Cisco AMP Threat Grid Appliance Setup and Configuration Guide

Version 2.1.4

Last Updated: 11/17/2016

Cisco Systems, Inc. www.cisco.com

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

Cisco AMP Threat Grid Appliance Setup and Configuration Guide

CONTENTS

LIST OF FIGURES

INTRODUCTION

A Cisco AMP Threat Grid Appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. Threat Grid Appliances provide the complete Threat Grid malware analysis platform, installed on a single UCS server (UCS C220-M3 or C220 M4). They empower organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.

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

With an AMP 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.

Who This Guide Is For

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 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.

For more information, please see the Cisco AMP *Threat Grid Appliance Administrator's Guide,* which can be found on the **Install and Upgrade page** on Cisco.com.

Release Notes

For detailed updates information, see the *Release Notes*, which may be found in the OpAdmin Portal:

Operations menu > **Update Appliance**

Formatted PDF versions of the *Threat Grid Appliance Release Notes* are also **available online**.

Note: To view the release notes for the Threat Grid Portal UI, click **Help** in the UI's navigation bar.

What's New

Cisco UCS C220 M4 Server

Released on November 17, 2016, the C220 M4 server includes a hardware refresh, as well as the Secure Boot feature. Please contact us at support@threatgrid.com to discuss any questions you may have about upgrading.

Note: Threat Grid will continue to provide support for M3s until after the expiration of their contracted lifespan. All the same M4 features are available as over-the-wire updates for existing M3s.

The M5 server upgrade is currently under development. We strongly encourage existing M3 and M4 customers to contact us at support@threatgrid.com to discuss any questions you may have about which server upgrade is best for your needs, as well as data migration, backups, rollout strategies, etc. Additional complexity is introduced by the migration to version 2.1.5 of the Threat Grid Appliance software, which is currently in

development. We think the best approach for planning the upgrade path to the M5 is to address our customers' requirements on an individual basis.

Version 2.0.3

FireAMP Private Cloud Integrations: The 2.0.3 release contains features to facilitate Threat Grid Appliance integrations with Fire AMP Private Cloud, including the ability to split the DNS between the Clean and Dirty network interfaces, CA Management, and FireAMP Private Cloud Integration Configuration.

Generated SSL certificates now have the CN duplicated as a subjectAltName. This addresses an incompatibility with SSL clients which ignore the CN field when at least one subjectAltName is present. It may be necessary to regenerate any previously appliance-generated certificates if using such tools.

Version 2.0

Version 2.0 is a major release, built upon an updated operating system. It includes enhancements that will support future hardware releases, and also brings the Threat Grid Portal UI more in line with the Cloud version. This includes significant numbers of new and updated Behavioral Indicators and other changes.

Please read the *Threat Grid Portal Release Notes* beginning with release 3.3.45 for details. (From the Portal UI Navigation bar select **Help**, then click on the link to the release notes. The release notes are cumulative: the most recent version contains all previous notes.)

Support - Contacting Threat Grid

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 here: https://tools.cisco.com/ServiceRequestTool/scm/mgmt/case

Call. For Cisco phone numbers see: http://www.cisco.com/c/en/us/support/index.html

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

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. This can be done via the **OpAdmin Portal Support** menu. (You can also enable **SUPPORT MODE** from the TGSH Dialog.)

To start a live support session with Threat Grid tech support:

In **OpAdmin**, select **Support > Live Support Session** and click **Start Support Session**.

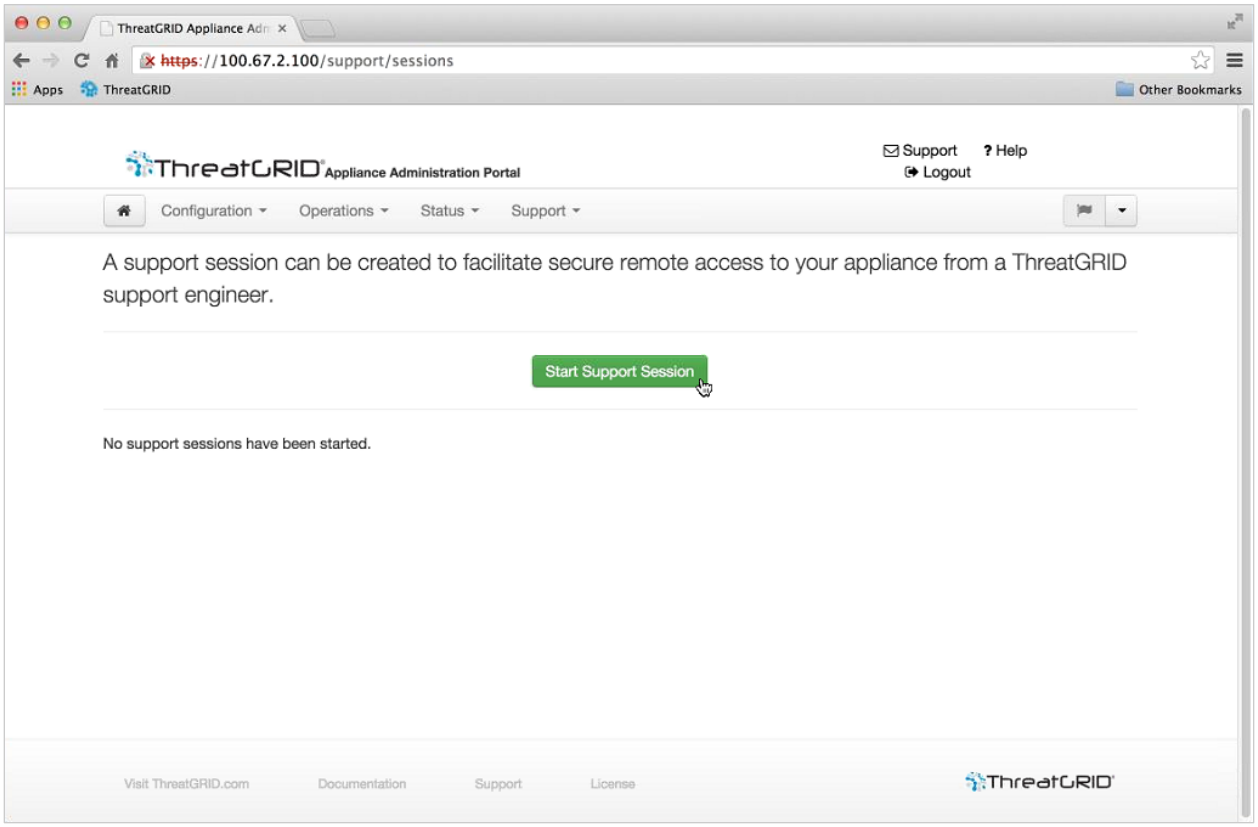
Note: You can break out of the OpAdmin wizard task-flow to enable Support Mode, prior to licensing.

