The main content area is titled 'Notifications' and contains the following fields:

- Recipient:** Email Addresses field with a text input containing 'recipient@domain.com' and a plus icon to add more.
- Notification Frequency:** Two dropdown menus. The 'Critical' dropdown is set to 'Every hour' and the 'Non-critical' dropdown is set to 'Every Week'.

At the bottom of the form are 'Save' and 'Continue >' buttons.

- Step 2** 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 3** Under **Notification Frequency**, choose the settings for **Critical** and **Non-critical** from the drop-down lists.
- Step 4** Click **Save**.
- Step 5** 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** Click **Date and Time** in the navigation pane to open the **Date and Time** page.

Figure 21: Date and Time

The screenshot shows the Cisco Threat Grid Appliance Admin UI. The top navigation bar includes 'Home', 'Setup', 'Status', 'Operations', and 'Support'. The 'Setup' tab is active. On the left, a 'Configuration Wizard' sidebar lists steps: Network (Configure Networking), License (Upload license), NFS (Configure NFS), Clustering (Configure Clustering), Email (Configure Email), Notifications (Configure Notifications), Date and Time (Configure Date and Time), System Log (Configure Logging), and Review and Install (Done!). The 'Date and Time' step is highlighted with a blue circle. The main content area is titled 'Date and Time' and contains an 'NTP servers' section with a text input field, a clear 'X' button, and an add '+' button. Below the input field are 'Save' and 'Continue >' buttons.

- Step 2** Enter the **NTP Server(s)** IP or NTP name.  
If there are multiple NTP servers, click the + icon to add another field; repeat as needed.
- Step 3** Click **Save**.
- Step 4** 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** Click **System Log** in the navigation pane to open the **System Log Server Information** page.

Figure 22: System Log Server Information

The screenshot shows the Cisco Threat Grid Appliance Admin UI. The top navigation bar includes 'Home', 'Setup', 'Status', 'Operations', and 'Support'. The 'Setup' tab is active. On the left, a 'Configuration Wizard' sidebar lists steps: Network (Configure Networking), License (Upload license), NFS (Configure NFS), Clustering (Configure Clustering), Email (Configure Email), Notifications (Configure Notifications), Date and Time (Configure Date and Time), System Log (Configure Logging), and Review and Install (Done!). The main content area is titled 'System Log Server Information' and contains three input fields: 'Host URL' (empty), 'Host Port' (531), and 'Protocol' (TCP). Below these fields are 'Save' and 'Continue >' buttons.

**Step 2** Complete the Host URL, Host Port, and Protocol fields and click **Save**.

**Step 3** 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

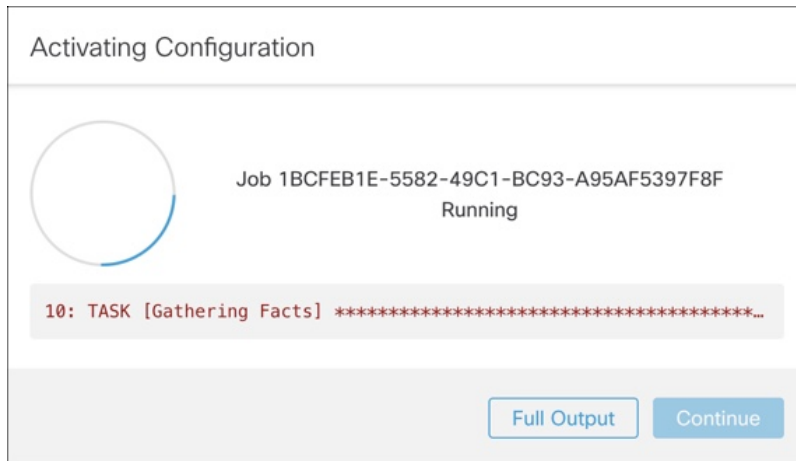
The final step in the workflow is to review and install your network configuration settings.

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

**Note** The installation may take over 10 minutes to complete. The screen displays configuration information as it is applied.

