



Cisco Threat Grid Appliance Setup and Configuration Guide Version 2.7

First Published: 2019-06-01

Last Modified: 2019-08-08

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.

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: <http://www.cisco.com/go/trademarks>. 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)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Introduction 1

- About Cisco Threat Grid Appliance 1
- What's New In This Release 1
- Audience 2
- Product Documentation 2
- Threat Grid Support 3
 - Enable Support Mode 4
 - Support Snapshots 4

CHAPTER 2

Planning 7

- Supported Browsers 7
- Environmental Requirements 8
- Hardware Requirements 8
- Network Requirements 8
- DNS Server Access 9
- NTP Server Access 9
- Integrations 10
 - DHCP 10
 - License 10
 - Rate Limits 10
- Organization and Users 10
- Updates 10
- User Interfaces 11
 - TGSH Dialog 11
 - Threat Grid Shell - tgsh 11
 - OpAdmin Portal 12

Threat Grid Portal	12
Cisco Integrated Management Controller (CIMC)	12
Network Interfaces	12
Login Names and Passwords (Default)	14
Setup and Configuration Overview	14

CHAPTER 3**Server Setup 15**

Connect Power Supplies and KVM Adapter	15
Network Interface Connections Setup	15
C220 M3 Rack Server Setup	15
C220 M4 Rack Server Setup	17
Network Interface Setup Diagram	18
Firewall Rules	19
Power On and Boot Up Appliance	22

CHAPTER 4**Initial Network Configuration 25**

Initial Network Configuration Using TGS dialog	25
--	----

CHAPTER 5**OpAdmin Portal Configuration Wizard 33**

Introduction	33
Log In to OpAdmin Portal	34
Change Admin Password	34
Review End User License Agreement	35
Configuration Wizard	35
Configure Network Settings	35
Install License	36
Configure NFS	37
Configure Email Host	39
Configure Notifications	39
Configure Date and Time (NTP Server)	40
Configure Syslog	41
Review and Install Configuration Settings	41
Install Updates	43
Test Appliance Setup	44

APPENDIX A

CIMC Configuration 47

Using CIMC Configuration Utility 47



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](#)
- [What's New In This Release, on page 1](#)
- [Audience, on page 2](#)
- [Product Documentation, on page 2](#)
- [Threat Grid Support, on page 3](#)

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 single UCS server: Cisco UCS C220-M3 (TG5000) or Cisco UCS C220 M4 (TG5400) for Threat Grid Appliance v2.7.2 or earlier, or Cisco Threat Grid M5 Appliance for Threat Grid Appliance v2.7.2 or later. It empowers organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.

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 are able to 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 2.7:

Table 1: Changes in Version 2.7.2ag - August 8, 2019

Feature or Update	Section
No changes.	

Table 2: Changes in Version 2.7.2 - July 23, 2019

Feature or Update	Section
Cisco Threat Grid M5 Appliance support.	About Cisco Threat Grid Appliance Product Documentation Environmental Requirements Network Interface Connections Setup
New option, <code>enable_clean_interface</code> (disabled by default), which enables access to the administrative interface on port 8443 of the assigned clean IP.	Network Interface Setup Diagram

Table 3: Changes in Version 2.7.1 - July 3, 2019

Feature or Update	Section
No changes.	

Table 4: Changes in Version 2.7 - June 1, 2019

Feature or Update	Section
Appliances now use their serial number as the hostname for better interoperability with some NFSv4 servers.	Log In to OpAdmin Portal

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](#)



Note Prior version of Cisco Threat Grid Appliance product documentation can be found on the [Threat Grid Install and Upgrade](#) page.

Threat Grid Portal UI Online Help

Threat Grid Portal user documentation, including *Release Notes*, *Using 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.

Hardware Documentation



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.

- [Cisco Threat Grid M5 Hardware Installation Guide](#)
- [Cisco UCS C220 M4 Server Installation and Service Guide](#)
- [Cisco UCS C220 Server Installation and Service Guide](#)
- [Spec Sheet for Cisco UCS C220 M4 High-Density Rack Server \(Small Form Factor Disk Drive Model\)](#) (product has been discontinued)
- [Spec Sheet for Cisco UCS C220 M3 High-Density Rack Server \(Small Form Factor Disk Drive Model\)](#) (product has been discontinued)

Threat Grid Support

There are several ways to request support from a Threat Grid engineer:

- **Email.** Send email to support@threatgrid.com with your query.
- **Open a Support Case.** You will need your Cisco.com ID (or to generate one) to open a support case. You will also need your service contract number, which was included on the order invoice. Enter your support case with the [Cisco Support Case Manager](#).
- **Call.** For Cisco phone numbers and contact information see the [Cisco Contact](#) page.

When requesting support from Threat Grid, please send the following information with your request:

- Appliance version (OpAdmin > Operations > Update Appliance)
- Full service status (service status from the shell)
- Network diagram or description (if applicable)

- Support Mode (Shell or Web interface)
- Support Request Details

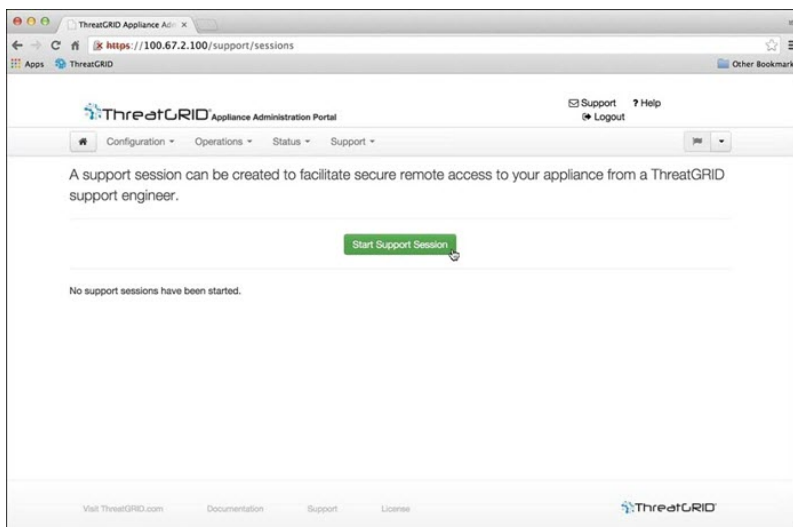
Enable Support Mode

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 TGSN 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 1: OpAdmin Start a Live Support Session



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

A Cisco Threat Grid Appliance is a Linux server with Threat Grid software installed by Cisco Manufacturing prior to shipping. Once a new appliance is received, it must be set up and configured for your on-premises network environment. Before you begin, there are a number of issues to consider and plan. This chapter includes the following information about the environmental, hardware, and network requirements:

- [Supported Browsers, on page 7](#)
- [Environmental Requirements, on page 8](#)
- [Hardware Requirements, on page 8](#)
- [Network Requirements, on page 8](#)
- [DNS Server Access, on page 9](#)
- [NTP Server Access, on page 9](#)
- [Integrations, on page 10](#)
- [DHCP, on page 10](#)
- [License, on page 10](#)
- [Organization and Users, on page 10](#)
- [Updates, on page 10](#)
- [User Interfaces, on page 11](#)
- [Network Interfaces, on page 12](#)
- [Login Names and Passwords \(Default\), on page 14](#)
- [Setup and Configuration Overview, on page 14](#)

Supported Browsers

Threat Grid supports the following browsers:

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



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

Environmental Requirements

The Threat Grid Appliance is deployed on a UCS C220-M3 or UCS C220-M4 server (v2.7.1 or earlier) or the Threat Grid M5 server (v2.7.2 or later). Before you set up and configure your appliance, make sure the necessary environment requirements for power, rack space, cooling, and other issues are met, according to the specification for your server.

Hardware Requirements

The form factor for the Admin interface is SFP+. If you are clustering appliances, each one will require an additional SFP+ module on the Cust interface.

**Note**

The SFP+ modules must be connected *before* the 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 2: Cisco 1000BASE-T Copper SFP (GLC-T)



You can attach a monitor to the server, or, if CIMC (Cisco Integrated Management Controller) is configured, you can use a remote KVM.

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 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 appliance (requests). This includes integrated appliances. For example, the Cisco Email Security appliances and Web Security appliances 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 kinds of network traffic can be outbound from the Clean network:

- Remote syslog connections
 - Email messages sent by the Threat Grid Appliance itself
 - 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 appliance (including malware traffic).



Note We recommend using a dedicated external IP address (i.e., the Dirty interface) that is different from your corporate IP, in order to protect your internal network assets.

For network interface setup information and illustrations, see the [Network Interfaces](#) section, and the [Network Interface Connections Setup](#) section.

DNS Server Access

The DNS server 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 itself needs to be accessible via the dirty network.

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.

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 support@threatgrid.com.