Start Support Mode - License Workaround Prior to Version 1.4.4

There is an issue with licenses that has been resolved in the Threat Grid Appliance v1.4.4. If your software version is prior to 1.4.4, you will need to have successfully connected to *Support Mode* servers at least once (after November 14th, 2015), in order for your license to be accepted. The connection does not need to be ongoing or active at the time of the license validation.

Required: The Dirty network needs to be up in order for this step to work.

Figure 1 - OpAdmin Start a Live Support Session



Support Servers

Establishing a support session requires that the TG appliance reach the following servers:

- support-snapshots.threatgrid.com
- rash.threatgrid.com

Both servers should be allowed by the firewall during an active support session.

Support Snapshots

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

1. Verify that SSH is specified for Support Snapshot services.
2. From the **Support** menu, select **Support Snapshots**.
3. Take the snapshot.
4. Once you take the snapshot you can either download it yourself as .tar .gz, or you can press **Submit**, which will automatically upload the snapshot to the Threat Grid snapshot server.

PLANNING

A Cisco AMP 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. Environmental requirements, hardware requirements, and network requirements are described below.

User Documentation and Online Help

Threat Grid Appliance - Threat Grid Appliance user documentation, including this document, the *Threat Grid Appliance Administrator's Guide*, Release Notes, integration guides, and more, can be found on the **Install and Upgrade page** on Cisco.com.

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.

Environmental Requirements

The Threat Grid Appliance is deployed on a UCS C220-M3 or C220-M4 server. 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 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)

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

Hardware Documentation

Installation and Service Guide for Cisco UCS C220 M4 Server:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M4/install/C220M4.pdf

Installation and Service Guide for Cisco UCS C220 M3 Server:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220/install/C220.html

Spec Sheet for Cisco UCS C220 M3 High-Density Rack Server (Small Form Factor Disk Drive Model):

http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/C220M3_SFF_SpecSheet.pdf

Cisco has a power/cooling calculator, which you may also find useful:

https://mainstayadvisor.com/Go/Cisco/Cisco-UCS-Power-Calculator.aspx

Network Requirements

The Threat Grid Appliance requires three networks:

ADMIN - The "*Administrative"* network. Must be configured in order to perform the appliance setup.

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 (ESA/WSA) connect to the IP address of the Clean interface.

Note: The following specific, restricted kinds of network traffic can be outbound from Clean:

- Remote syslog connections
- Email messages sent by the Threat Grid Appliance itself
- Disposition Update Service connections to FireAMP Private Cloud devices
- DNS requests related to any of the above

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, and Network Interface Connections Setup sections below.

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 FireAMP Private Cloud integrations. If the FireAMP 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 *Threat Grid Appliance Administrator's Guide* for additional information.

NTP Server Access

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

Integrations – ESA/WSA/FireAMP etc.

Additional planning may be required if the Threat Grid Appliance is going to be used with other Cisco products, such as ESA/WSA appliances, FireAMP Private Cloud, etc.

DHCP

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

License

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

For questions about licenses, please contact support@threatgrid.com.

Organization and Users

Once you have completed the appliance setup and network configuration, you will need to create the initial Threat Grid Organizations and 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 and users is documented in the *Threat Grid Appliance Administrator's Guide*.

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.

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. Instructions for updating the appliance are located in the *Threat Grid Appliance Administrator's Guide*.

Note: Verify that SSH is specified for updates.

Threat Grid Appliance 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:

TGSH Dialog

The first interface is the **TGSH Dialog**, which is used to configure the Network Interfaces. TGSH Dialog is displayed when the appliance successfully boots up.

Reconnecting to the TGSH Dialog

TGSH 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 TGSH 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 TGSH Dialog, or the new Admin password you create during the first step of the OpAdmin Portal Configuration, which is described in the next section.

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, SSL Certificates, etc.

AMP 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.

CIMC

Another user interface is the Cisco Integrated Management Controller ("CIMC"), which is used to manage the server.

Network Interfaces

Admin Interface

- Connect to the Admin network. **Only inbound** from Admin network.
- OpAdmin UI traffic
- SSH (inbound) for tgsh-dialog

Note: The form factor for the Admin interface is SFP+. See Figure 2 - Cisco 1000BASE-T Copper SFP (GLC-T).

Clean Interface

- Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet, except in Recovery Mode.
- UI and API traffic (inbound)

- Sample Submissions
- SMTP (outbound connection to the configured mail server)
- Recovery Mode Support Session (outbound)
- SSH (in for tgsh-dialog)
- Syslog (outbound to configured syslog server)
- ESA/WSA – CSA Integrations
- FireAMP Private Cloud Integration
- DNS – Optional.