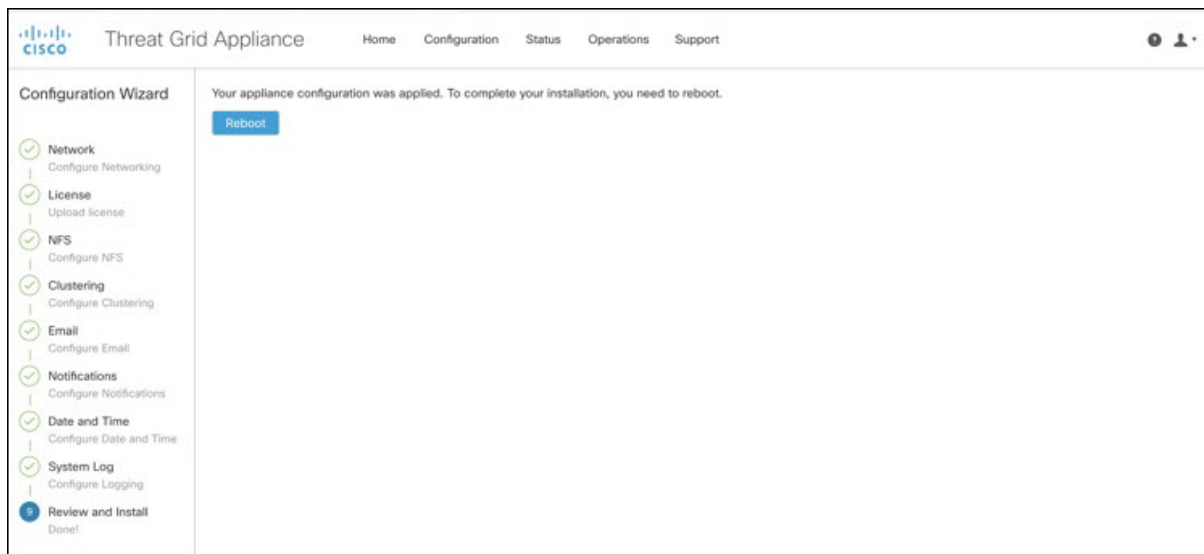


Figure 23: Activating Configuration



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

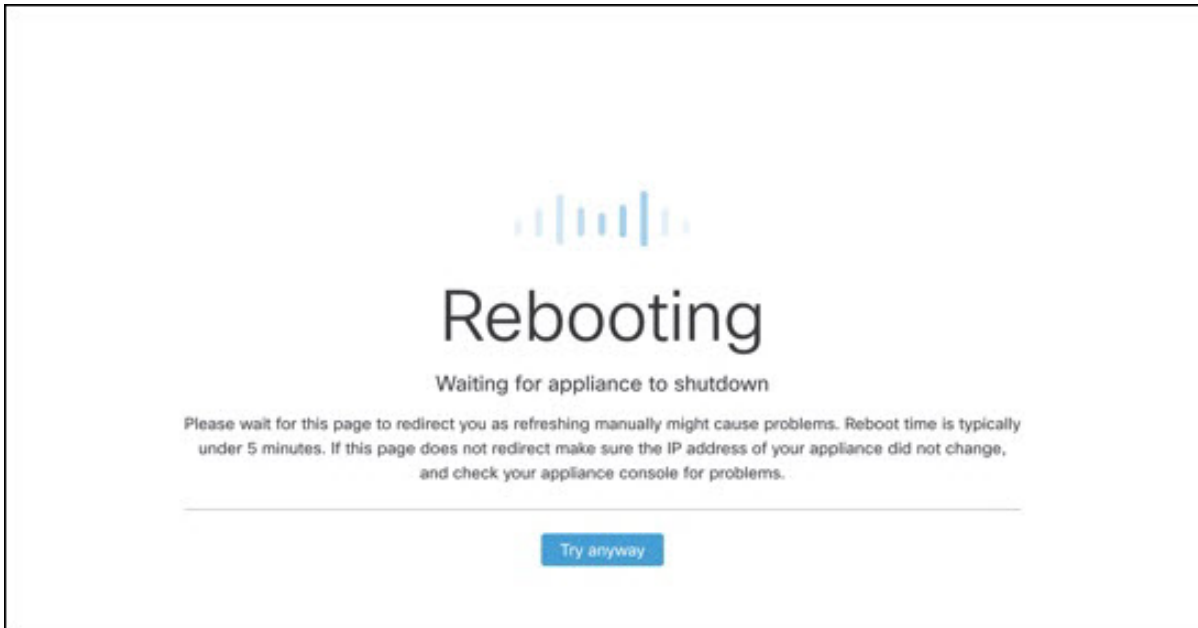
Figure 24: Successful Appliance Installation



**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 25: Appliance is Rebooting



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

## Install Threat Grid Appliance Updates

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

Users with air-gapped implementations may contact [Threat Grid Support](#) and request a downloadable update boot image.