Rate Limits

The API rate limit is global for the 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 Threat Grid portal UI FAQ entry on rate limits for a more detailed description.

Organization and Users

Once you have completed the appliance setup and network configuration, you will need to create the initial Threat Grid Organizations and add user account(s), so 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.

Managing Threat Grid Organizations is documented in the [Cisco Threat Grid Appliance Administrator Guide](#). Managing users is documented in the Threat Grid portal Help.

Updates

The initial 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 described in this guide (see [Install Updates](#)).

Updates must be done in sequence. Threat Grid Appliance updates cannot be downloaded until the license is installed, and the update process requires the initial appliance configuration to be completed.



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 TGSN Dialog and OpAdmin with version 2.1.6.

TGSN Dialog

The **TGSN Dialog** interface is used to configure the Network Interfaces. TGSN Dialog is displayed when the appliance successfully boots up.

Reconnecting to the TGSN Dialog

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

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

The required password will either be the initial, randomly generated password, which is visible initially in the TGSN Dialog, or the new Admin password you create during the first step of the [OpAdmin Portal Configuration Wizard](#).

Threat Grid Shell - tgsh

The Threat Grid Shell (tgsh) is an administrator's interface that is used for executing a couple of commands (including destroy-data and forced backup), as well as for expert, low-level debugging. To access tgsh, select **CONSOLE** in the TGSN 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 TGSN Dialog should be used instead.

OpAdmin Portal

This is the primary Threat Grid GUI configuration tool. Much of the 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.

Cisco Integrated Management Controller (CIMC)

The Cisco Integrated Management Controller (CIMC) is the user interface used to manage the server.

Network Interfaces

The available network interfaces are described in the following table:

Interface	Description
Admin	<ul style="list-style-type: none"> • 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 nodes. <p>Note The form factor for the Admin interface is SFP+. See Figure 2 - Cisco 1000BASE-T Copper SFP (GLC-T) in Hardware Requirements.</p>
Clust	<p>The non-Admin SFP+ port that was formerly reserved, is now being used for clustering.</p> <ul style="list-style-type: none"> • 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.

Interface	Description
Clean	<ul style="list-style-type: none"> • 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)
Dirty	<p>Connect to the Dirty network; requires Internet access. Outbound Only.</p> <p>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.</p> <ul style="list-style-type: none"> • DNS <p>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.</p> <ul style="list-style-type: none"> • NTP • Updates • Support Session in Normal Operations Mode • Support Snapshots • Malware Sample-initiated Traffic • Recovery Mode Support Session (outbound) • OpenDNS, TitaniumCloud, Virus Total, ClamAV • SMTP Outbound connections are redirected to a built-in honeypot <p>Note Although using IPv4LL address space (168.254.0.16) for the Dirty interface has never been documented as supported, from version 2.3.0 forward it is recognized as broken, and therefore explicitly unsupported.</p>

Interface	Description
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 CIMC Configuration .

Login Names and Passwords (Default)

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

User	Login/Password
Web UI Administrator	Login: admin Password: changeme
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, follow the Lost Password instructions located in the Support section of the Cisco Threat Grid Appliance Administrator Guide .
CIMC	Login: admin Password: password

Setup and Configuration Overview

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

- Server Setup
- Network Interface Connections Setup (Admin, Clust, Clean, Dirty)
- Initial Network Configuration - TGSH Dialog
- Main Configuration - OpAdmin Portal
- Install Updates
- Test the Appliance Setup - Submit a Sample for Analysis

Complete the remaining administrative configuration tasks (license installation, email server, SSL Certificates, etc.) in the OpAdmin Portal as documented in the [Cisco Threat Grid Appliance Administrator Guide](#).

You should allow yourself approximately 1 hour to complete the server setup and initial configuration steps.



CHAPTER 3

Server Setup

This chapter provides instructions for setting up the server. It includes the following topics:

- [Connect Power Supplies and KVM Adapter](#), on page 15
- [Network Interface Connections Setup](#), on page 15
- [Network Interface Setup Diagram](#), on page 18
- [Firewall Rules](#), on page 19
- [Power On and Boot Up Appliance](#), on page 22

Connect Power Supplies and KVM Adapter

To begin, connect both power supplies on the back of your appliance. Connect the included KVM adapter to an external monitor and keyboard, and plug into the KVM port located at the front of the server, as illustrated in Figure 3.

If CIMC is configured, you can use a remote KVM. See [CIMC Configuration](#).

Refer to the server product documentation for detailed hardware and environmental setup information (See [Product Documentation](#)).

Network Interface Connections Setup

The SFP+ modules must be connected to the chassis *before* the appliance is powered on for the session in which the configuration wizard is going to be run. However, wiring the SFP up to the network can be done between power on and configuration.



Note For Threat Grid Appliance (version 2.7.2 or later), only the Threat Grid M5 Appliance is supported. Refer to the [Cisco Threat Grid M5 Appliance Hardware Installation Guide](#) for server setup instructions.

C220 M3 Rack Server Setup

The interfaces must be properly connected and configured for the appliance to operate.



Note The details for your appliance may differ from the illustrations. Contact support@threatgrid.com if you have any questions.

Find the two SFP+ ports and three Ethernet ports on the back of the appliance and attach the network cables as illustrated in Figure 4.

Reserved is the non-Admin SFP+ port that is reserved for future use.

Figure 3: Cisco UCS C220 M3 SFF Rack Server

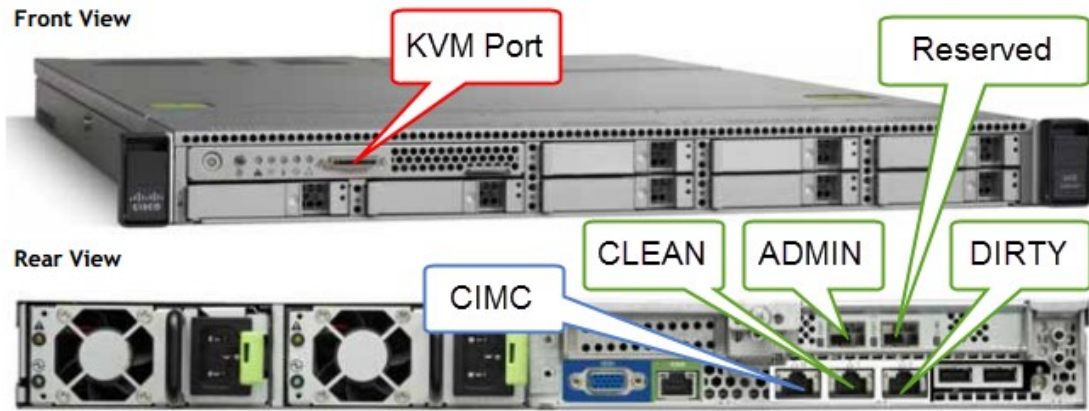
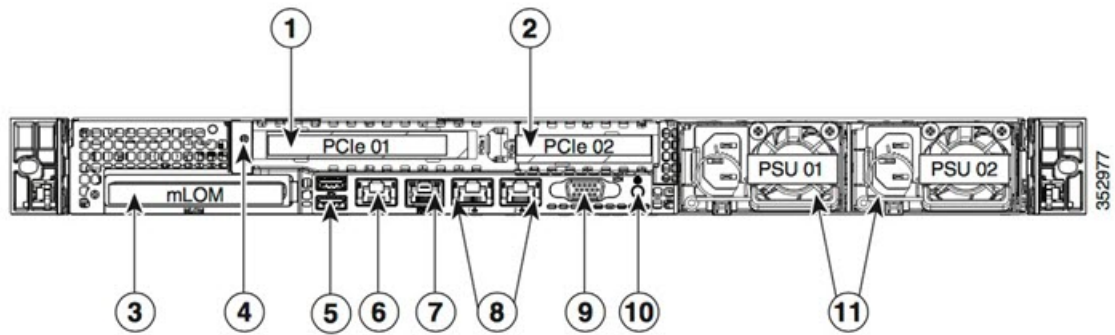


Figure 4: Cisco UCS C220 M3 Rear View Details



1	PCIe riser 1/slot 1	7	Serial port (RJ-45 connector)
2	PCIe riser 2/slot 2	8	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
3	Modular LAN-on-motherboard (mLOM) card slot	9	VGA video port (DB-15)
4	Grounding-lug hole (for DC power supplies)	10	Rear unit identification button/LED
5	USB 3.0 ports (two)	11	Power supplies (up to two, redundant as 1+1)
6	1-Gb Ethernet dedicated management port		



Note For releases 1.0-1.2 a reboot may be needed if an interface was not plugged in at boot time. This is a pre-1.3 issue, except for any interface requiring an SFP, which will still need to be plugged in at boot time post 1.3. The network cable plugged into the SFP may be safely hot-plugged.

C220 M4 Rack Server Setup

The interfaces must be properly connected and configured for the appliance to operate.