Dirty Interface

- Connect to the Dirty network. Requires Internet access. **Outbound Only!**
- DNS.
  Note: If you are setting up an integration with a FireAMP Private Cloud, and the FireAMP 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

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 APPENDIX A – CIMC CONFIGURATION (RECOMMENDED).

Reserved Interface

The non-Admin SFP+ port is reserved for future use.

Login Names and Passwords - Defaults

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 *Threat Grid Appliance Administrator's Guide*.

CIMC (Cisco Integrated Management Controller)

Login: admin

Password: "password"

Setup and Configuration Steps Outline

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

Server Setup.

Network Interface Connections Setup:

- Admin
- Clean
- Dirty

Initial Network Configuration - TGSH Dialog.

Main Configuration – OpAdmin Portal.

Install Updates.

Test the Appliance setup: Submit a Sample for Analysis.

Admin Configuration – Complete the remaining administrative configuration tasks (license installation, email server, SSL Certificates, etc.) in the OpAdmin Portal as documented in the *Threat Grid Appliance Administrator's Guide*.

Time Required for Setup and Configuration

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

Note: Please be patient during the "Apply" sections of the TGSH Dialog during the initial Appliance configuration installation steps

These steps can sometimes take more than 10 minutes to complete.

SERVER SETUP

To begin, connect both power supplies on the back of your appliance and 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 the figure below.

If CIMC is configured, you can use a remote KVM. For CIMC configuration see **Configuring CIMC (Optional)** in the *Appendix*.

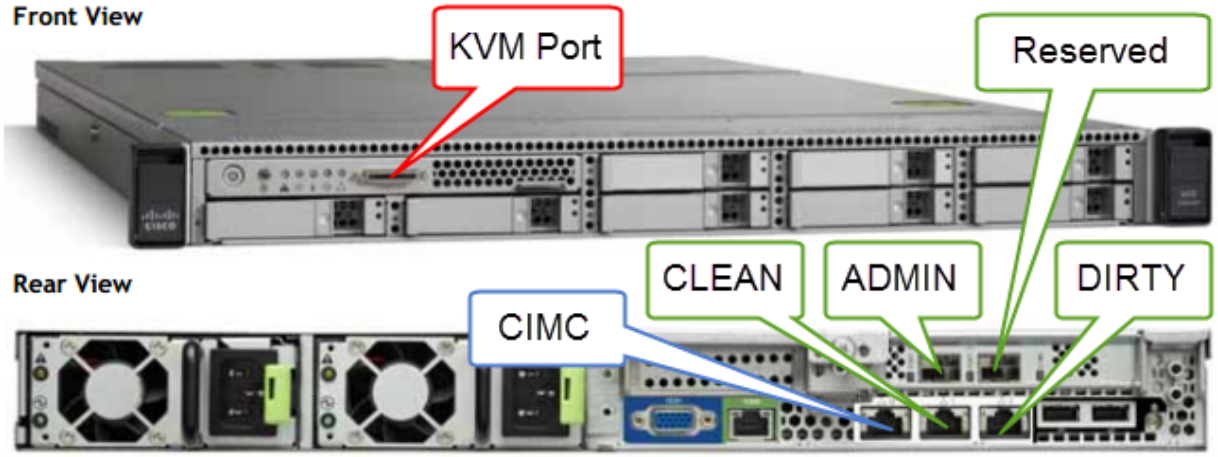
Please refer to the server product documentation for detailed hardware and environmental setup information. Links to product documentation are provided in the Hardware Documentation section, above.

Network Interface Connections Setup

Find the SFP+ ports (there are two) and the three Ethernet ports on the back of the appliance and attach the network cables as illustrated below:

C220 M3 Rack Server Setup

Figure 3 - Cisco UCS C220 M3 SFF Rack Server



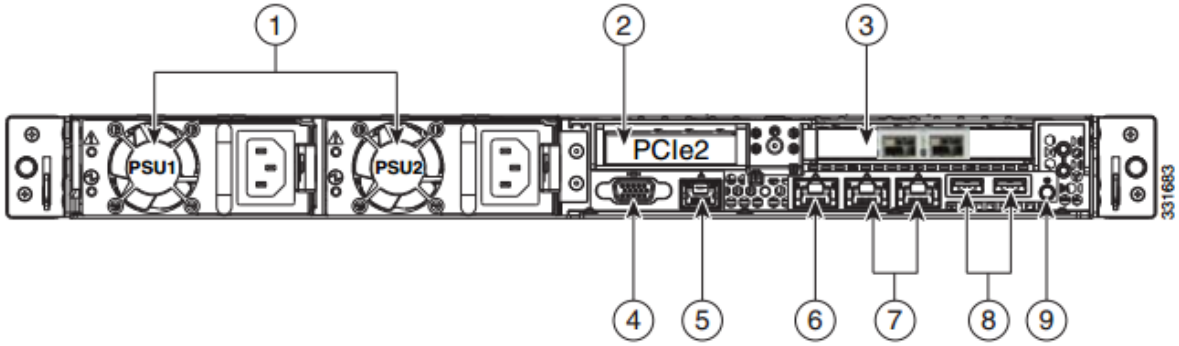
The interfaces must be properly connected and configured for the appliance to operate.

Note: The details of your appliance may differ from the image above. Please contact **support@threatgrid.com** if you have any questions.

Note: "Reserved" is the non-Admin SFP+ port, which is reserved for future use.

See the diagram below for more information about the C220 M3 server.

