Cisco Threat Grid Appliance Setup and Configuration Guide Version 2.9

First Published: 2019-12-12

Last Modified: 2019-12-17

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.

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

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

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

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

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

CONTENTS

CHAPTER 1

Introduction

This chapter provide 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

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.

What's New In This Release

The following changes have been implemented in this guide in Version 2.9:

Table 1: Changes in Version 2.9Mfg - December 17, 2019

Feature or Update	Section
No changes.	

Table 2: Changes in Version 2.9 - December 12, 2019

Feature or Update	Section
Threat Grid Shell command for disabling the Admin port.	Threat Grid Shell (tgsh)
Updated Network Interfaces to include ability to disable Admin port in Admin interface.	Network Interfaces
Updated Threat Grid Web portal UI Administrator password	Login Names and Passwords (Default) Test Appliance Setup
Updated Support information.	Threat Grid Support

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.

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 Administrator 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

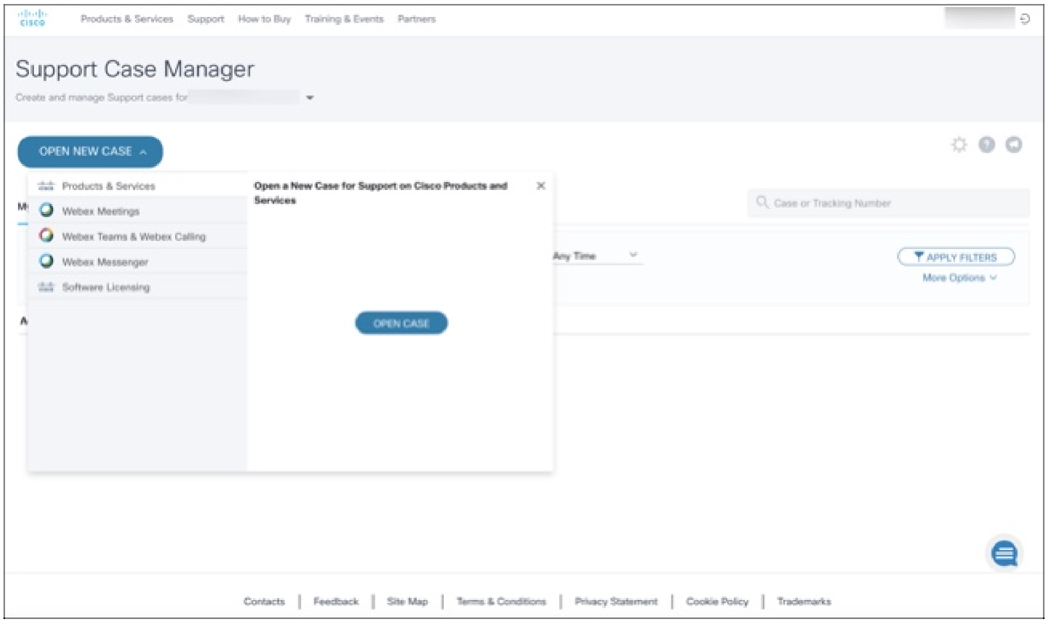
Threat Grid Portal user documentation, including Release Notes, Threat Grid Online Help, API documentation, and other information is available from the **Help** menu located in the navigation bar at the top of the user interface.

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**.

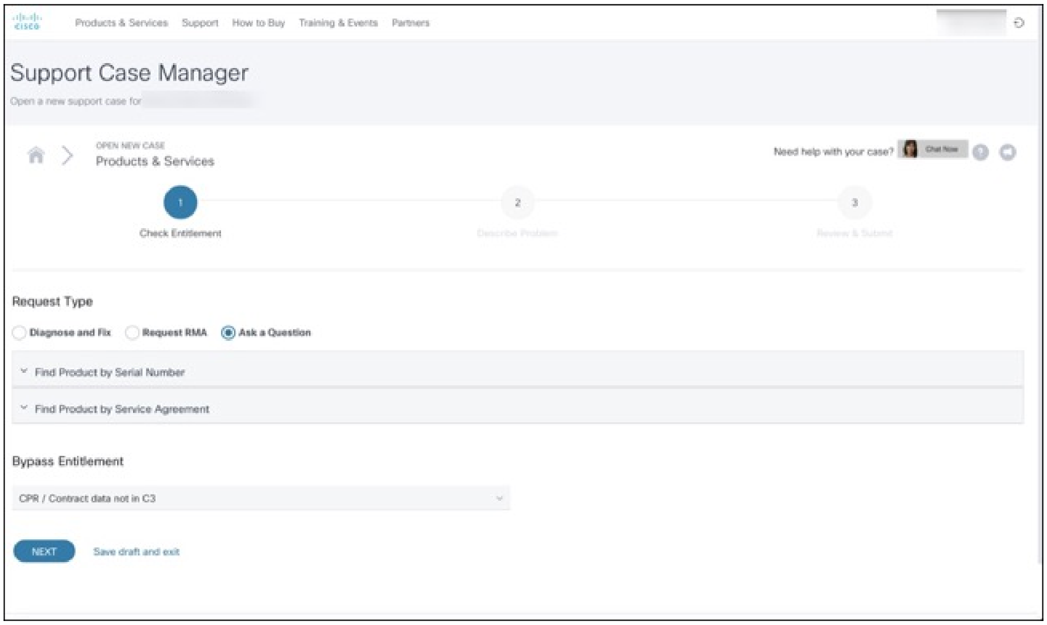
Figure 1: Open New Case



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.

Step 3 If you want to bypass entitlement, choose **Contract Data not in C3** and click **Next**.

Figure 2: Check Entitlement



Support Case Manager

Open a new support case for [redacted]

Request Type

○ Diagnose and Fix ○ Request RMA ● Ask a Question

Find Product by Serial Number
Find Product by Service Agreement

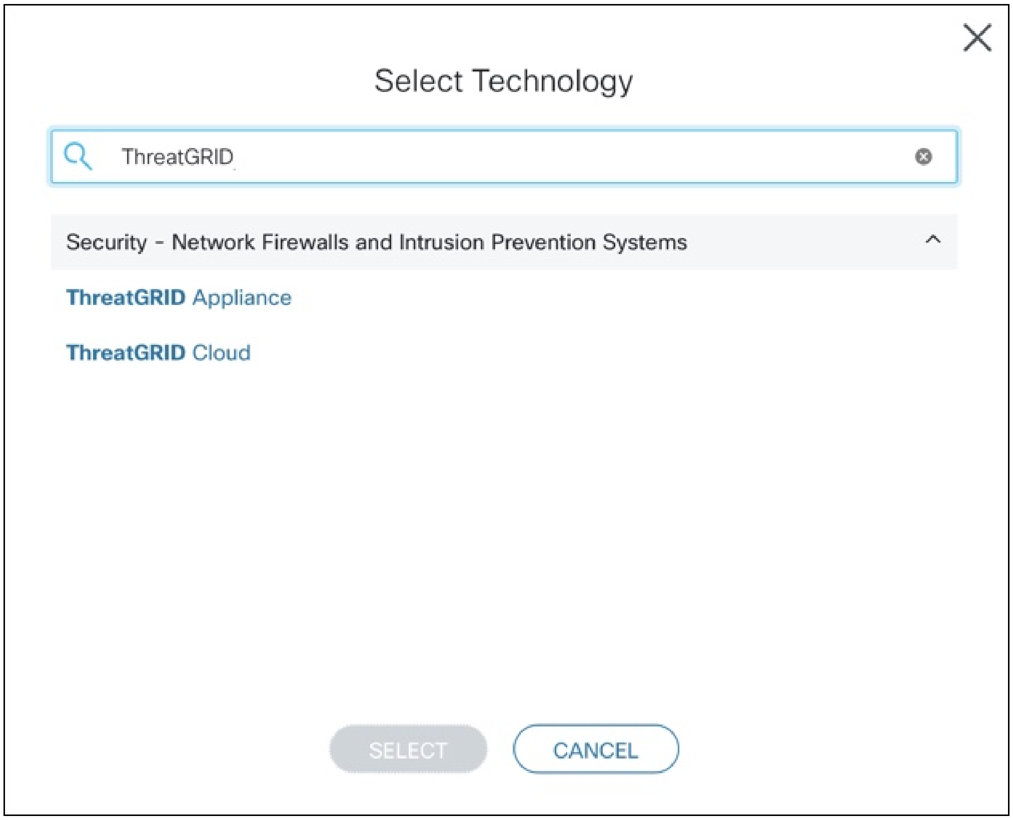
Bypass Entitlement

CPR / Contract data not in C3

Step 4 On the **Describe Problem** page, enter a **Title** and **Description** of the problem (mention Threat Grid in the title).

Step 5 Click **Manually select a Technology** and search for **ThreatGRID**.

Figure 3: Select Technology



Step 6 Choose **ThreatGRID Appliance** from the list and click **Select**.

Step 7 Complete the remainder of the form and click **Submit**.

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

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

For additional information on how to request support:

- See the blog post: **Changes to the Cisco 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

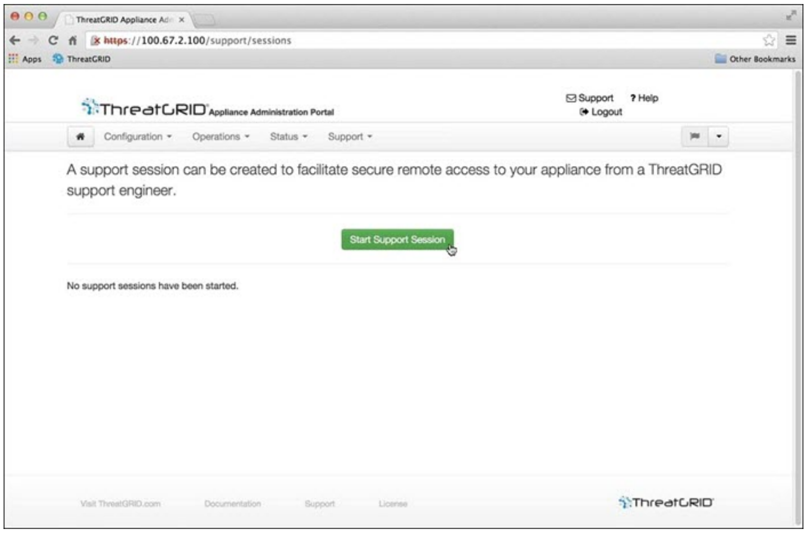
Enable Support Mode

If you require support from a Threat Grid engineer, they may ask you to enable Support Mode, which is a live support session that gives Threat Grid support engineers remote access to the appliance. Normal operations of the appliance will not be affected.