Use port 3 Slot 2 for the (optional) Clust interface.



Note The details for your appliance may differ from the illustrations. Contact support@threatgrid.com if you have any questions.

Figure 5: Cisco UCS C220 M4 SFF Rack Server

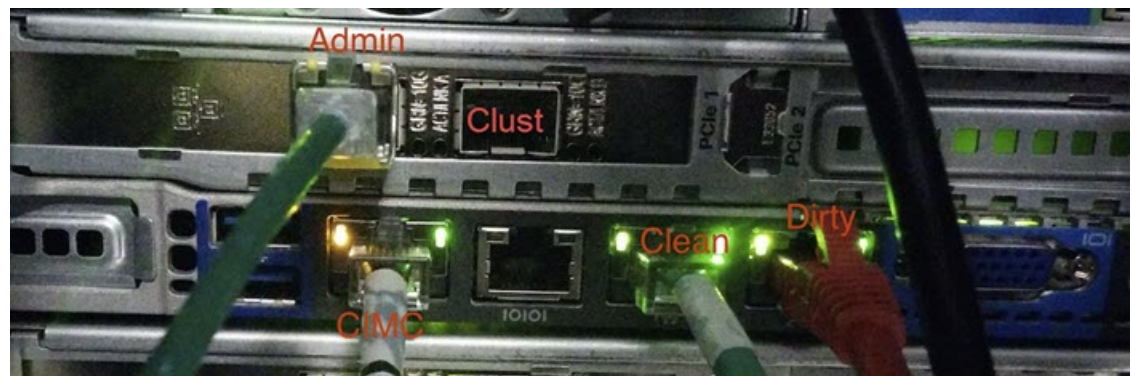
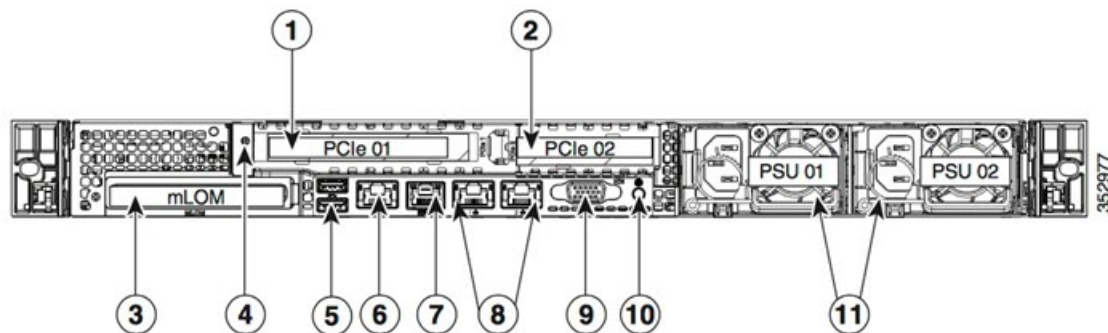


Figure 6: Cisco UCS C220 M4 Rear View Details



1	PCIe riser 1/slot 1	7	Serial port (RJ-45 connector)
2	PCIe riser 2/slot 2	8	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
3	Modular LAN-on-motherboard (mLOM) card slot	9	VGA video port (DB-15)
4	Grounding-lug hole (for DC power supplies)	10	Rear unit identification button/LED
5	USB 3.0 ports (two)	11	Power supplies (up to two, redundant as 1+1)
6	1-Gb Ethernet dedicated management port		

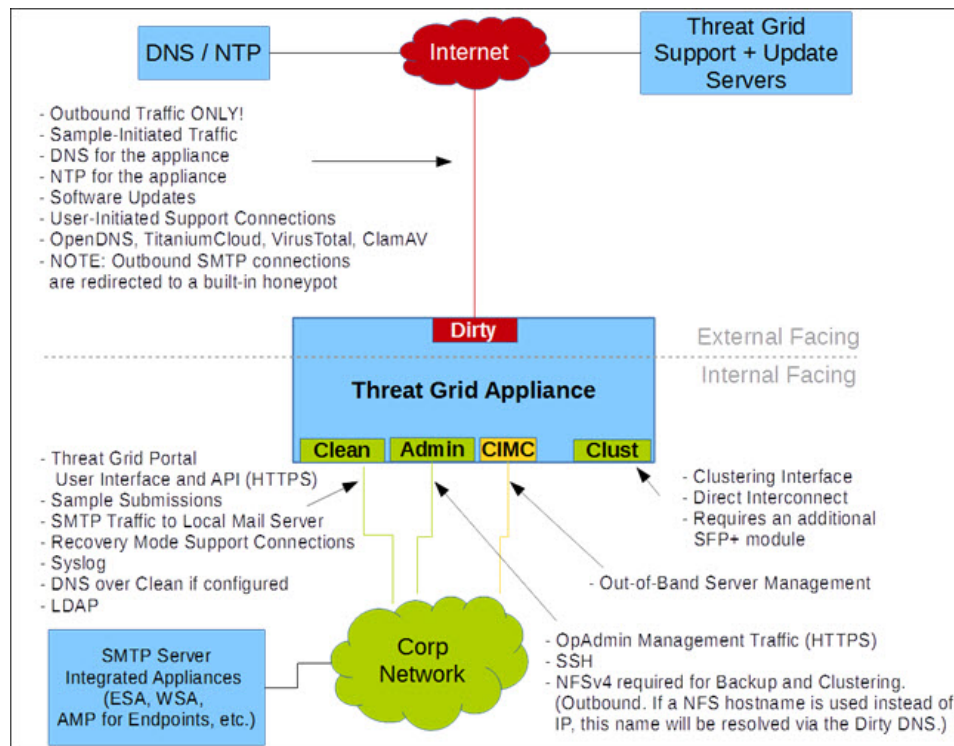
Connections:

- 1 Admin, Clust
- 8 (left) Clean
- 8 (right) Dirty
- 6 CIMC

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, for example.

Figure 7: Network Interfaces Setup Diagram



Note In Threat Grid Appliance (v2.7.2 and later), there is also the **enable_clean_interface option**, which 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. See the required destinations in the configuration sections.



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

Dirty Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	ANY	ANY	Allow	Allow outbound traffic from samples. (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 connectivity 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 TGS 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

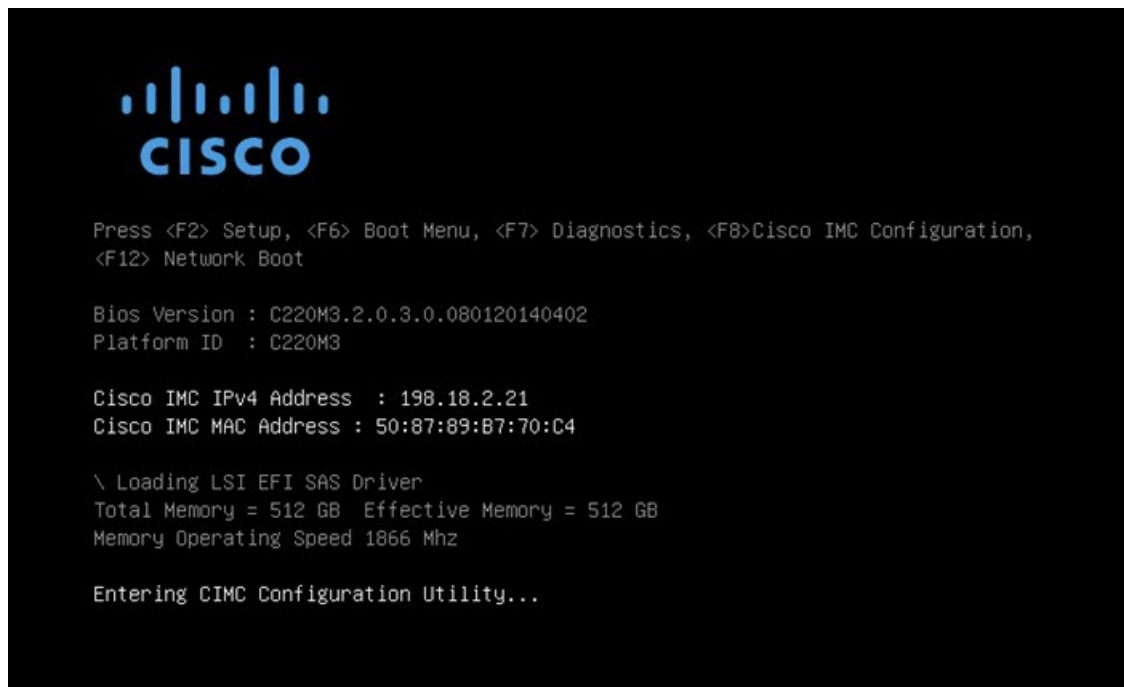
Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	22	Allow	Update, support snapshot, and licensing services.
Dirty Interface	Internet	TCP/UDP	53	Allow	Allow outbound DNS.
Dirty Interface	Internet	UDP	123	Allow	Allow outbound NTP.