Figure 4 - Cisco UCS C220 M3 Rear View Details

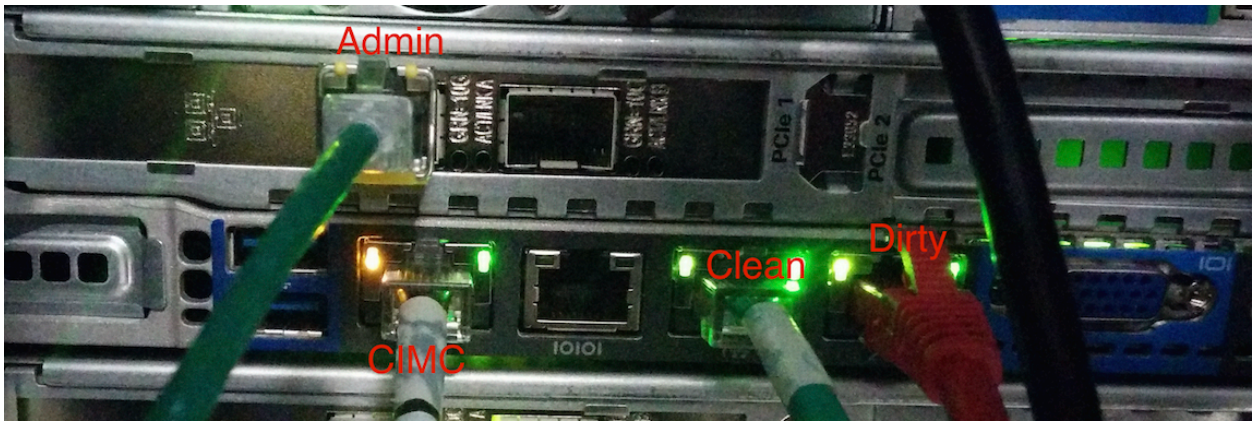


1	Power supplies (up to two)	6	One 10/100/1000 Ethernet dedicated management port
2	Slot 2: Low-profile PCIe slot on riser: (half-height, half-length, x16 connector, x8 lane width)	7	Dual 1-GbE ports (LAN1 and LAN2)
3	Two SFP+ Ports. Slot 1: Admin Slot 2: Reserved for backup and storage support.	8	USB ports
4	VGA video connector	9	Rear Identification button/LED
5	Serial port (RJ-45 connector)[1]	–	–

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 needs to be plugged in at boot time post 1.3. The network cable plugged into the SFP may be hot-plugged safely.

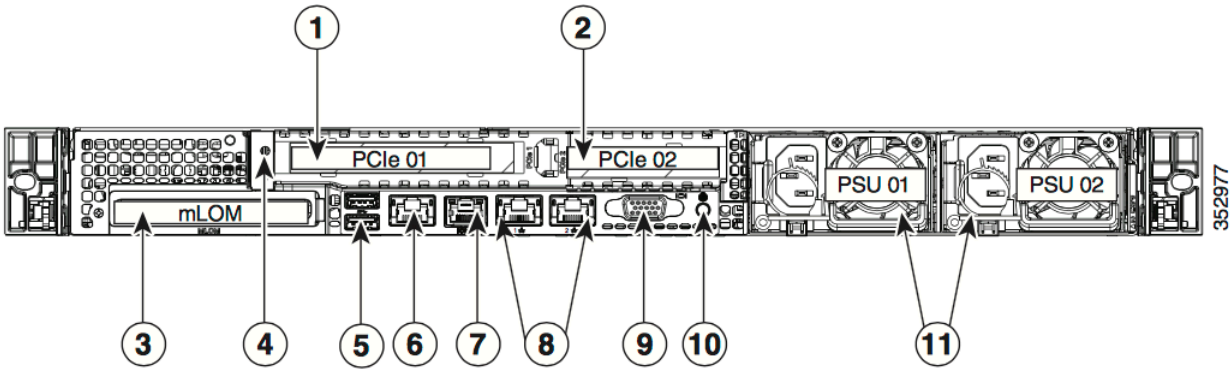
C220 M4 Rack Server Setup

Figure 5 - Cisco UCS C220 M4 SFF Rack Server



Note: The details of your appliance may differ from the image above. Please contact **support@threatgrid.com** if you have any questions.