You can enable Support Mode from the OpAdmin portal **Support** menu. You can also enable it from the TGSH Dialog, the legacy Face Portal UI, and when booting up in Recovery Mode.

Step 1 In the OpAdmin portal, click the **Support** menu and choose **Live Support Session**.

Figure 4: OpAdmin Start a Live Support Session



A support session can be created to facilitate secure remote access to your appliance from a ThreatGRID support engineer.

No support sessions have been started.

Step 2 Click **Start Support Session**.

Note You can exit the OpAdmin configuration wizard to enable Support Mode prior to licensing.

Support Snapshots

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

Step 1 Verify that SSH is specified for Support Snapshot services.

Step 2 From the **Support** menu, choose **Support Snapshots**.

Step 3 Take the snapshot.

Step 4 Once you take the snapshot, download it as a **.tar** or **.gz** file, or click **Submit**, to automatically upload the snapshot to the Threat Grid snapshot server.

CHAPTER 2

Planning

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

This chapter includes the following information about the environmental, hardware, and network requirements that should be reviewed prior to configuration:

Supported Browsers

Threat Grid supports the following browsers:

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

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

Environmental Requirements

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

Hardware Requirements

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

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

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

Figure 5: Cisco 1000BASE-T Copper SFP (GLC-T)

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

Note CIMC is not supported on the Threat Grid M5 Appliance server.

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

Network Requirements

The Threat Grid Appliance requires three networks:

- **ADMIN** - The Administrative network must be configured to perform the Threat Grid Appliance setup.

  - OpAdmin Management Traffic (HTTPS)
  - SSH
  - NFSv4 (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.)

- **CLEAN** - The Clean network is used for inbound, trusted traffic to the Threat Grid Appliance (requests), and integrated appliances such as the Cisco Email Security Appliance and Web Security Appliance; integrated applicances connect to the IP address of the Clean interface.

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

  The following specific, restricted types of network traffic can be outbound from the Clean network:

  - Remote syslog connections
  - Email messages sent by the Threat Grid Appliance
  - Disposition Update Service connections to AMP for Endpoints Private Cloud devices
  - DNS requests (related to any of the above)
  - LDAP

- **DIRTY** - The Dirty network is used for outbound traffic from the Threat Grid Appliance (including malware traffic).

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

For network interface setup information, see Network Interfaces.

DNS Server Access

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

By default, DNS uses the Dirty interface. The Clean interface is used for AMP for Endpoints Private Cloud integrations. If the AMP for Endpoints Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the OpAdmin interface.

See the Cisco Threat Grid Appliance Administrator Guide for additional information.

NTP Server Access

The NTP server needs to be accessible via the Dirty network.

Integrations

Additional planning may be required if the Threat Grid Appliance is going to be used with other Cisco products, such as the Email Security Appliance, Web Security Appliance, or AMP for Endpoints Private Cloud. See the *Cisco Threat Grid Appliance Administrator Guide* for more information.

DHCP

If you are connected to a network configured to use DHCP, follow the instructions provided in the Using DHCP section of the *Cisco Threat Grid Appliance Administrator Guide*.

License

You will receive a license and password from Cisco Threat Grid.

For questions about licenses, contact Threat Grid Support.

Rate Limits

The API rate limit is global for the Threat Grid Appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions.

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

Organization and Users

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

See the Create New Organization section in the *Cisco Threat Grid Appliance Administrator Guide*. See the Threat Grid portal Help for information about managing users.

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.

User Interfaces

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

Note LDAP authentication is available for TGSH Dialog and OpAdmin (v2.1.6 and later).

TGSH Dialog

The **TGSH Dialog** interface is used to configure the network interfaces. The TGSH Dialog is displayed when the Threat Grid Appliance successfully boots up.

Reconnecting to the TGSH Dialog

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

Note CIMC is not supported on the Threat Grid M5 Appliance server.

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

The required password is either the initial, randomly generated password, which is visible initially in the TGSH Dialog, or the new Admin password you create during the first step of the OpAdmin Portal Configuration.

Threat Grid Shell (tgsh)

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

Note OpAdmin uses the same credentials as the Threat Grid user, so any password changes/updates made via tgsh will also impact OpAdmin.

Caution Network configuration changes made with tgsh are not supported unless specifically directed by Threat Grid support; OpAdmin or TGSH Dialog should be used instead.

OpAdmin Portal

This is the primary Threat Grid GUI configuration tool. Much of the Threat Grid Appliance configuration can ONLY be done via OpAdmin, including licenses, email host, and SSL certificates.

Threat Grid Portal

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

Network Interfaces

The available network interfaces are described in the following table:

Interface	Description
Admin	• Connect to the Admin network. **Only inbound** from Admin network. • OpAdmin UI traffic • SSH (inbound) for TGSH Dialog • NFSv4 for backups and clustering (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.) Must be accessible from all cluster notes. • The Admin port can be disabled (from the tgsh shell). When disabled, non-clustered Threat Grid Appliances can operate correctly with only the clean and dirty ports connected, and the admin UI will be presented on port 8443 of the clean interface. If the port is not disabled, unplugging the admin port results in a non-functional (or at best, a partially-functional) Threat Grid Appliance. **Note** The form factor for the Admin interface is SFP+. See Hardware Requirements.

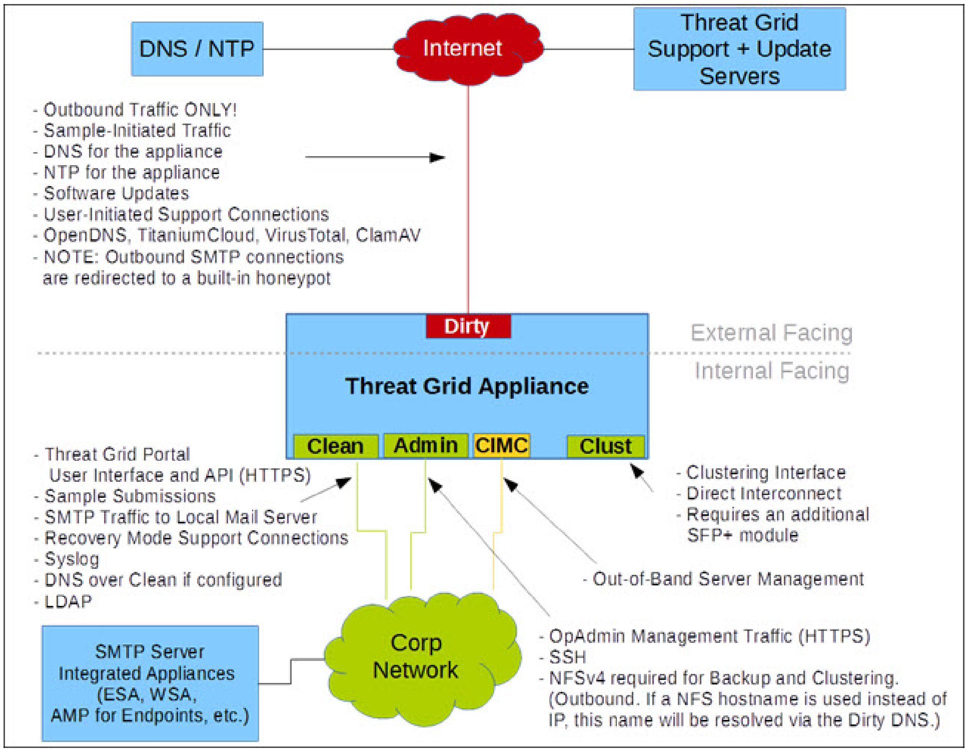
Interface	Description
Clust	The non-Admin SFP+ port is used for clustering. • Clust interface required for clustering (optional) • Requires an additional SFP+ module for direct interconnect. This interface does not require any configuration. Addresses are automatically assigned.
Clean	• Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet. • UI and API traffic (inbound) • Sample submissions • SMTP (outbound connection to the configured mail server) • SSH (inbound for TGSH Dialog) • Syslog (outbound to configured syslog server) • ESA/WSA and CSA Integrations • AMP for Endpoints Private Cloud Integration • DNS optional • LDAP (outbound)

Interface	Description
Dirty	Connect to the Dirty network; requires Internet access. Outbound Only. You should not use your own DNS (private IP) for the Dirty Interface because traffic sent to a private IP is dropped at the Network Exit Localization firewall. • DNS **Note** If you are setting up an integration with a AMP for Endpoints Private Cloud, and the AMP for Endpoints appliance hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in OpAdmin. • NTP • Updates • Support session in Normal operations mode • Support snapshots • Malware sample-initiated traffic • Recovery mode support session (outbound) • OpenDNS, TitaniumCloud, VirusTotal, ClamAV • SMTP outbound connections are redirected to a built-in honeypot **Note** Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.
CIMC Interface	Recommended. If the Cisco Integrated Management Controller (CIMC) interface is configured, it can be used for server management and maintenance. For more information see the *Cisco Threat Grid Appliance Administrator Guide*. **Note** CIMC is not supported on the Threat Grid M5 Appliance server.

Network Interface Setup Diagram

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

Figure 6: Network Interfaces Setup Diagram


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

Note In Threat Grid Appliance (v2.7.2 and later), the **enable_clean_interface**option is available but is disabled by default. This option (after applying configuration and rebooting) enables access to the administrative interface on port 8443 of the assigned clean IP.

Firewall Rules

This section provides suggested firewall rules.

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

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

Dirty Interface Outbout

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

Dirty Interface Inbound

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

Clean Interface Outbound

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

Clean Interface Outbound (Optional)

Source	Destination	Protocol	Port	Action	Note
Clean Interface	Corporate DNS Server	TCP/UDP	53	Allow	Optional, only required if Clean DNS is configured.
Clean Interface	AMP Private Cloud	TCP	443	Allow	Optional, only required if AMP for Endpoints Private Cloud integration is used.
Clean Interface	Syslog Servers	UDP	514	Allow	Allow connectivity to server designated to receive Syslog messages and Threat Grid notifications.
Clean Interface	LDAP Servers	TCP/UDP	389	Allow	Optional, only required if LDAP is configured.
Clean Interface	LDAP Servers	TCP	636	Allow	Optional, only required if LDAP is configured.