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.

Power On and Boot Up Appliance

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

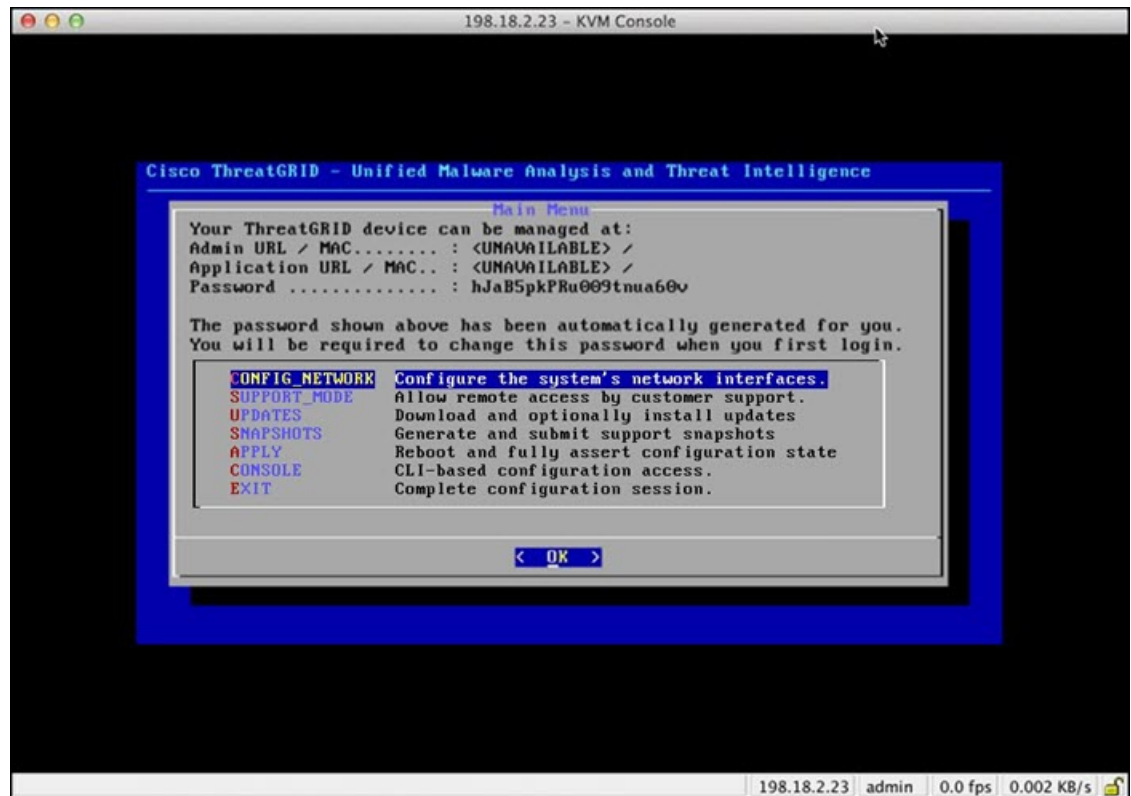
Figure 8: Cisco Screen During Bootup



Note If you want to configure this interface, press **F8** after the memory check is completed and follow the instructions in [CIMC Configuration](#).

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

Figure 9: TGSH Dialog



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).



CHAPTER 4

Initial Network Configuration

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

- [Initial Network Configuration Using TGSN Dialog, on page 25](#)

Initial Network Configuration Using TGSN Dialog

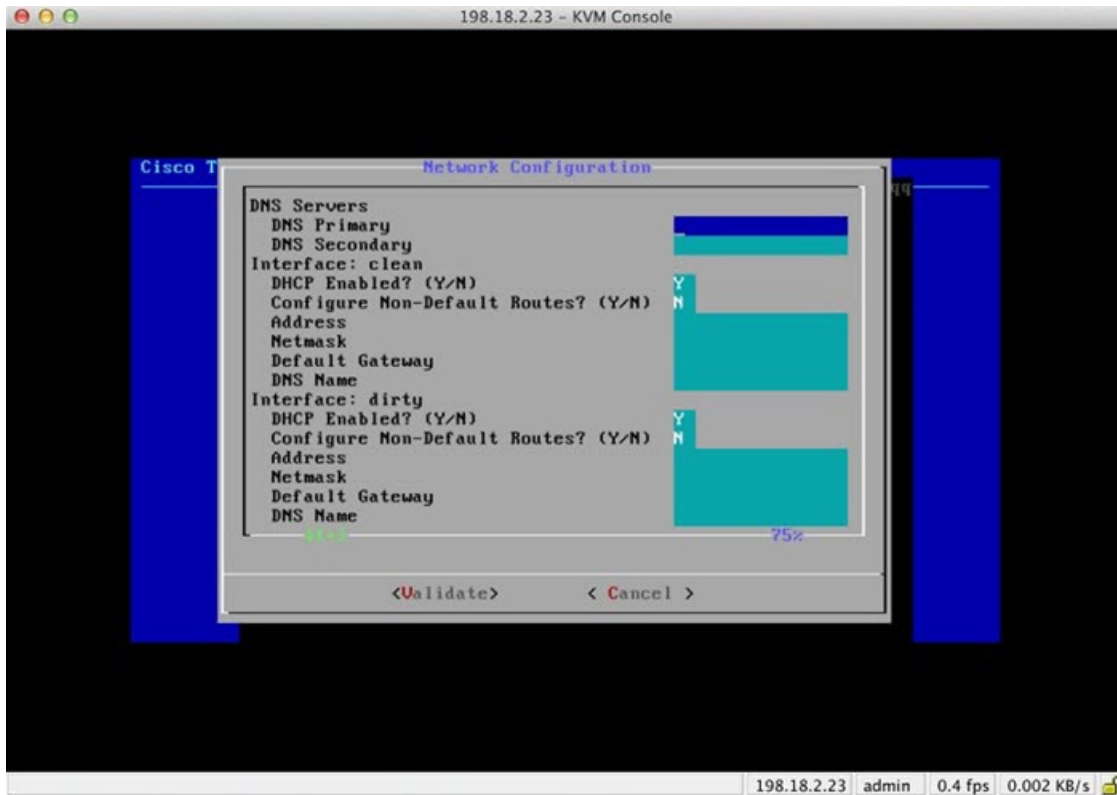
The initial network configuration is completed in the TGSN Dialog. The goal is to complete the basic configuration that allows access to the OpAdmin interface tool to complete the remaining configuration, including the license, email host, and SSL Certificates.



Note For DHCP users, the following steps assume that you are using static IP addresses. If you are using DHCP to obtain your IPs, then see the [Cisco Threat Grid Appliance Administrator Guide](#) for more information.

Step 1 In the TGSN Dialog interface, select **CONFIG_NETWORK**. The Network Configuration console opens.

Figure 10: TGS 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** from Y 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 of 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 11: Network Configuration In-Progress (Clean and Dirty)