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

8 (left) Clean

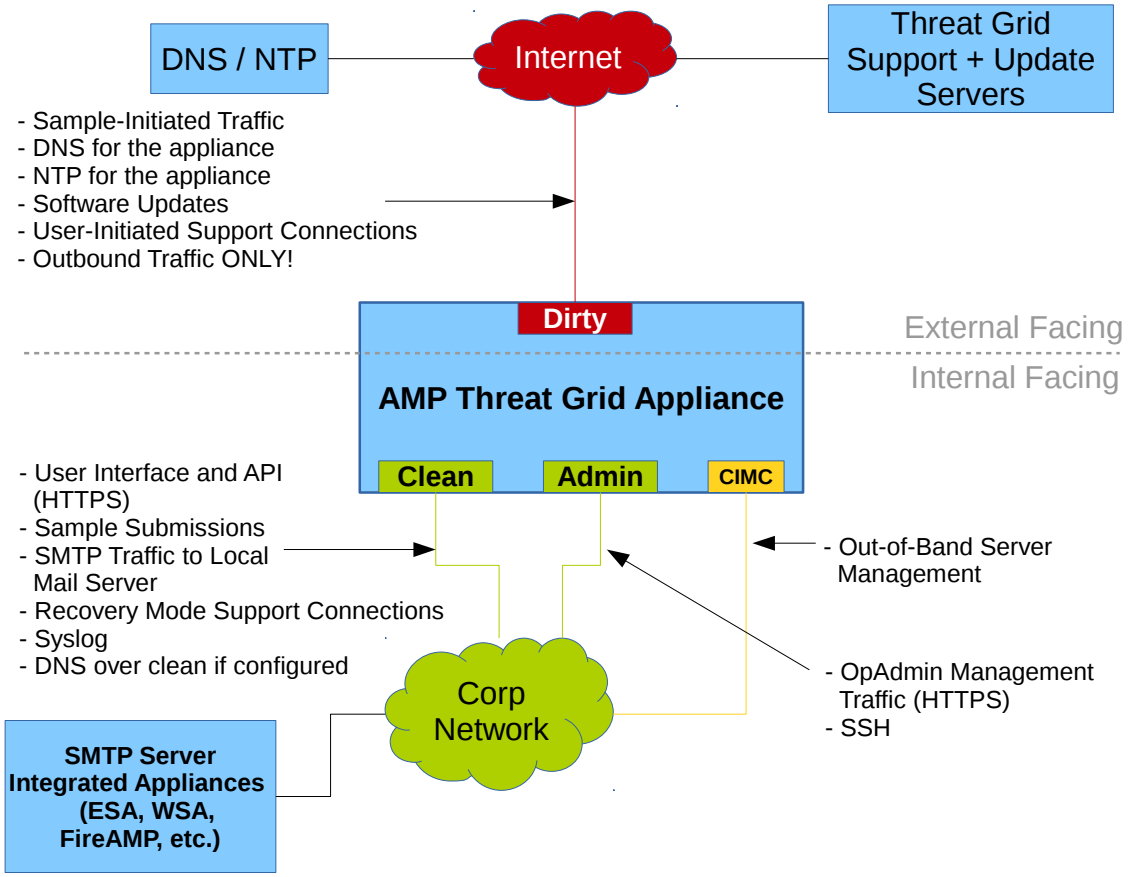
8 (right) Dirty

6 CIMC

Network Interface Setup Diagram

This section describes the most logical/recommended setup for an AMP Threat Grid Appliance. However, each customer's interface setup is different. Depending on your network requirements, you may well 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



Firewall Rules Suggestions

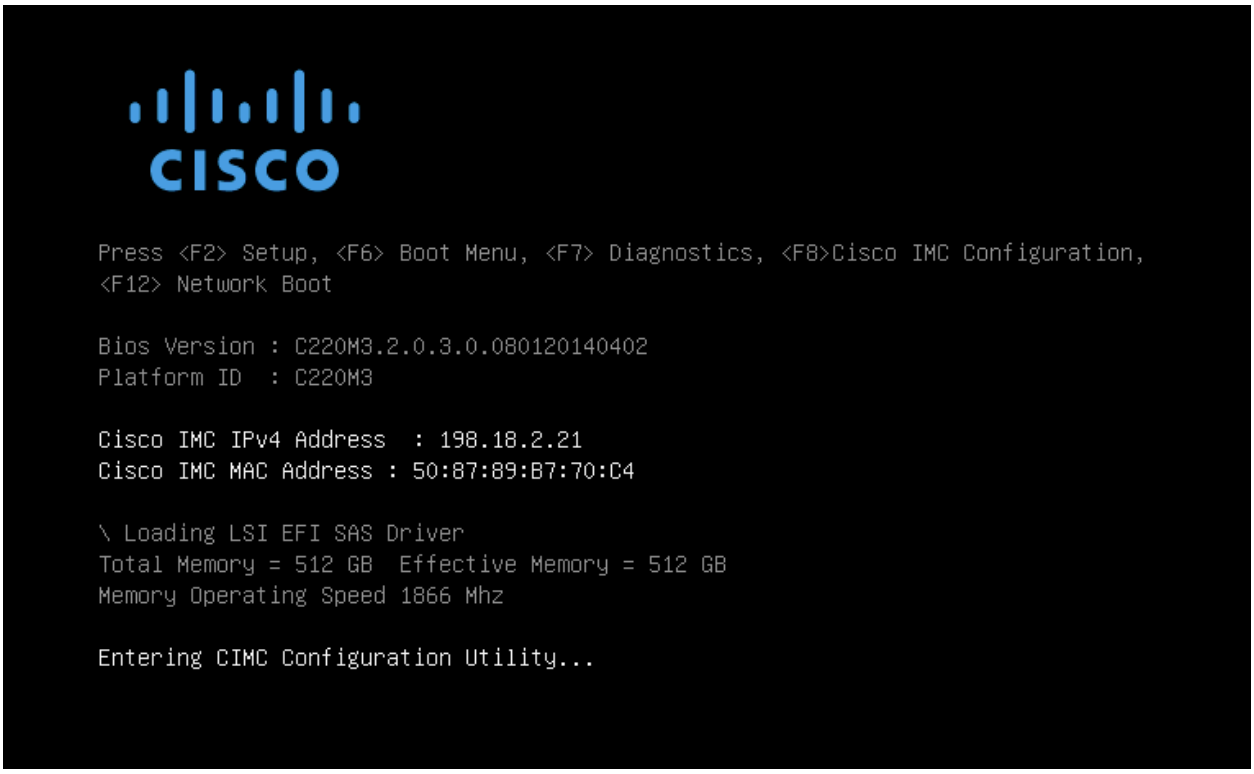
From	To	Protocol/Port	Action	Reason
Dirty interface	Internet	SMTP	Deny	Prevent malware from spamming
Dirty interface	Internet	TCP/19791	Allow	Allow connectivity to Threat Grid support
Dirty Interface	Internet	TCP/22	Allow	Update and support snapshot services
Dirty interface	Internet	IP/ANY	Allow	Allow outbound traffic from malware samples (To get accurate results it is required that malware be allowed to contact its command and control server.)
Dirty interface	Internet	DNS	Allow	Allow outbound DNS.
Dirty interface	Internet	NTP (UDP/123)	Allow	Allow outbound traffic to access NTP.
Clean interface	SMTP Server	SMTP	Allow	The appliance uses the clean interface to initiate SMTP connections to the configured mail server. (The Clean interface does not need outbound connectivity "to the Internet".)
Clean interface	Internet	TCP/19791	Allow	Allow connectivity to Thread Grid Recovery Mode support connections
User network	Clean interface	TCP/80 TCP/443	Allow	Appliance API and user interface
Clean interface	User network	Syslog/Configurable	Allow	Allow connectivity to server designated to receive Syslog messages and Threat Grid notifications.
Administration network	Admin interface	TCP/22 TCP/80 TCP/443	Allow	SSH OpAdmin Portal interface
User network	Clean interface	TCP/9443	Allow	Allow connectivity to the Threat Grid UI Glovebox