Clean Interface Inbound

Source	Destination	Protocol	Port	Action	Note
User Subnet	Clean Interface	TCP	22	Allow	Allow SSH conectivity to the TGSH Dialog.
User Subnet	Clean Interface	TCP	80	Allow	Appliance API and Threat Grid user interface. This will redirect to HTTPS TCP/443.
User Subnet	Clean Interface	TCP	443	Allow	Appliance API and Threat Grid user interface.
User Subnet	Clean Interface	TCP	9443	Allow	Allow connectivity to the Threat Grid UI Glovebox.

Admin Interface Outbound (Optional)

The following depends on what services are configured.

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

Admin Interface Inbound

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	22	Allow	Allow SSH connectivity to the TGSH Dialog.
Admin Subnet	Admin Interface	TCP	80	Allow	Allow access to the OpAdmin Portal interface. This will redirect to HTTPS TCP/443.
Admin Subnet	Admin Interface	TCP	443	Allow	Allow access to the OpAdmin Portal interface.

Dirty Interface for Non Cisco-Validated/Recommended Deployment

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	22	Allow	Update, support snapshot, and licensing services.
Dirty Interface	Internet	TCP/UDP	53	Allow	Allow outbound DNS.
Dirty Interface	Internet	UDP	123	Allow	Allow outbound NTP.

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	19791	Allow	Allow connectivity to Threat Grid support.
Dirty Interface	Cisco Umbrella	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	VirusTotal	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	TitaniumCloud	TCP	443	Allow	Connect with third-party detection and enrichment services.

Login Names and Passwords (Default)

The default login names and passwords are listed in the following table:

User	Login/Password
OpAdmin and Shell User	Use the initial Threat Grid/TGSH Dialog randomly generated password, and then the new password entered during the first step of the OpAdmin configuration workflow. If you lose the password, see the Reset Administrator Password section in the of the *Cisco Threat Grid Appliance Administrator Guide*.
Threat Grid Web portal UI Administrator	Login: **admin** Password: Initialize with the first OpAdmin password, and then it becomes independent.
CIMC	Login: **admin** Password: **password**

Setup and Configuration Overview

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

- Initial Network Configuration
- OpAdmin Portal Configuration
- Installing Updates
- Testing Appliance Setup

Complete the remaining administrative configuration tasks (such as license installation, email server, and SSL certificates) in the OpAdmin Portal as documented in the *Cisco Threat Grid Appliance Administrator Guide*.

You should allow approximately 1 hour to complete the initial configuration steps.

CHAPTER 3

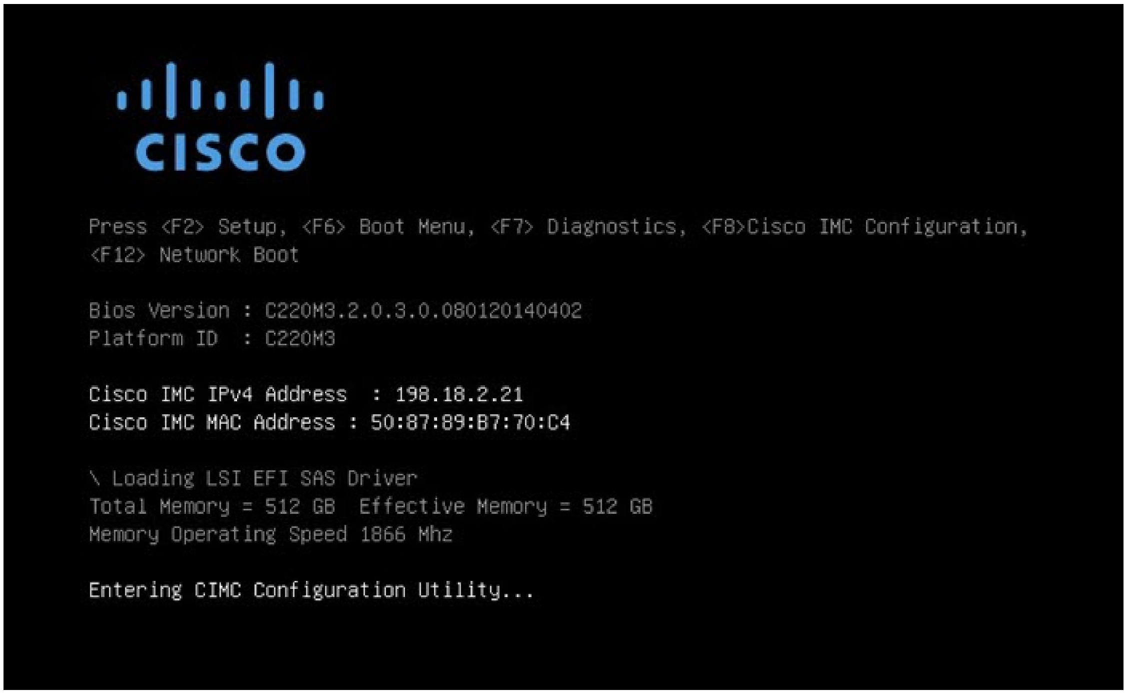
Initial Network Configuration

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

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 7: Cisco Screen During Bootup

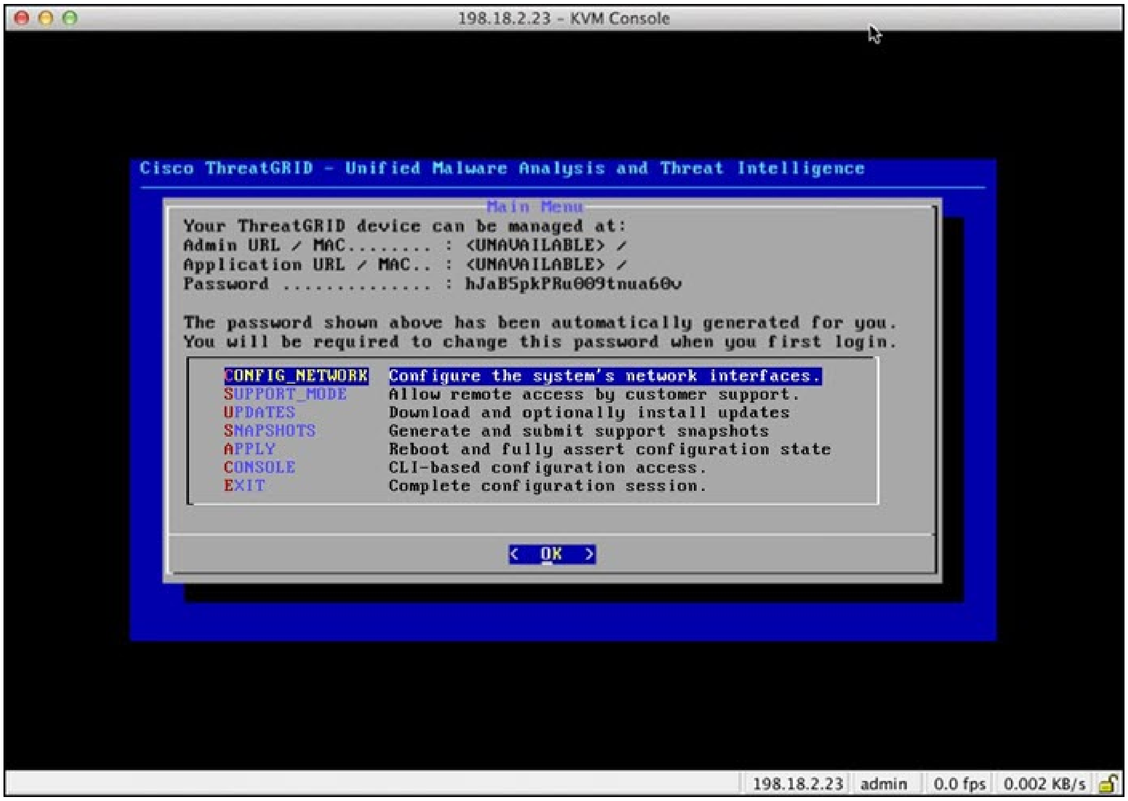


```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

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...
```

Note If you want to configure this interface, press **F8** after the memory check is completed. See the CICM Configuration appendix in the *Cisco Threat Grid Appliance Administrator Guide*.

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

Figure 8: TGSH Dialog



```
Cisco ThreatGRID - Unified Malware Analysis and Threat Intelligence

                          Main Menu
 Your ThreatGRID device can be managed at:
 Admin URL / MAC........ : <UNAVAILABLE> /
 Application URL / MAC.. : <UNAVAILABLE> /
 Password .............. : hJaB5pkPRu009tnua60v

 The password shown above has been automatically generated for you.
 You will be required to change this password when you first login.

     CONFIG_NETWORK    Configure the system's network interfaces.
     SUPPORT_MODE      Allow remote access by customer support.
     UPDATES           Download and optionally install updates
     SNAPSHOTS         Generate and submit support snapshots
     APPLY             Reboot and fully assert configuration state
     CONSOLE           CLI-based configuration access.
     EXIT              Complete configuration session.

                          <  OK  >
```

The Admin URL shows as unavailable because the network interface connections are not yet configured and the OpAdmin Portal 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 OpAdmin Portal interface later in the configuration. Make a note of the Password in a separate text file (copy and paste).