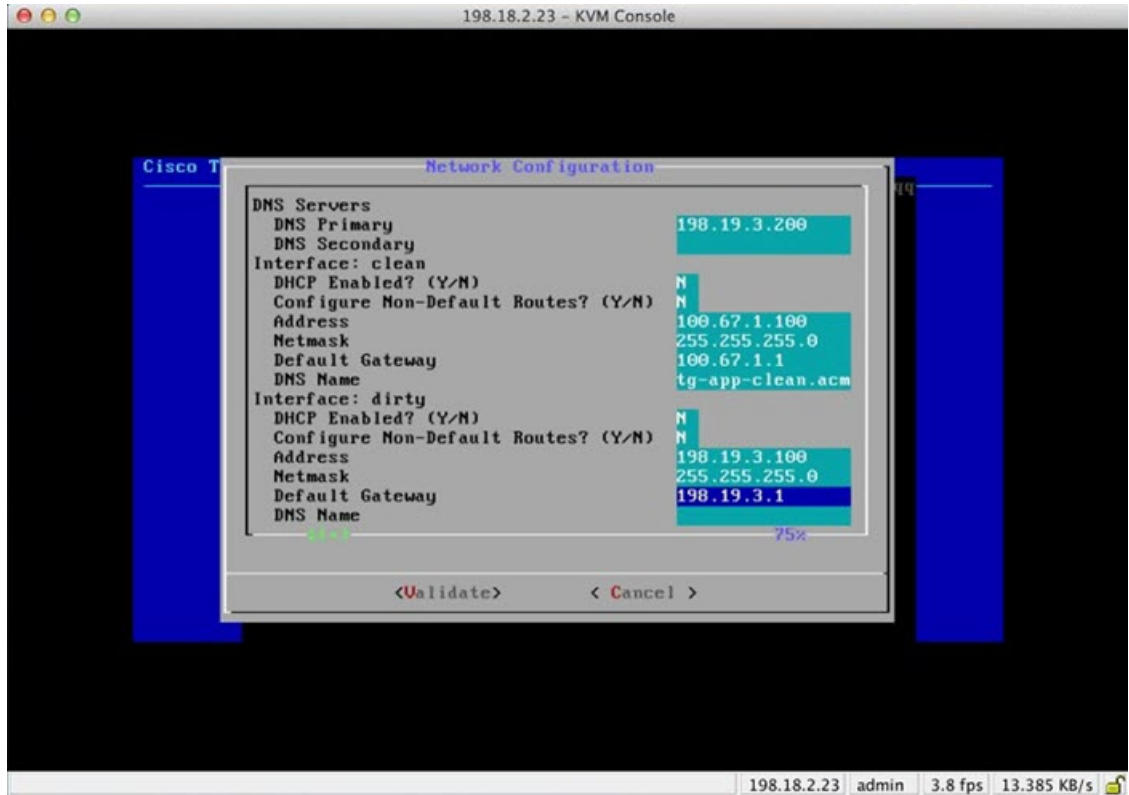
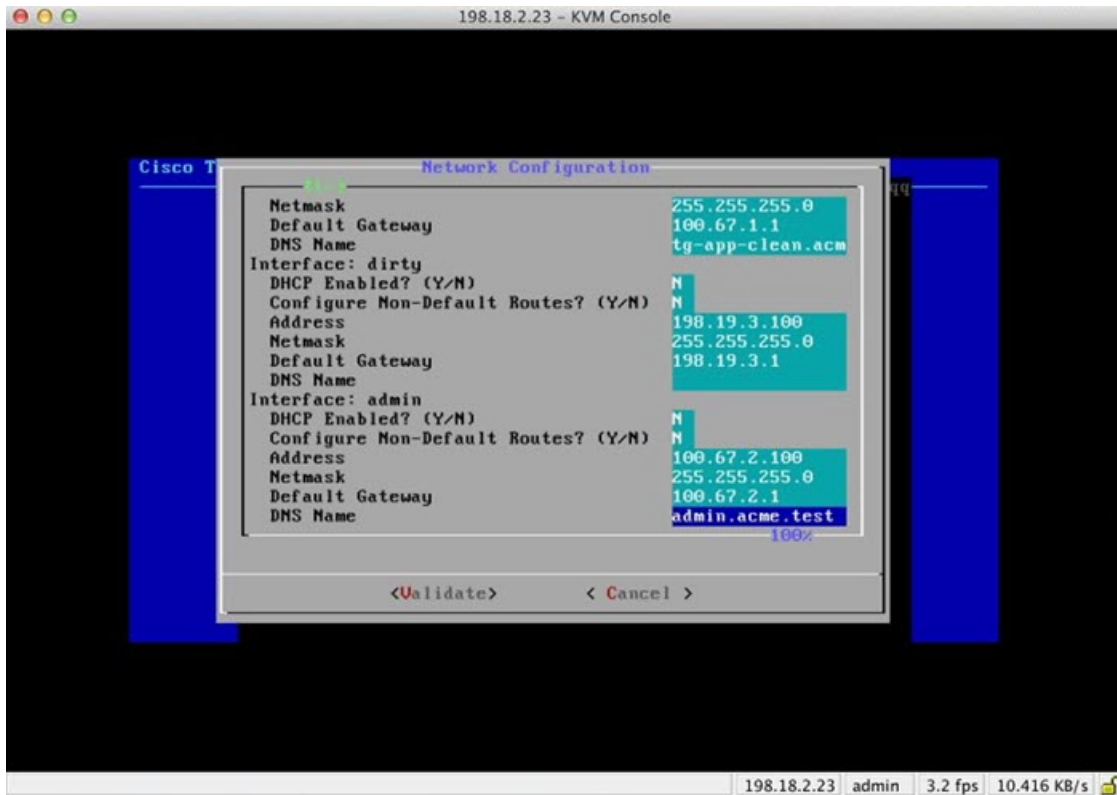
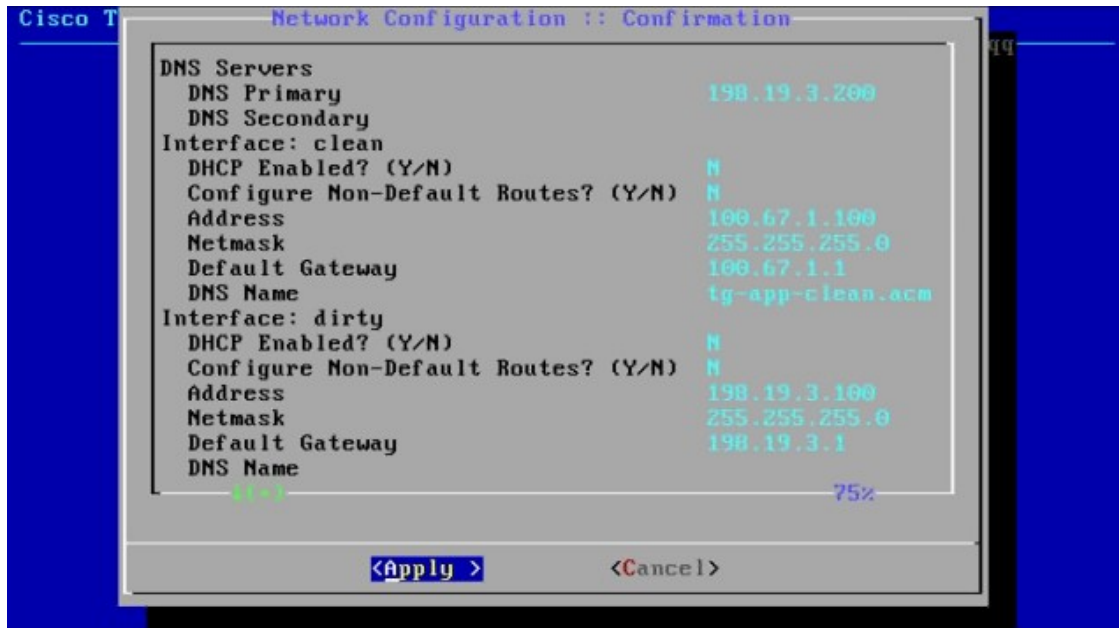


Figure 12: Network Configuration In-Progress (Admin)



- Step 7** After you finish entering all the network settings, tab down and select **Validate** to validate your entries. If invalid values have been entered, you may see errors. If this occurs, fix the invalid values and select **Validate** again. After validation, the Network Configuration Confirmation displays the entered values.

Figure 13: Network Configuration Confirmation

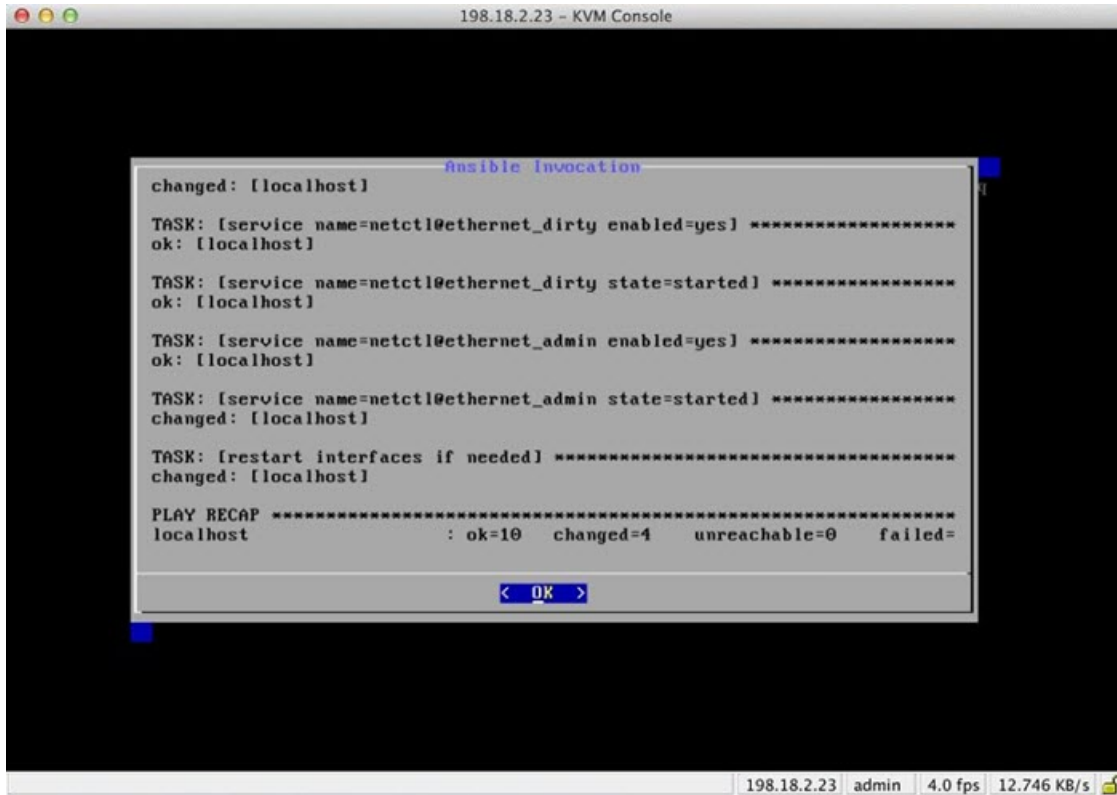


Step 8 Select **Apply** to apply your configuration settings.