From	To	Protocol/Port	Action	Reason
Clean interface	Corporate DNS server	UDP/53 and TCP/53	Allow	Optional, only required if Clean DNS is configured
Clean interface	FireAMP Private Cloud	TCP/443	Allow	Optional, only required if FireAMP Private Cloud integration is used

Power On and Boot Up

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

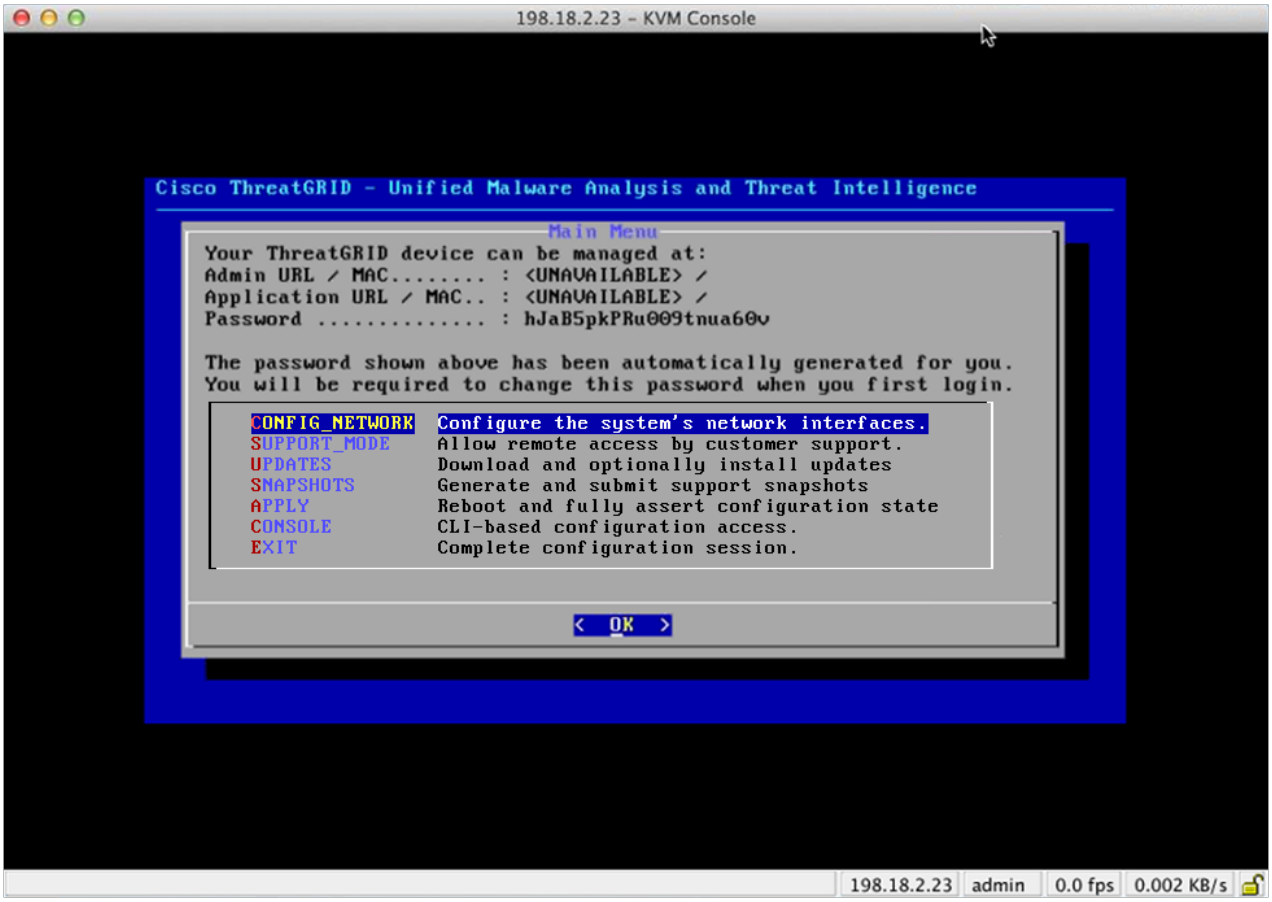
Figure 8 - Cisco Screen During Boot Up



Note: If you want to configure this interface, press **F8** after the memory check is completed, and follow the instructions provided in the section, *CONFIGURING CIMC (Optional)*.

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 - the network interface connections are not yet configured and the OpAdmin Portal cannot be reached yet to perform this task.

Note: Make a note of the administrator Password into a separate text file for convenience (copy-paste) during the OpAdmin Portal configuration steps.

IMPORTANT: The **TGSH Dialog** displays the initial administrator password, which will be needed in order to access and configure the OpAdmin Portal interface later in the configuration workflow steps.