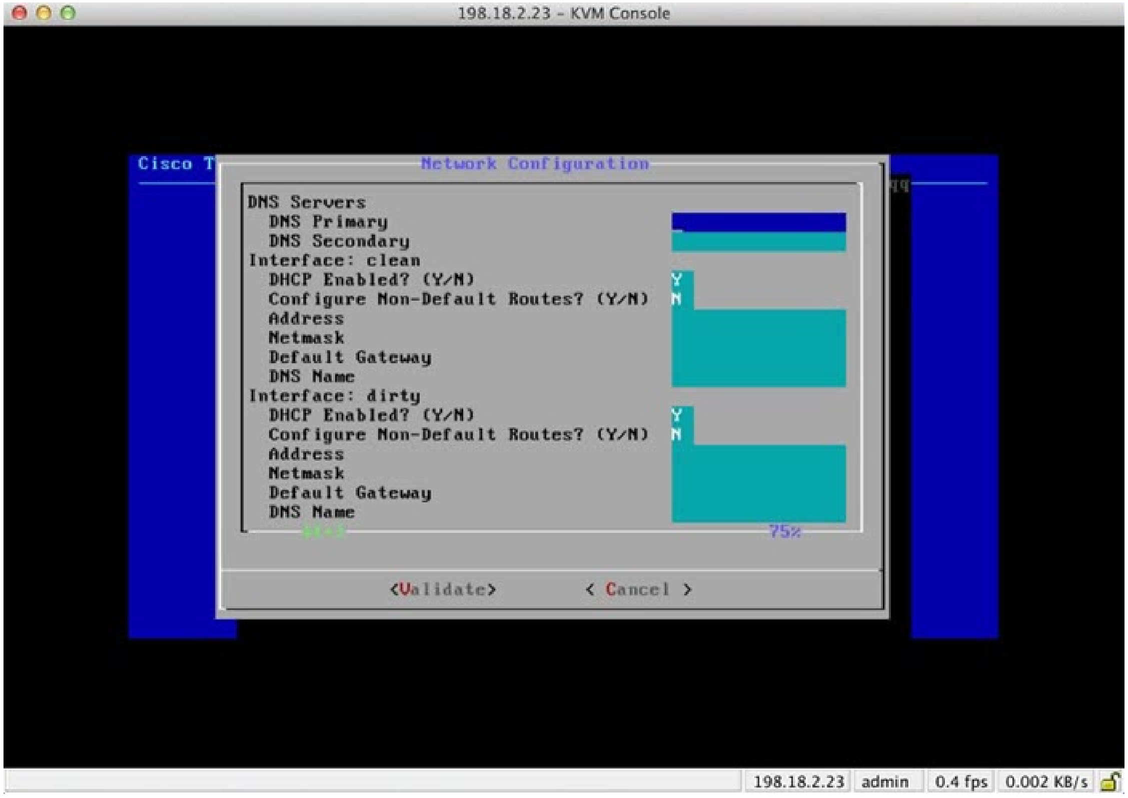
Configure Network Using TGSH Dialog

The initial network configuration is completed in the TGSH Dialog. The basic configuration, once completed, allows access to the OpAdmin portal, 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 Administrator Guide*.

Step 1 On the TGSH Dialog, select **CONFIG_NETWORK**. The **Network Configuration** console opens.

Figure 9: TGSH Dialog - Network Configuration Console



```
                    Network Configuration
DNS Servers
  DNS Primary
  DNS Secondary
Interface: clean
  DHCP Enabled? (Y/N)                          Y
  Configure Non-Default Routes? (Y/N)          N
  Address
  Netmask
  Default Gateway
  DNS Name
Interface: dirty
  DHCP Enabled? (Y/N)                          Y
  Configure Non-Default Routes? (Y/N)          N
  Address
  Netmask
  Default Gateway
  DNS Name
                                              75%

          <Validate>          < Cancel >
```

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**.

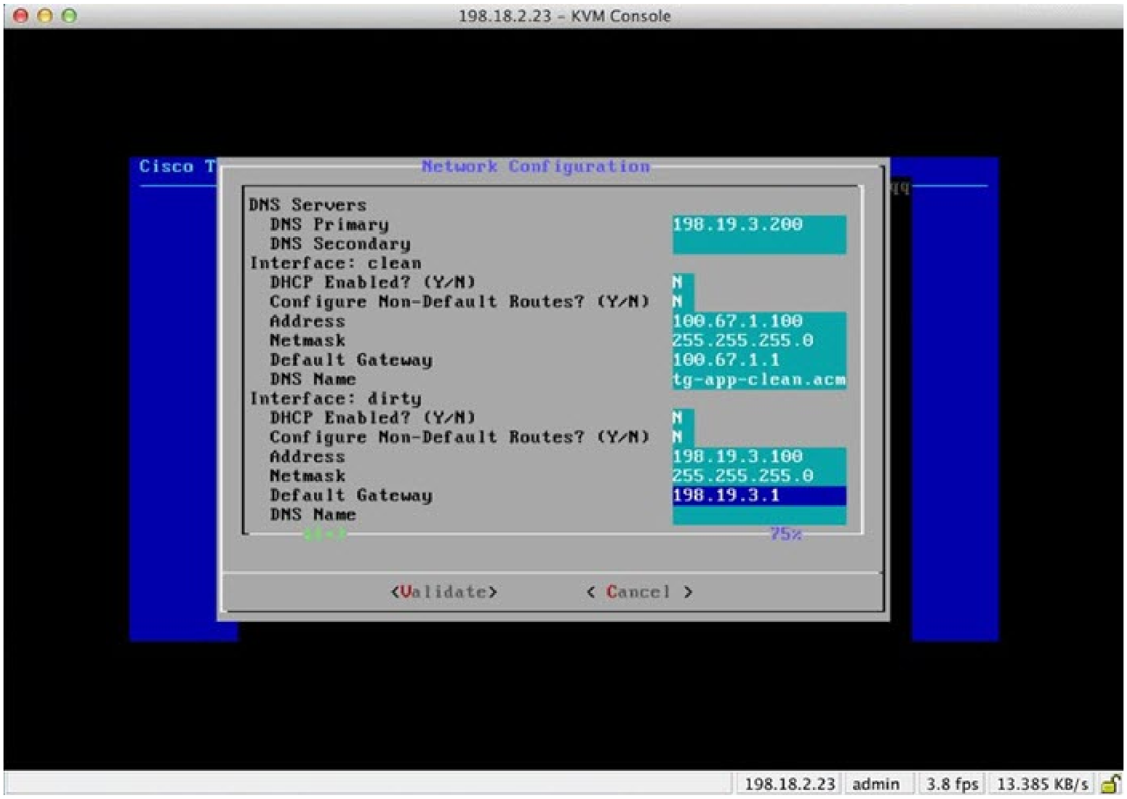
Note You need to backspace over the old character before you can enter the new one.

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.

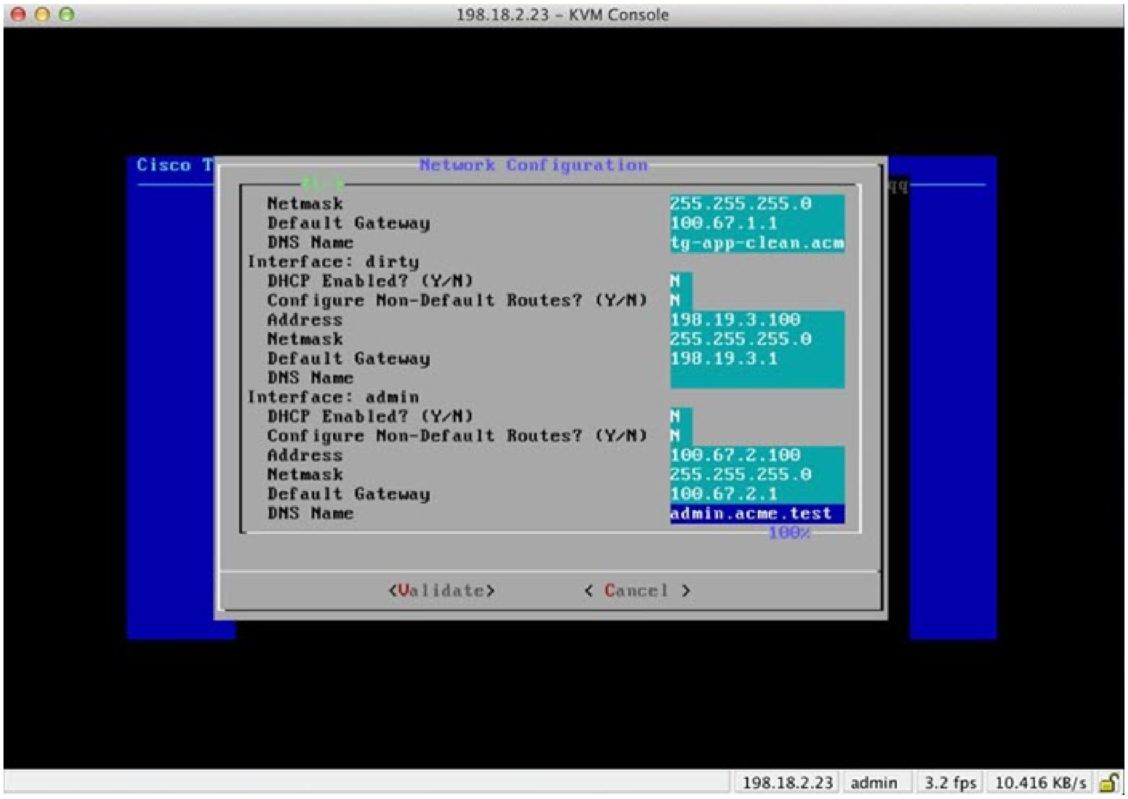
Step 6 Leave the Dirty network **DNS Name** field blank.