It may take 10 minutes or more to complete.

The console becomes a blank grey box, and the screen may display scrolling configuration information as the settings are applied, and then it lists detailed information about the configuration changes that have been made.

Figure 14: Network Configuration - List of Changes Made



The screenshot shows a KVM Console window titled "198.18.2.23 - KVM Console". Inside the console, an Ansible invocation window is displayed with the following output:

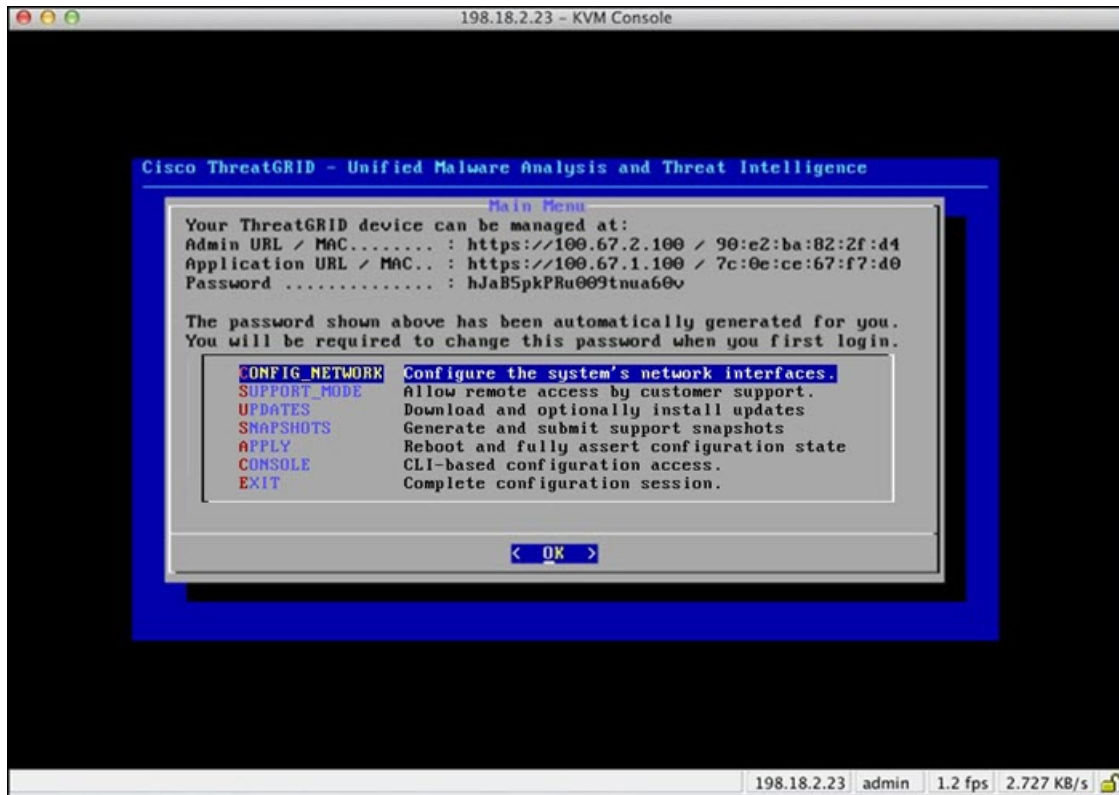
```
changed: [localhost]
TASK: [service name=netctl@ethernet_dirty enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_dirty state=started] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin state=started]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

At the bottom of the Ansible invocation window, there is a button labeled "< OK >".

Step 9 Select **OK**.

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

Figure 15: IP Addresses



You have completed the network configuration of your appliance.

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

What to do next

The next step in the appliance setup is to complete the remaining configuration tasks using the OpAdmin Portal, as described in [OpAdmin Portal Configuration Wizard](#).



CHAPTER 5

OpAdmin Portal Configuration Wizard

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

- [Introduction, on page 33](#)
- [Configuration Wizard, on page 35](#)
- [Install Updates, on page 43](#)
- [Test Appliance Setup, on page 44](#)

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 16: OpAdmin Login Screen



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 administrator's 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 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 appliance network configuration.

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

Step 2 If you used DHCP for your initial connection and now need to change the Clean and Dirty IP networks to static IP addresses, follow the steps in the *Using DHCP* section of the [Cisco 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 17: License Page Prior to Installation

The screenshot shows a web interface for license management. It is divided into several sections:

- Appliance ID:** A text field containing the value "FCH1832V32N".
- License:** A section with the text "No license has been installed."
- Upload New License:** A section containing:
 - A "Choose File" button next to the text "No file chosen".
 - A "Passphrase" input field with a lock icon on the left.
 - An "Upload" button.
- Retrieve License From Server:** A section with a "Retrieve" button.

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 (v2.3 or later). 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 18: 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	
<input type="button" value="Choose File"/>	No file chosen
<input type="password" value="Passphrase"/>	
<input type="button" value="Upload"/>	
Retrieve License From Server	