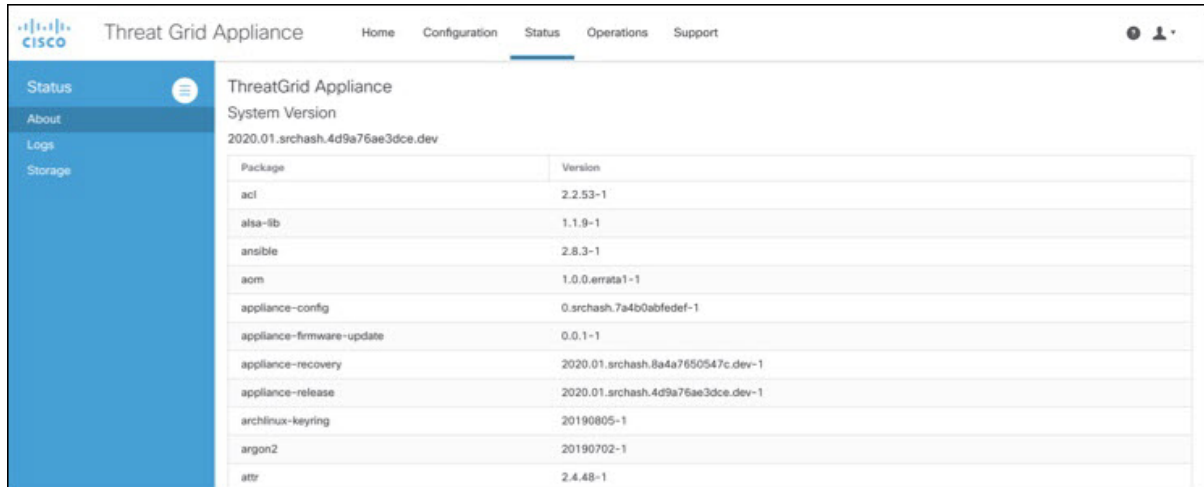


**Note** For more information about installing updates, see the [Cisco Threat Grid Appliance Administration Guide](#).

**Step 1** Log in to the Admin UI, if you are not already logged in.

**Step 2** From the **Operations** menu, choose **Update Appliance** to open the **Updates** page, which displays the current build of the appliance.

Figure 26: Appliance Build Number



The screenshot shows the Threat Grid Appliance Status page. The left sidebar contains navigation options: Status, About, Logs, and Storage. The main content area displays the system version as 2020.01.srchash.4d9a76ae3dce.dev and a table of installed packages with their versions.

Package	Version
acl	2.2.53-1
alsa-lib	1.1.9-1
ansible	2.8.3-1
aom	1.0.0.errata1-1
appliance-config	0.srchash.7a4b0abfedef-1
appliance-firmware-update	0.0.1-1
appliance-recovery	2020.01.srchash.8a4a7650547c.dev-1
appliance-release	2020.01.srchash.4d9a76ae3dce.dev-1
archlinux-keyring	20190805-1
argon2	20190702-1
attr	2.4.48-1

**Note** See the [Cisco Threat Grid Appliance Version Lookup Table](#) for the corresponding release version.

**Step 3** Click **Check for Updates**.

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

**Step 4** Once the updates have been downloaded, click **Apply Update** to install them.

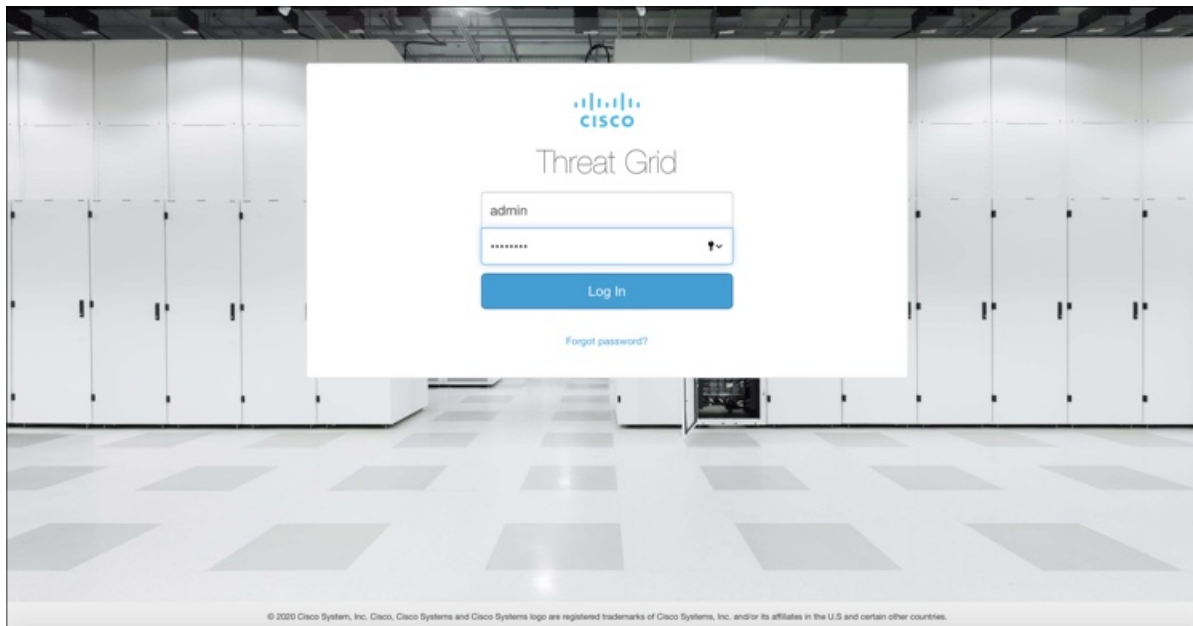
## Test the Appliance Setup

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

**Step 1** In a browser, open Threat Grid using the address you configured as the Clean interface.

The Threat Grid login page opens.