Figure 10: Network Configuration In-Progress (Clean and Dirty)



```
                     Network Configuration
DNS Servers
  DNS Primary                              198.19.3.200
  DNS Secondary
Interface: clean
  DHCP Enabled? (Y/N)                      N
  Configure Non-Default Routes? (Y/N)      N
  Address                                  100.67.1.100
  Netmask                                  255.255.255.0
  Default Gateway                          100.67.1.1
  DNS Name                                 tg-app-clean.acm
Interface: dirty
  DHCP Enabled? (Y/N)                      N
  Configure Non-Default Routes? (Y/N)      N
  Address                                  198.19.3.100
  Netmask                                  255.255.255.0
  Default Gateway                          198.19.3.1
  DNS Name
      ↓(+)                                          75%

              <Validate>          < Cancel >
```

Figure 11: Network Configuration In-Progress (Admin)



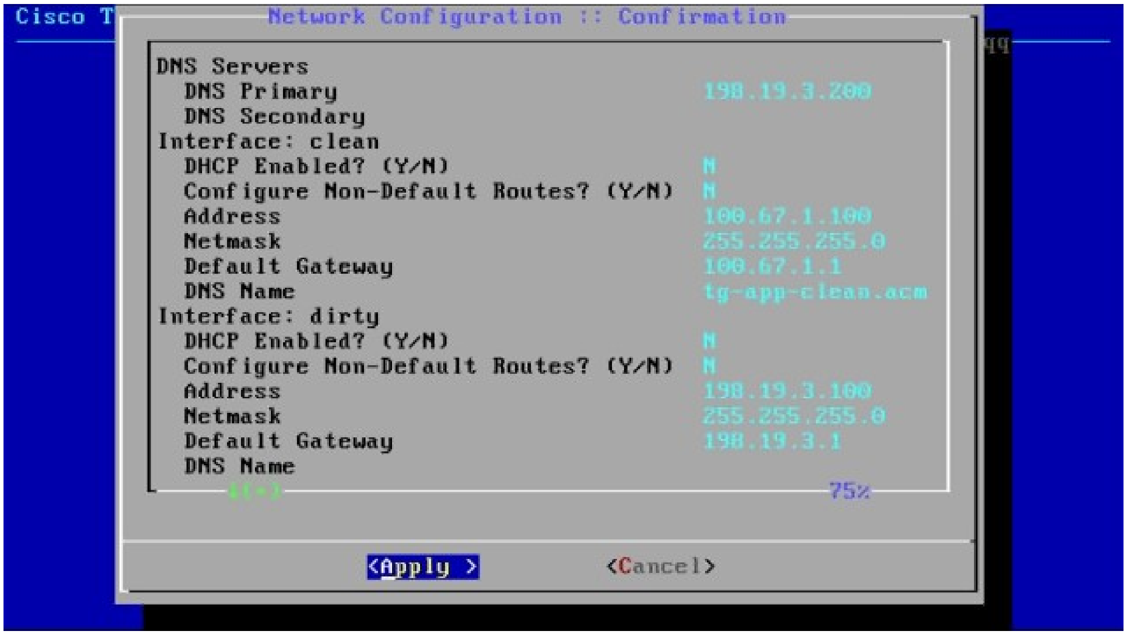
```
  Netmask                                 255.255.255.0
  Default Gateway                         100.67.1.1
  DNS Name                                tg-app-clean.acm
Interface: dirty
  DHCP Enabled? (Y/N)                     N
  Configure Non-Default Routes? (Y/N)     N
  Address                                 198.19.3.100
  Netmask                                 255.255.255.0
  Default Gateway                         198.19.3.1
  DNS Name
Interface: admin
  DHCP Enabled? (Y/N)                     N
  Configure Non-Default Routes? (Y/N)     N
  Address                                 100.67.2.100
  Netmask                                 255.255.255.0
  Default Gateway                         100.67.2.1
  DNS Name                                admin.acme.test
```

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 12: Network Configuration Confirmation

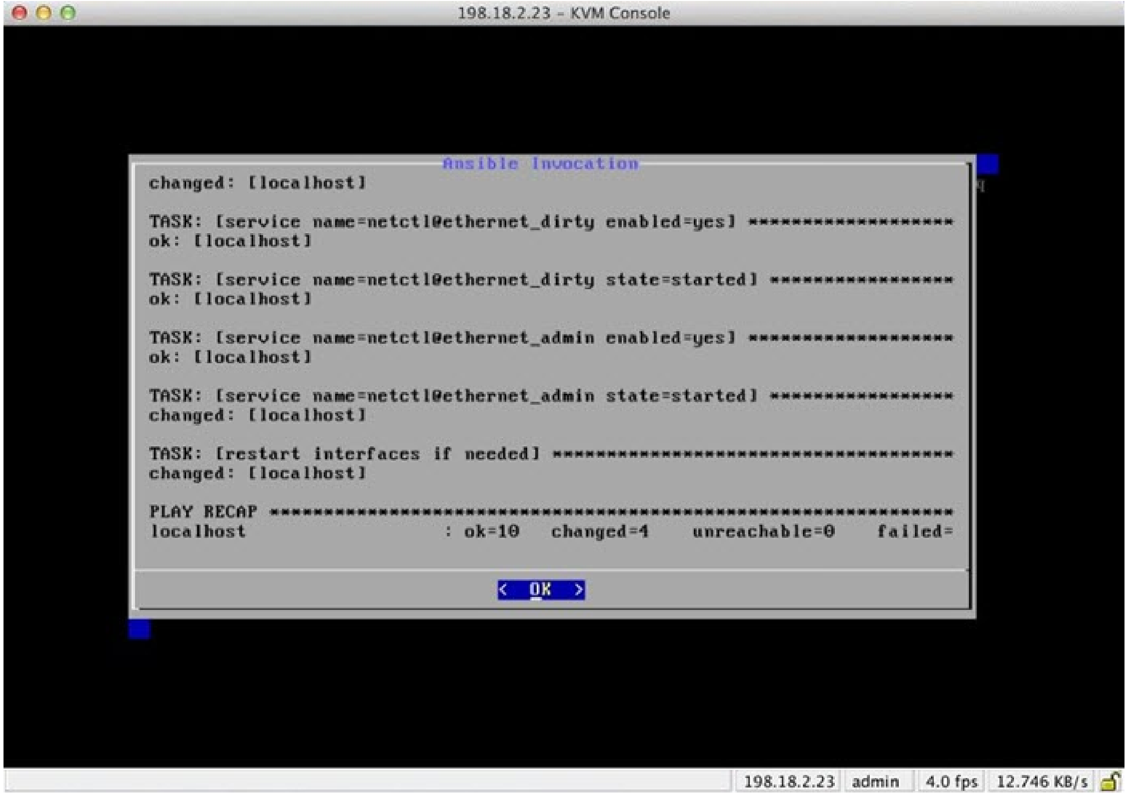


```
Cisco T     Network Configuration :: Confirmation
 DNS Servers
   DNS Primary                               198.19.3.200
   DNS Secondary
 Interface: clean
   DHCP Enabled? (Y/N)                       N
   Configure Non-Default Routes? (Y/N)       N
   Address                                   100.67.1.100
   Netmask                                   255.255.255.0
   Default Gateway                           100.67.1.1
   DNS Name                                  tg-app-clean.acm
 Interface: dirty
   DHCP Enabled? (Y/N)                       N
   Configure Non-Default Routes? (Y/N)       N
   Address                                   198.19.3.100
   Netmask                                   255.255.255.0
   Default Gateway                           198.19.3.1
   DNS Name
      ↓(+)                                              75%

              <Apply >           <Cancel>
```

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 13: Network Configuration - List of Changes Made



198.18.2.23 - KVM Console

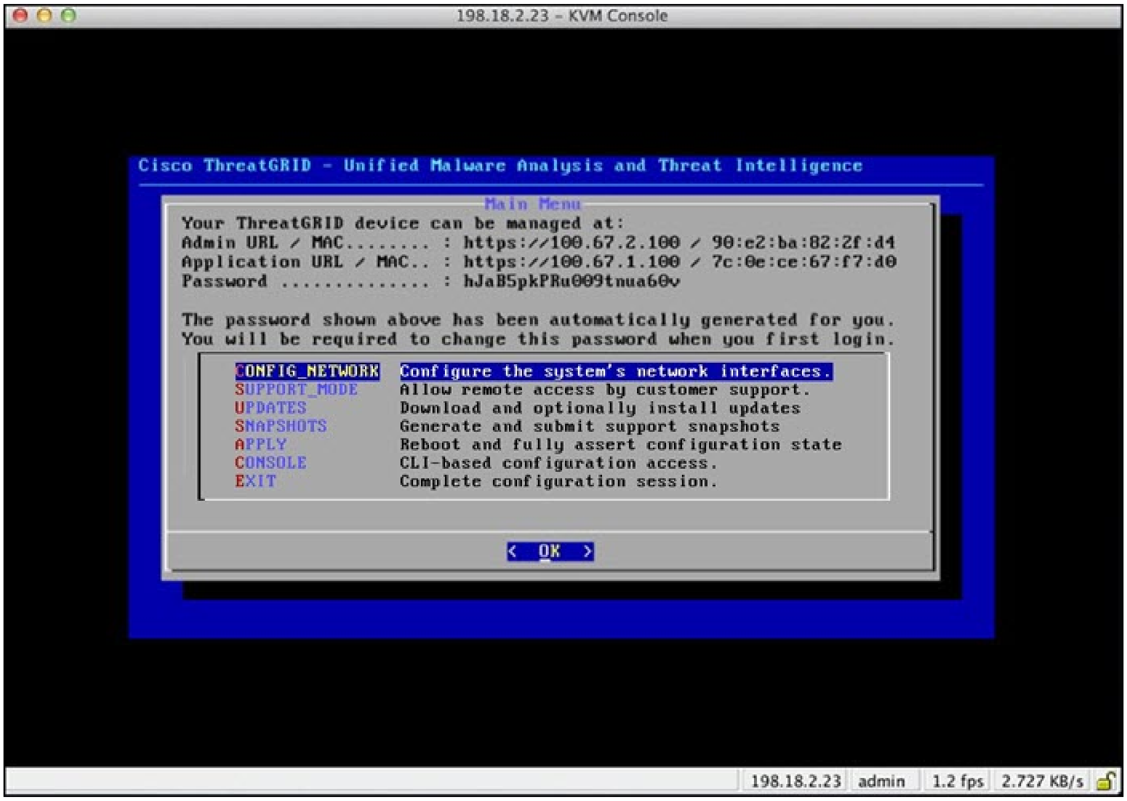
Ansible Invocation

```
changed: [localhost]

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=
```

Step 9 Select **OK**.

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

Figure 14: IP Addresses



```
Cisco ThreatGRID - Unified Malware Analysis and Threat Intelligence

                              Main Menu
Your ThreatGRID device can be managed at:
Admin URL / MAC........ : https://100.67.2.100 / 90:e2:ba:82:2f:d4
Application URL / MAC.. : https://100.67.1.100 / 7c:0e:ce:67:f7:d0
Password .............. : hJaB5pkPRu009tnua60v

The password shown above has been automatically generated for you.
You will be required to change this password when you first login.

    CONFIG_NETWORK   Configure the system's network interfaces.
    SUPPORT_MODE     Allow remote access by customer support.
    UPDATES          Download and optionally install updates
    SNAPSHOTS        Generate and submit support snapshots
    APPLY            Reboot and fully assert configuration state
    CONSOLE          CLI-based configuration access.
    EXIT             Complete configuration session.

                              < OK >
```

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

Note The URL for the Clean interface is not active until the OpAdmin portal 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 OpAdmin Portal, as described in OpAdmin Portal Configuration.