<input type="button" value="Retrieve"/>	
<input type="button" value="Next >"/>	

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 *NFS Requirements* in the *Backups* section of 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 appliance's local datastores from the NFS store's contents.

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

Figure 19: NFS Configuration

The screenshot shows the ThreatGRID Appliance Administration Portal interface. At the top, there are links for Support and Help, and a Logout button. Below this is a navigation bar with tabs for Configuration, Operations, Status, and Support. On the left, a sidebar menu lists various configuration categories: Configuration (with sub-items: Network, License, NFS, Clustering, Email, Notifications, Date and Time, Syslog), and Other (with sub-item: Review and Install). A 'Start Installation' button is visible below the sidebar. The main content area is titled 'NFS' and contains a form titled 'NFS Configuration'. The form has four rows: 'Host' with a text input field and a refresh icon; 'Path' with a text input field and a folder icon; 'Opts' with a text input field and a list icon; and 'Status' with a dropdown menu currently showing 'Disabled'. A green 'Next >' button is positioned at the bottom right of the form. At the bottom of the page, there are links for 'Visit the Cisco Threat Grid homepage', 'Documentation', 'Support', and 'License', along with the ThreatGRID logo.

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 configuration page.

Figure 20: Email Configuration

The screenshot shows the ThreatGRID Appliance Administration Portal interface. On the left is a navigation pane with categories like Configuration, Other, and Start Installation. The main content area is titled 'Email' and contains an 'SMTP Configuration' section. This section includes several rows of settings, each with a 'HELP' icon and a dropdown menu:

- Delivery Mode:** Set to 'Upstream Relay'.
- Upstream Host:** Set to 'smtp.acme.test' with a port of '587'. This row is highlighted in yellow.
- SSL:** Set to 'Detect from Port'.
- Upstream Authentication:** Set to 'No Authentication'.
- From Address:** An empty text input field.

A green 'Next >' button is located at the bottom right of the configuration area. At the bottom of the page, there are links for 'Visit the Cisco Threat Grid homepage', 'Documentation', 'Support', and 'License', along with the ThreatGRID logo.

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

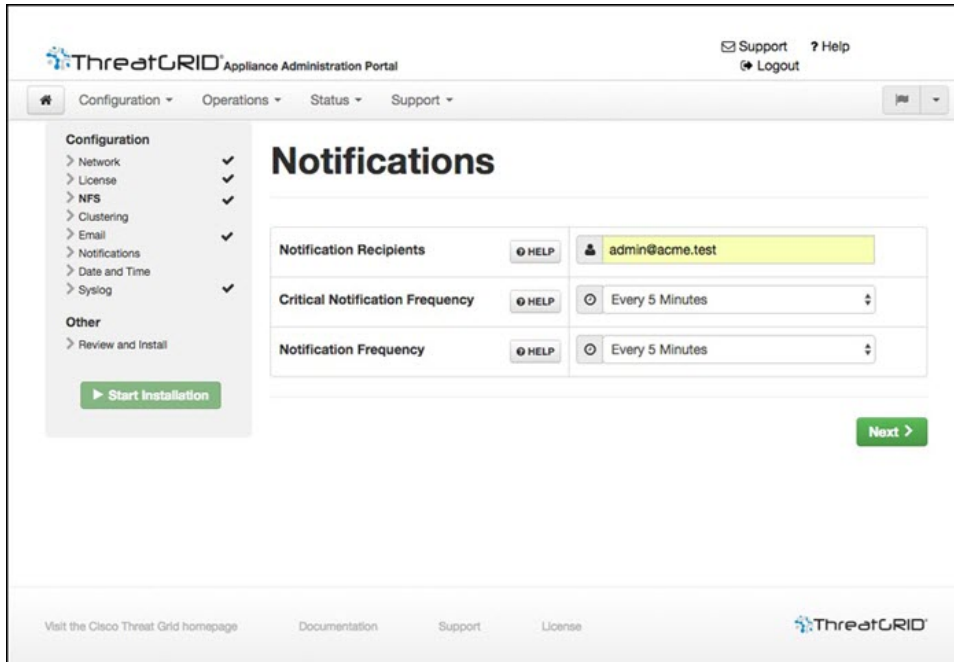
Proceed to [Configure Notifications](#).

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 configuration page.

Figure 21: Notifications Configuration



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 menus.

Step 4 Click **Next** to continue.

What to do next

Proceed to [Configure Date and Time \(NTP Server\)](#).

Configure Date and Time (NTP Server)

The next step is to identify the Network Time Protocol (NTP) servers.