Figure 27: Threat Grid Login

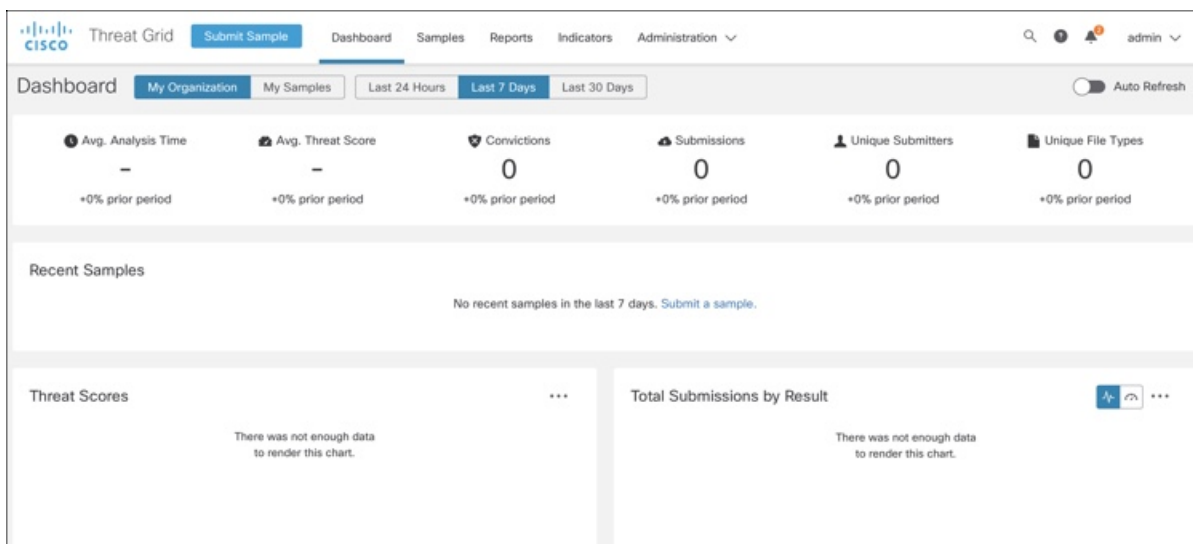


**Step 2** Enter the default credentials:

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

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

Figure 28: Threat Grid Dashboard



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

Figure 29: Submit Sample

Submit Sample

Submission Type

URL

Sample Name

Options

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

Access  Mark private

Notification  Email me when analysis is complete

Virtual Machine

Playbook

> Description

Network Simulation

No network traffic will be simulated.

**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 Threat Grid 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 Threat Grid 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 30: Analysis Report**

The screenshot shows the Cisco Threat Grid interface. The top navigation bar includes 'Submit Sample', 'Dashboard', 'Samples', 'Reports', 'Indicators', and 'Administration'. The user is logged in as 'admin'. The main content area is titled 'Report / Samples / Burning Daylight.pdf' and includes options for 'Public', 'Change Access', 'Resubmit', 'Downloads', and 'Delete'. A left sidebar lists various analysis categories like Metrics, Metadata, Indicators, Network, TCP/IP Streams, Processes, Artifacts, Registry Activity, Consolidated, Created Keys, Modified Keys, Deleted Keys, and File Activity. The main panel displays the following information:

Metrics	
Threat Score	56

Metadata			
Sample ID	81dfa29471f3edc0b360c1b312db2f1b	Filename	Burning Daylight.pdf
Submitted By	admin	Magic Type	PDF document, version 1.5
OS	Windows 7 64-bit	File Type	pdf
Started	4/30/20 11:49:47 am	First Seen	4/30/20 11:49:40 am
Ended	4/30/20 11:56:55 am	Last Seen	4/30/20 11:49:40 am
Duration	0:07:08	SHA-256	c3ed5099be47d523b34ab502f49392d2fd4e...
Sandbox	FCH1825V2W3	SHA-1	73ec32bc9e15ab2d750ca422796ba056a662db9c
Playbook	No Playbook Applied	MD5	c9b22fcf4e8704833b069d9451d7eaa6
Network Exit	LO - Local - Dirty Network Interface	Tags	
Localization			

Below the metadata, there is a section for 'Behavioral Indicators'.

### What to do next

Once the Threat Grid 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 Threat Grid Appliance Administration Guide](#) for information about administrator tasks.