CHAPTER 4

OpAdmin Portal Configuration

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

Introduction

The OpAdmin Portal is the Threat Grid administrator's portal on the appliance and is the recommended tool for configuring your 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 OpAdmin Admin Password
- Review End User License Agreement
- Review Network Configuration Settings (not configured using wizard)
- Install License
- Configure NFS
- Configure Email Host
- Configure Notifications
- Configure Date and Time (NTP Server)
- Configure SysLog
- Review and Install Configuration Settings

Note Not all configuration steps are completed using the configuration wizard. See the *Cisco Threat Grid Appliance Administrator 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.

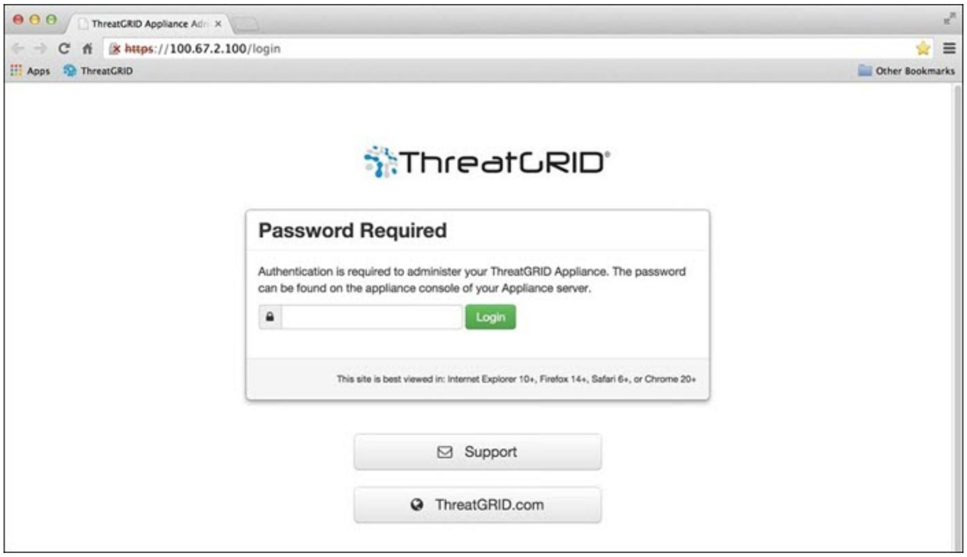
Log In to OpAdmin Portal

Perform the following steps to log in to the Threat Grid OpAdmin portal.

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

Note The Hostname is the appliance serial number (v2.7 or later).

Figure 15: OpAdmin Login Screen



Password Required

Authentication is required to administer your ThreatGRID Appliance. The password can be found on the appliance console of your Appliance server.

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

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

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 TGSH Dialog. You must change the initial Admin password before continuing with the configuration.

Step 1 Enter the password from the TGSH Dialog in the **Old Password** field. (You should have this saved in a text file.)

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

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

Note The new password will not be displayed in visible text in the TGSH 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 TGSH Dialog, the IP addresses displayed on the **Network** page reflect the values you entered in the TGSH Dialog during the Threat Grid Appliance network configuration.

Step 1 Review the IP addreses 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 Administrator Guide.

What to do next

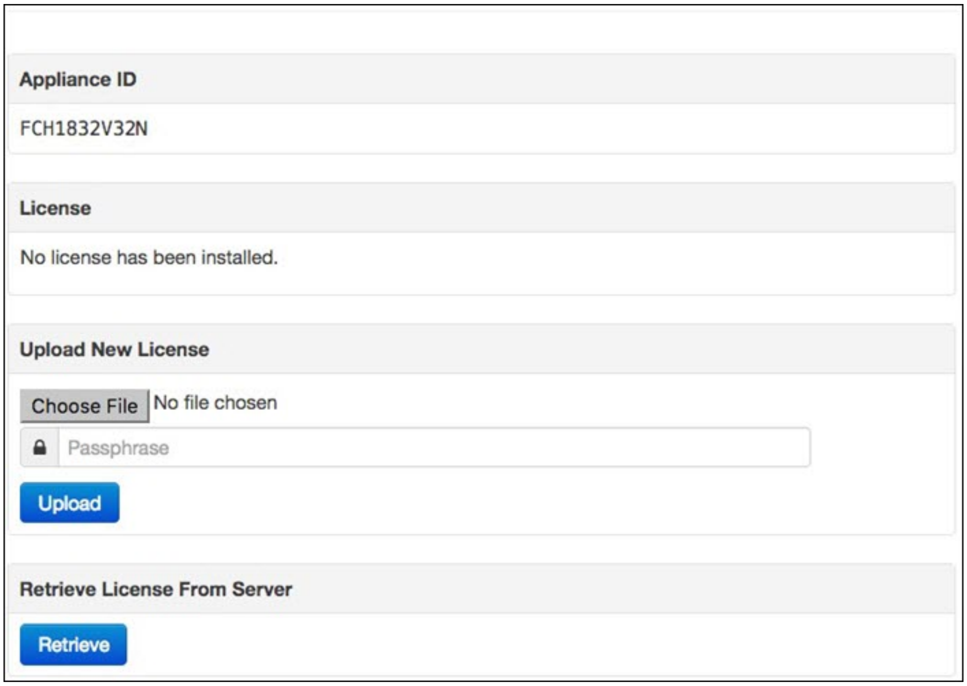
Proceed to Install License.

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 16: License Page Prior to Installation



Appliance ID

FCH1832V32N

License

No license has been installed.

Upload New License

No file chosen

Retrieve License From Server

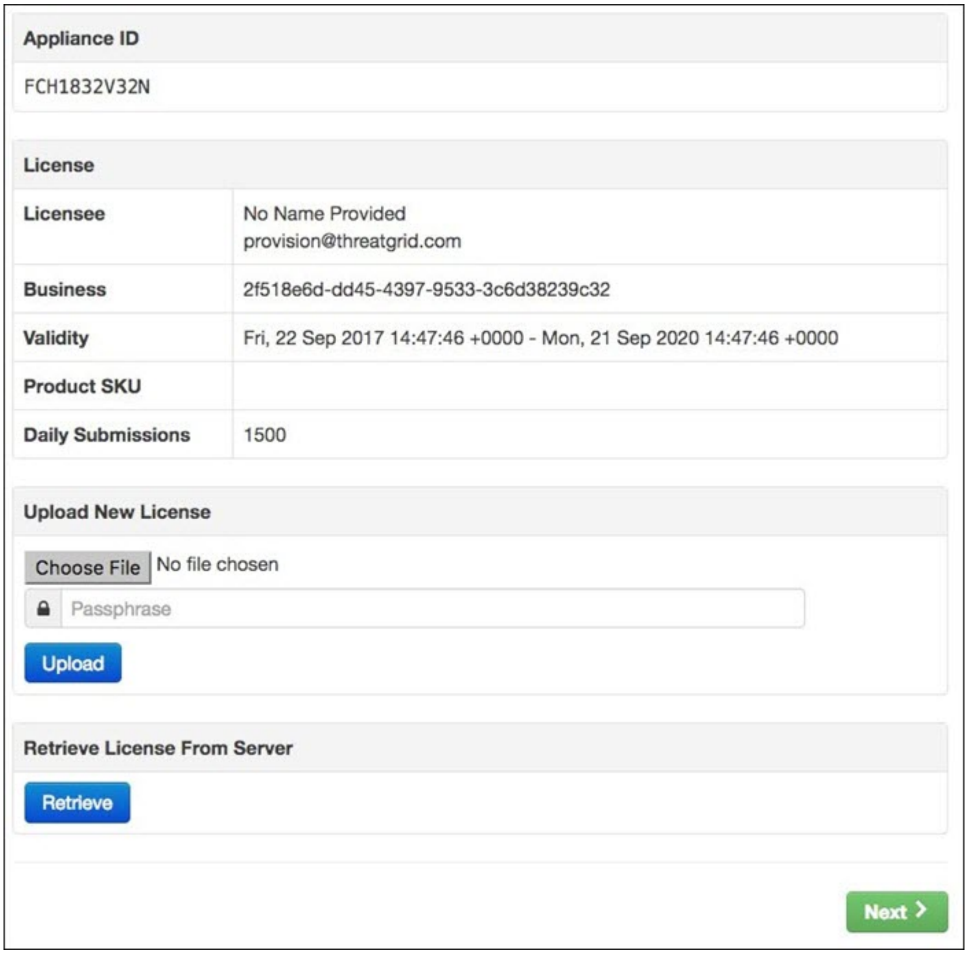
Step 2 In the **Upload New License** pane, click **Choose File** and select the license from your file manager.

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

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

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

Figure 17: License Information After Successful Installation



Appliance ID

FCH1832V32N

License	
Licensee	No Name Provided provision@threatgrid.com
Business	2f518e6d-dd45-4397-9533-3c6d38239c32
Validity	Fri, 22 Sep 2017 14:47:46 +0000 - Mon, 21 Sep 2020 14:47:46 +0000
Product SKU	
Daily Submissions	1500

Upload New License

Choose File No file chosen

Step 5 Click **Next** to continue.

What to do next

Proceed to Configure NFS.