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](#).

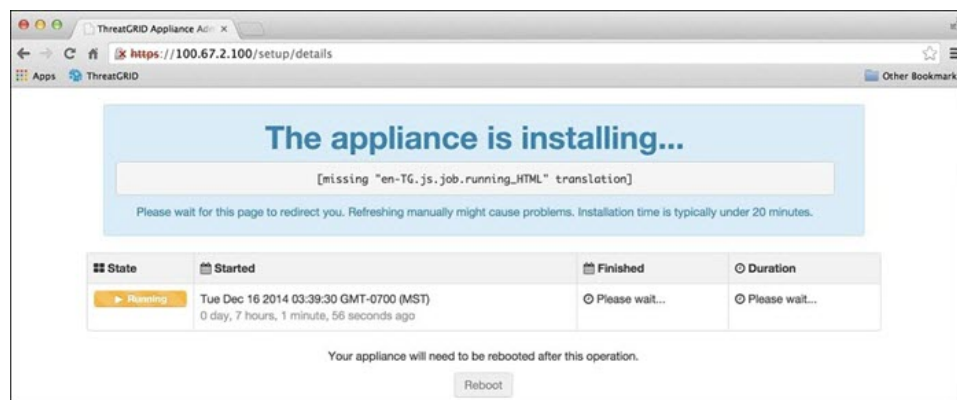
Review and Install Configuration Settings

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.

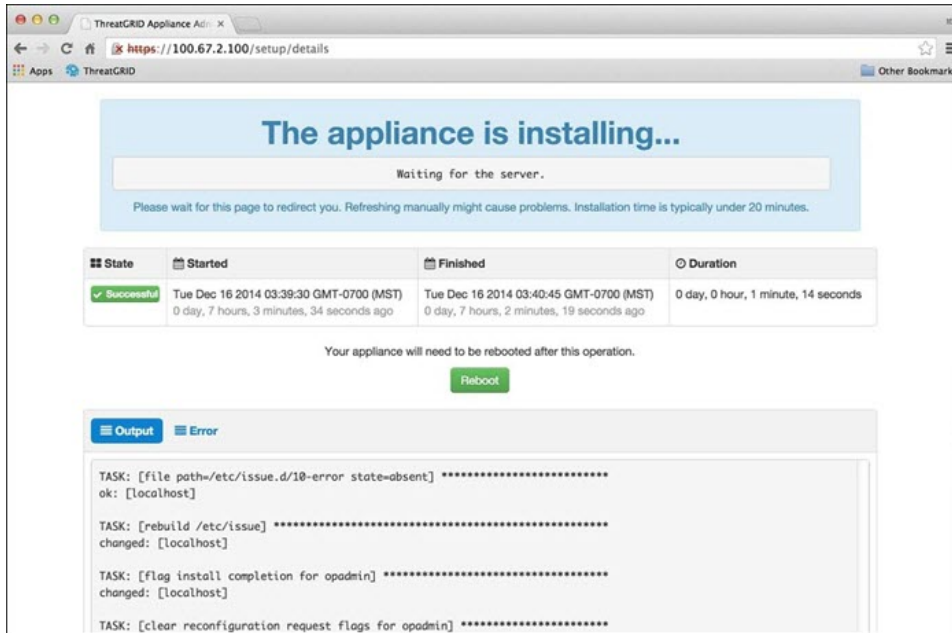
Note The installation may take over 10 minutes to complete. The screen displays configuration information as it is applied.

Figure 22: Appliance Is Installing



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

Figure 23: Successful Appliance Installation



Step 2 Click **Reboot**.

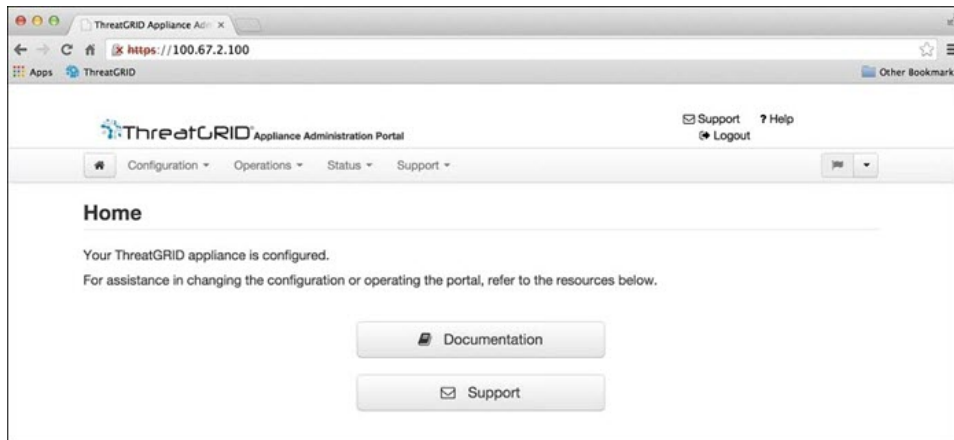
Note Rebooting may take up to 5 minutes. Do not make any changes while the appliance is rebooting.

Figure 24: Appliance Is Rebooting



Once the appliance has successfully rebooted, a message is displayed on the Home page indicating that your appliance is configured.

Figure 25: Appliance Successfully Configured



The appliance configuration is complete.

Install 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.

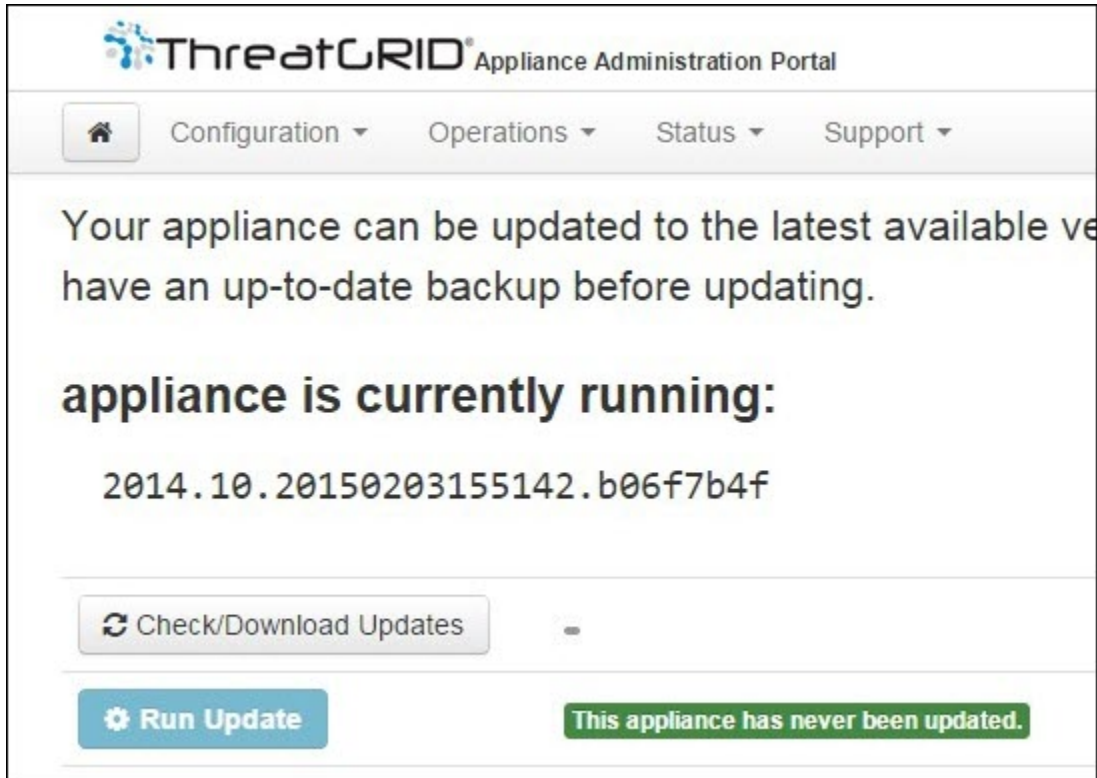


Note For more information about installing updates, see the [Cisco Threat Grid Appliance Administrator Guide](#).

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 26: Appliance Build Number



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

Step 3 Click **Check/Download Updates**.

The software checks 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.

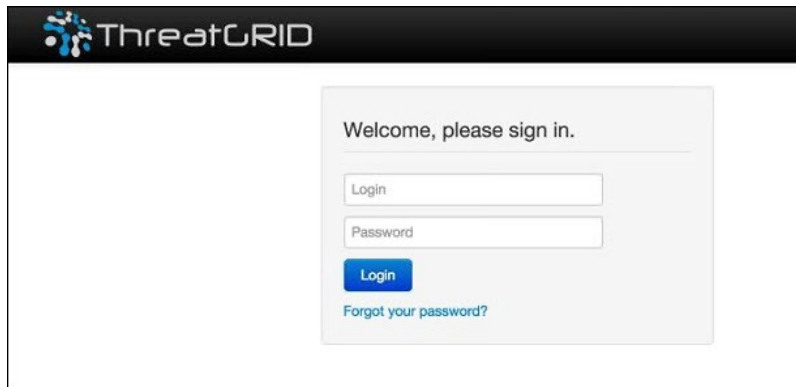
Test Appliance Setup

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 27: Threat Grid Portal Login



Step 2 Enter the default **Login** (admin) and **Password** (changeme).

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.



APPENDIX **A**

CIMC Configuration

This appendix describes using the Cisco Integrated Management Controller (CIMC) Configuration Utility to set up remote server management.

- [Using CIMC Configuration Utility, on page 47](#)

Using CIMC Configuration Utility

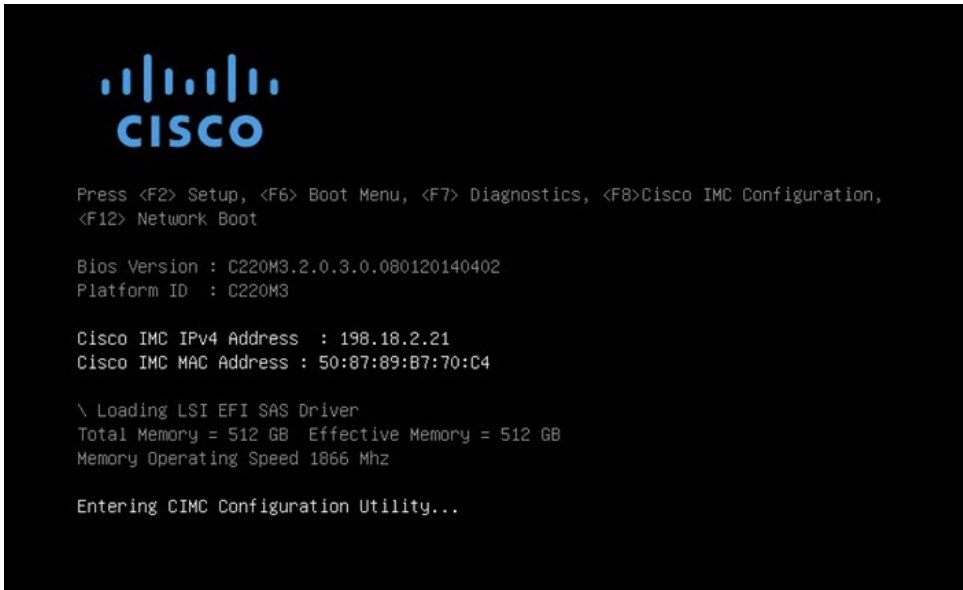
After booting the server, the Cisco screen is displayed, which allows you to enter the Cisco Integrated Management Controller (CIMC) Configuration Utility. The CIMC interface can be used for remote server management.



Note A monitor and keyboard must be attached directly to the appliance to use this utility.

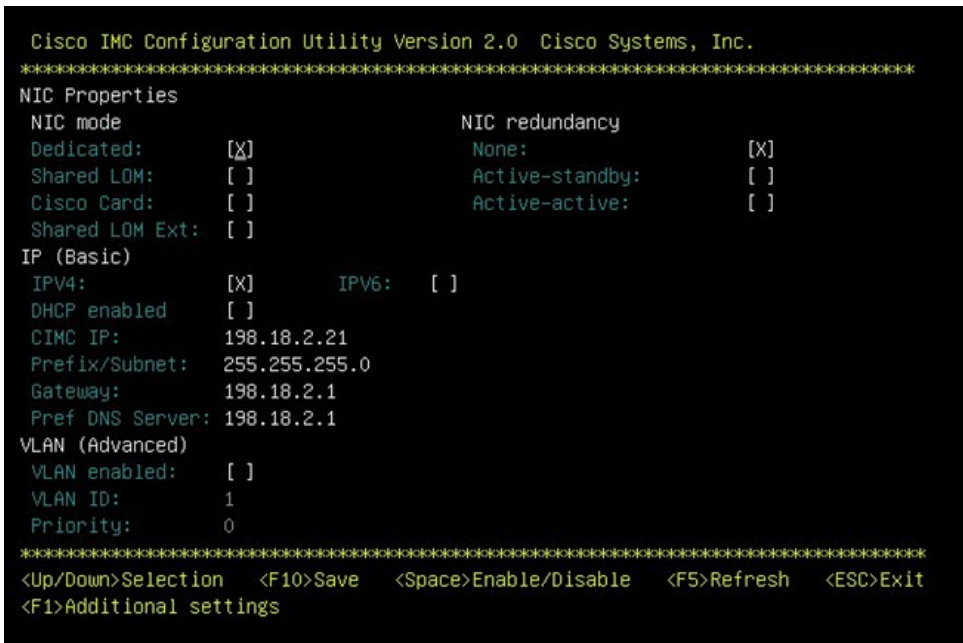
Step 1 Power on the server.

Figure 28: Cisco Screen



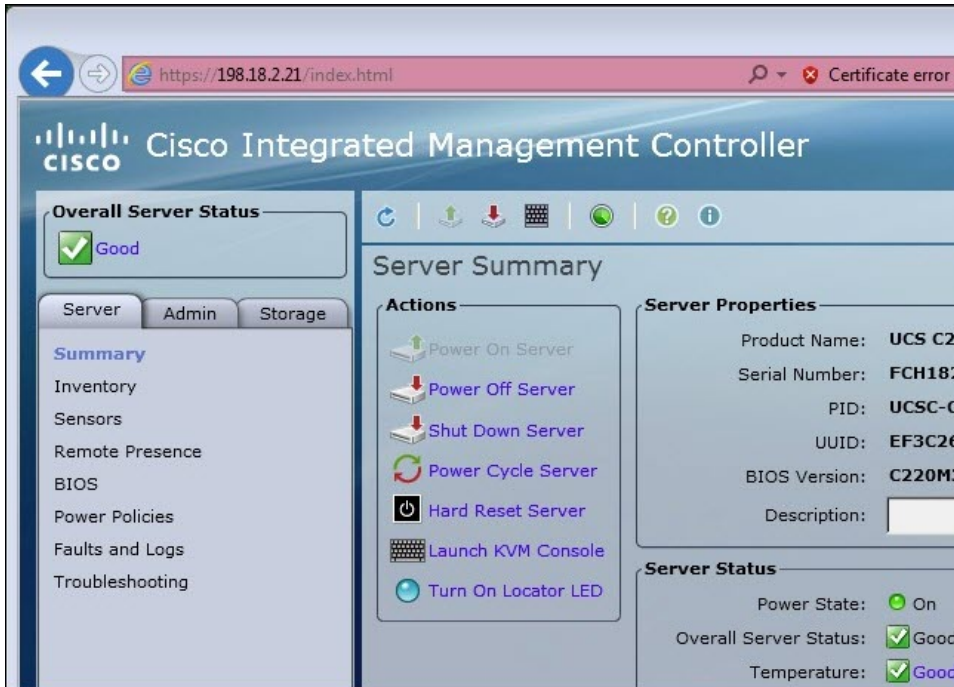
Step 2 After the memory check is completed, press **F8** to enter the CIMC Configuration Utility.

Figure 29: CIMC Configuration Utility



- Step 3** In the CIMC configuration utility, set up an IP address that can be used for remote server management.
- Step 4** Save the configuration and exit the utility.
- Step 5** In a web browser, enter **https://<CIMC-IP address>/** to open the CIMC Interface.
- Step 6** Enter the initial **User Name** (admin) and **Password** (password).

Figure 30: Cisco Integrated Management Controller (CIMC) Interface



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