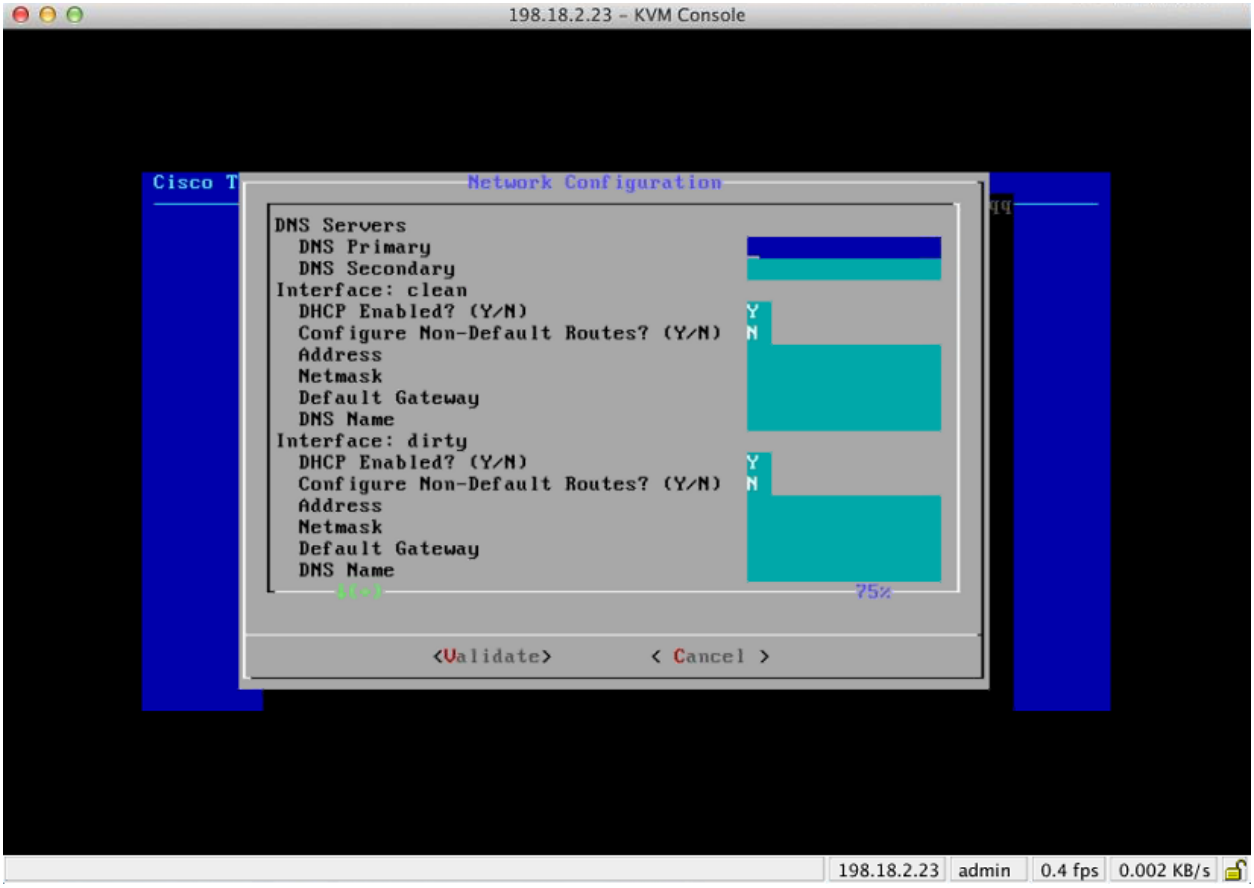
INITIAL NETWORK CONFIGURATION – TGSH DIALOG

The initial network configuration is completed in the TGSH Dialog. The goal is to complete the basic configuration that will allow access to the OpAdmin interface tool to finish the remaining configuration, including the license, email host, SSL Certificates, etc.

DHCP Users: The following steps assume that you are using static IP addresses. If you are using DHCP to obtain your IPs, then please see the *Threat Grid Appliance Administrator's Guide* for more information.

1. In the TGSH Dialog interface, select **CONFIG_NETWORK**. The Network Configuration console opens:

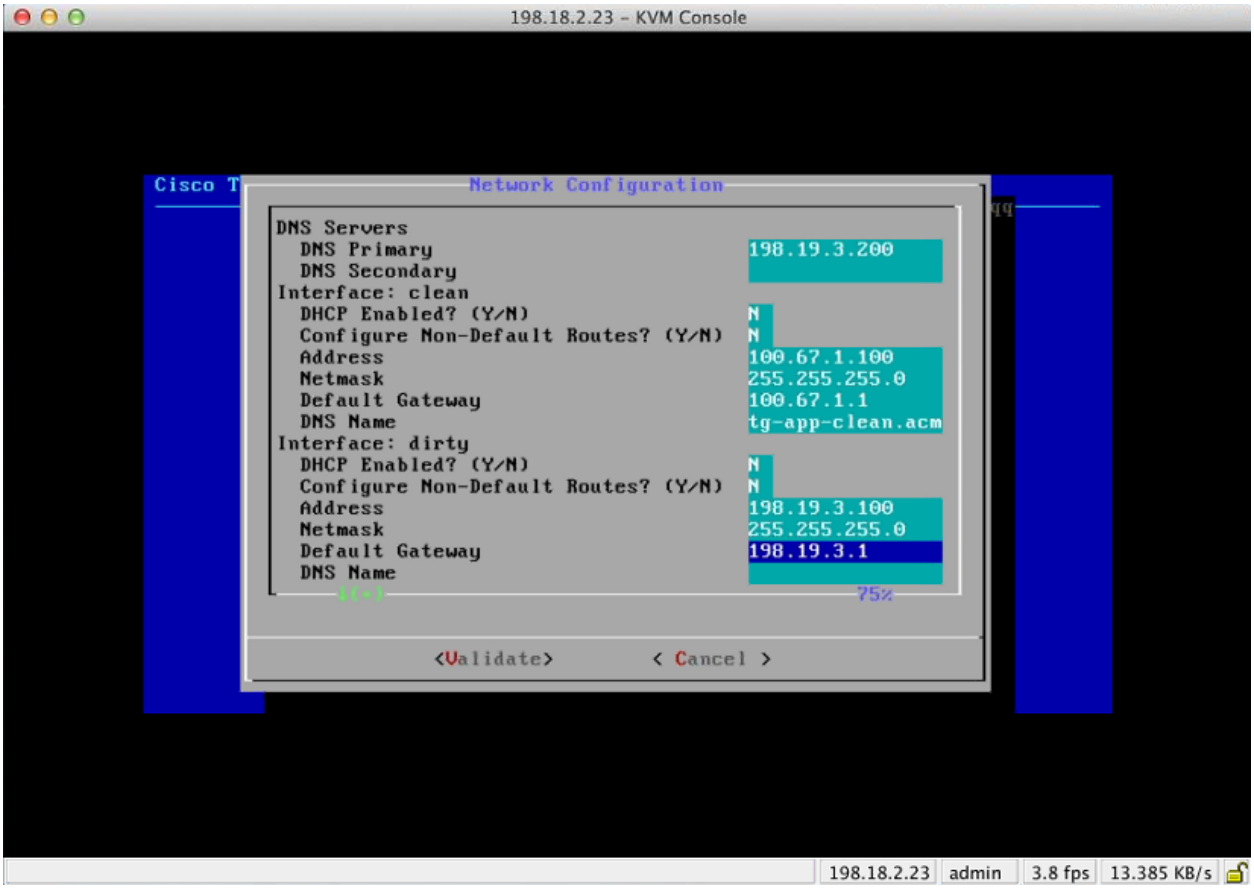
Figure 10 - TGSH Dialog - Network Configuration Console