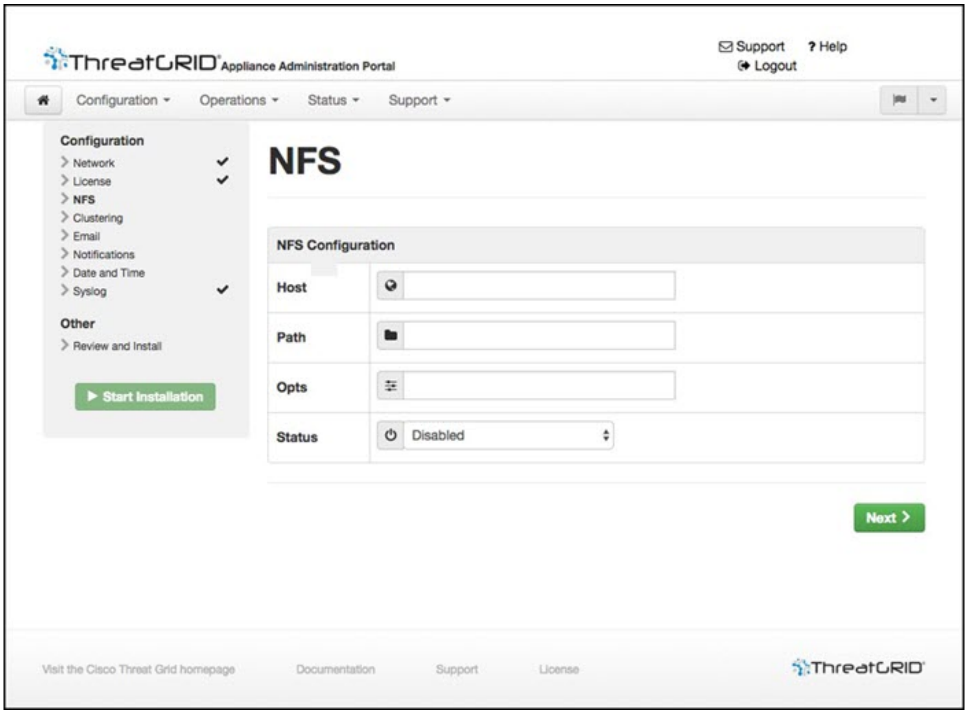
Configure NFS

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 Administrator Guide* for more information.

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

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

Figure 18: NFS Configuration



NFS Configuration

Host

Path

Opts

Status: Disabled

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.
- **Opts** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.
- **Status** - Choose **Enabled** from the drop-down list (Pending Key).

Step 3 Click **Next**. The page refreshes and a **FS Encryption Password Key ID** is displayed.

The first time you configure this page, options to **Remove** 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 OpAdmin after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key.

Step 4 Click **Next** to continue.

What to do next

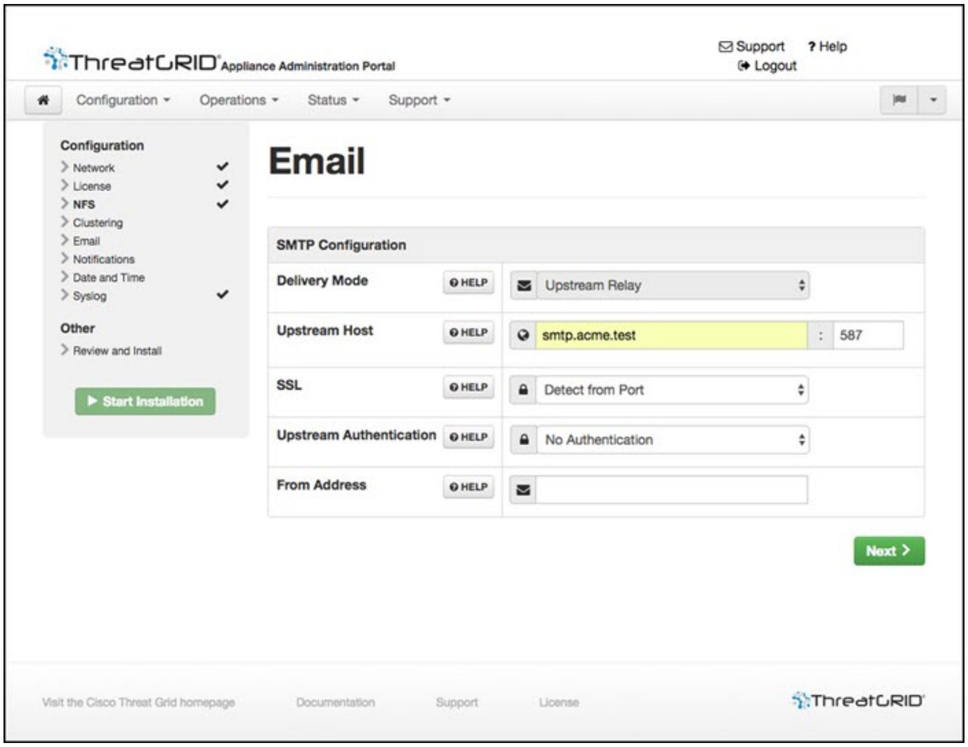
Proceed to Configure Email Host.

Configure Email Host

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

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

Figure 19: Email Configuration



Email

SMTP Configuration

Delivery Mode	Upstream Relay
Upstream Host	smtp.acme.test : 587
SSL	Detect from Port
Upstream Authentication	No Authentication
From Address	

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 **Next** to continue.

What to do next

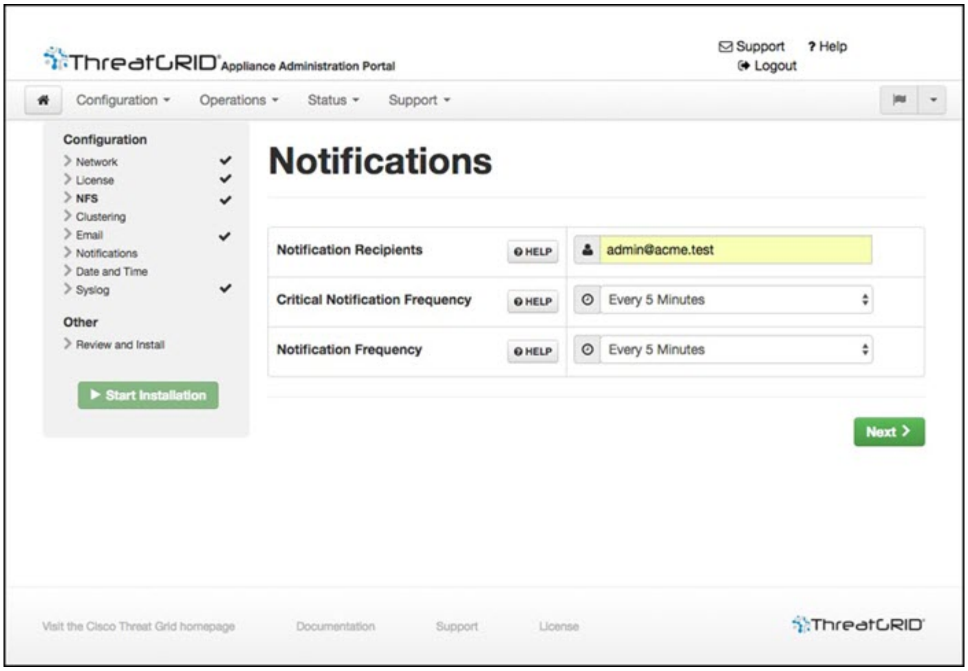
Proceed to Configure Notifications.

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 Configuration



Notifications

Notification Recipients	admin@acme.test
Critical Notification Frequency	Every 5 Minutes
Notification Frequency	Every 5 Minutes

Step 2 In the **Notification Recipients** field, enter one or more email addresses separated by commas.

Step 3 Choose the **Critical Notification Frequency** and the **Notification Frequency** from the drop-down lists.

Step 4 Click **Next** to continue.

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.

Step 2 Enter the **NTP Server(s)** IP or NTP name.

If there are multiple NTP servers, separate them with a space or comma.

Step 3 Ignore the **Current System Time** and **Synchronize with Browser** fields.

Step 4 Click **Next** to continue.

What to do next

Proceed to Configure Syslog.

Configure Syslog

The **Syslog** page is used to configure a Syslog server to receive syslog messages and Thread Grid notifications.

Step 1 Click **Syslog** in the navigation pane.

Step 2 Complete the information on page and click **Next** to continue.

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

What to do next

Proceed to Review and Install Configuration Settings.

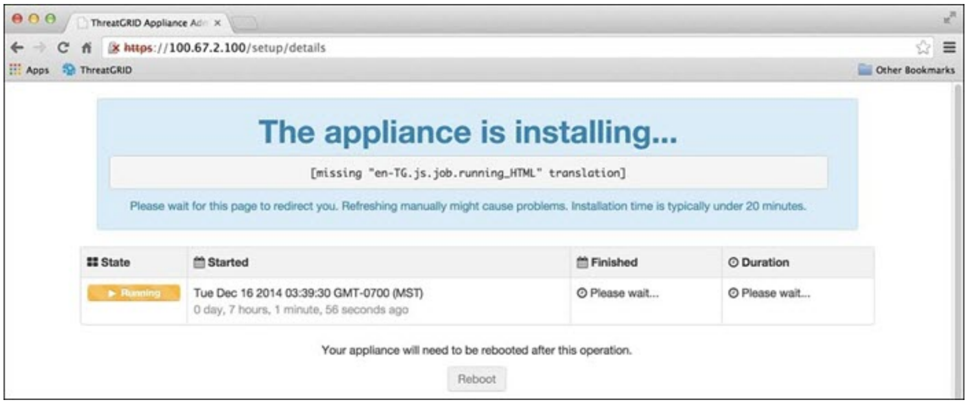
Review and Install Configuration Settings

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 21: Appliance Is Installing



The appliance is installing...

[missing "en-TG.js.job.running_HTML" translation]

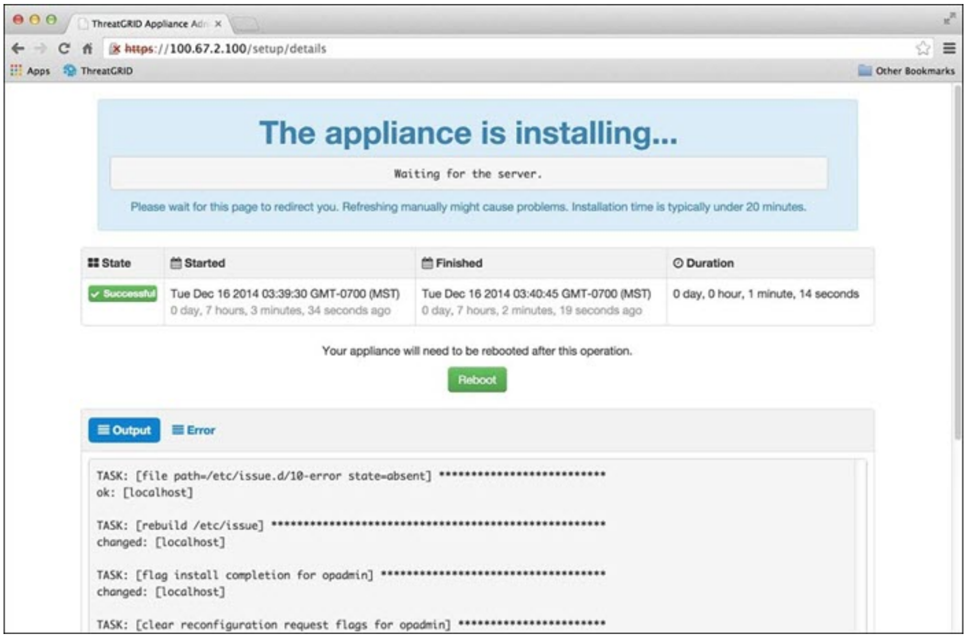
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Tue Dec 16 2014 03:39:30 GMT-0700 (MST) 0 day, 7 hours, 1 minute, 56 seconds ago	Please wait...	Please wait...

Your appliance will need to be rebooted after this operation.

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

Figure 22: Successful Appliance Installation


ThreatGRID Appliance Adm ×
https://100.67.2.100/setup/details
Apps
ThreatGRID
Other Bookmarks

The appliance is installing...

Waiting for the server.

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Tue Dec 16 2014 03:39:30 GMT-0700 (MST) 0 day, 7 hours, 3 minutes, 34 seconds ago	Tue Dec 16 2014 03:40:45 GMT-0700 (MST) 0 day, 7 hours, 2 minutes, 19 seconds ago	0 day, 0 hour, 1 minute, 14 seconds

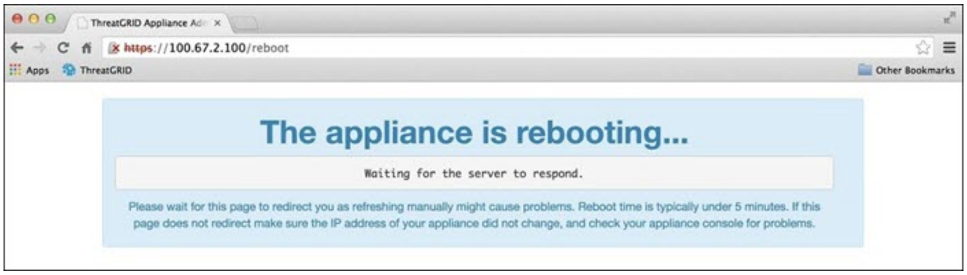
Your appliance will need to be rebooted after this operation.

```
TASK: [file path=/etc/issue.d/10-error state=absent] **************************
ok: [localhost]

TASK: [rebuild /etc/issue] ******************************************************
changed: [localhost]

TASK: [flag install completion for opadmin] ************************************
changed: [localhost]

TASK: [clear reconfiguration request flags for opadmin] ************************
```

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 23: Appliance Is Rebooting



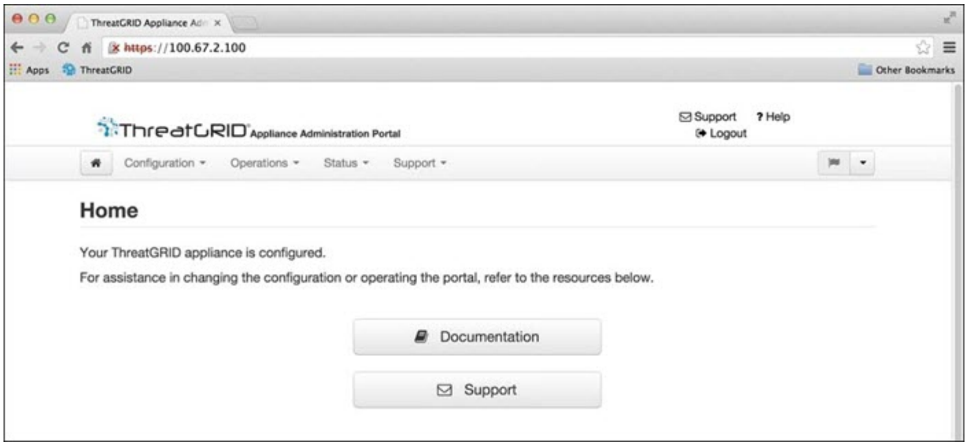
The appliance is rebooting...

Waiting for the server to respond.

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, a message is displayed on the **Home** page indicating that the Threat Grid Appliance is configured.

Figure 24: Appliance Successfully Configured



Home

Your ThreatGRID appliance is configured.

For assistance in changing the configuration or operating the portal, refer to the resources below.

This completes the configuration process.

Install Threat Grid Appliance Updates

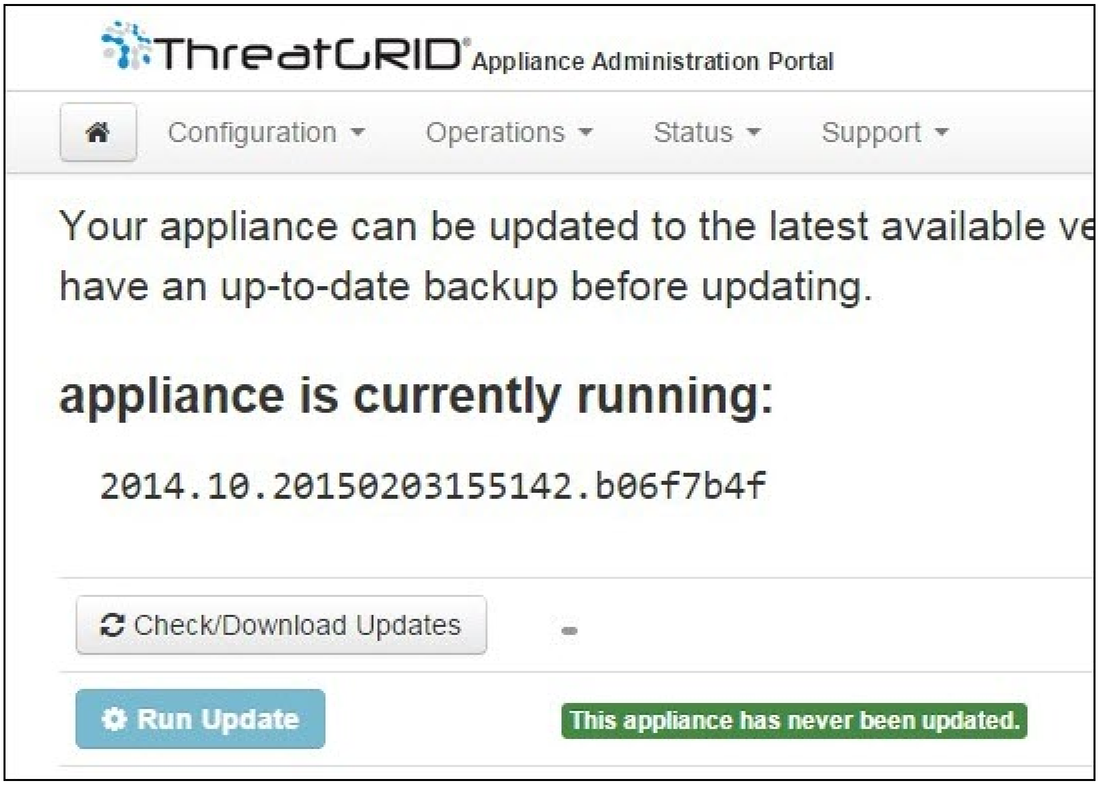
After you complete the initial Threat Grid Appliance setup, we recommend that you install any available updates before continuing. Threat Grid Appliance updates are applied through the OpAdmin portal.

Note For more information about installing updates, see the *Cisco Threat Grid Appliance Administrator Guide*.

Step 1 If you are not already in the OpAdmin portal, log in to the portal.

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

Figure 25: Appliance Build Number


ThreatGRID Appliance Administration Portal
Configuration
Operations
Status
Support
Check/Download Updates
Run Update
This appliance has never been updated.

Your appliance can be updated to the latest available ve
have an up-to-date backup before updating.

appliance is currently running:

```
2014.10.20150203155142.b06f7b4f
```

Note See the *Cisco Threat Grid Appliance Version Lookup Table* for the corresponding release version.

Step 3 Click **Check/Download 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 **Run Update** to install them.

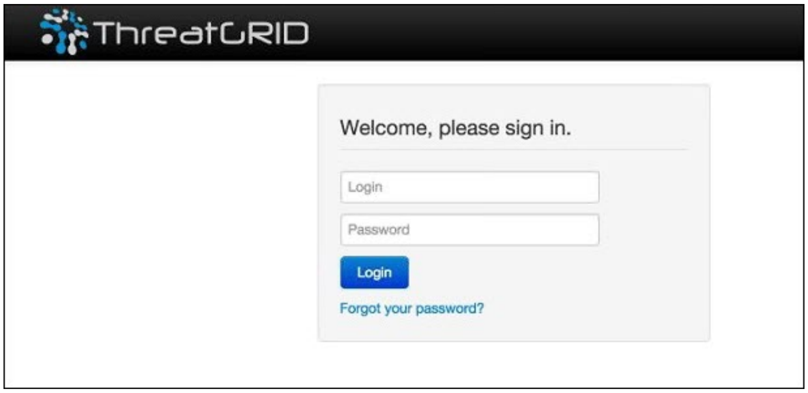
Test Appliance Setup

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 Sign in to the Threat Grid Portal using the address you configured as the Clean interface.

The Threat Grid login page opens.

Figure 26: Threat Grid Portal Login



Step 2 Enter the default credentials:

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

Step 3 Click **Login** to open the main **Threat Grid Sample Analysis** page.

Step 4 In the **Submit a Sample** box located in the upper-right corner, select a sample file or enter a URL to submit for malware analysis.

Step 5 Click **Upload Sample**.

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 **Submissions** section. Once analysis is completed, the results should be available in the **Samples** section, with details in the Analysis Report.

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 Administrator Guide* for information about administrator tasks.