2. Complete the blank fields according to the settings provided by your network administrator for the clean, dirty, and admin interfaces.
3. Change **DHCP Enabled** from **Y** to **N**.

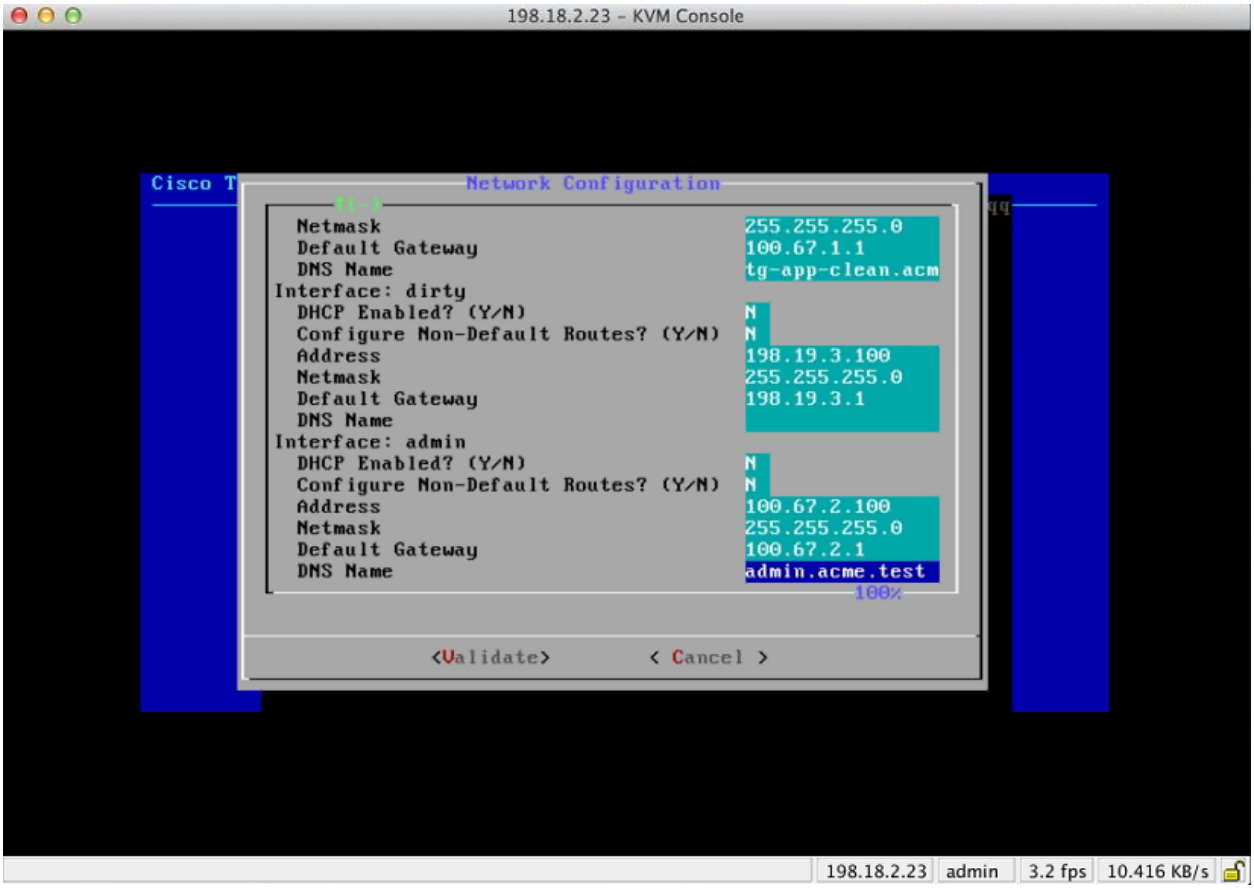
   Note: You need to **BACKSPACE** over the old character before you can enter the new one.
4. **DNS NAME.** If your network is using a DNS name for the clean network, then enter the name here.
5. Leave **Configure Non-Default Routes?** set to the default of **N** (unless additional routes are needed).

Figure 11 - Network Configuration In-Progress (clean and dirty)



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

Figure 12 - Network Configuration In-Progress (admin)

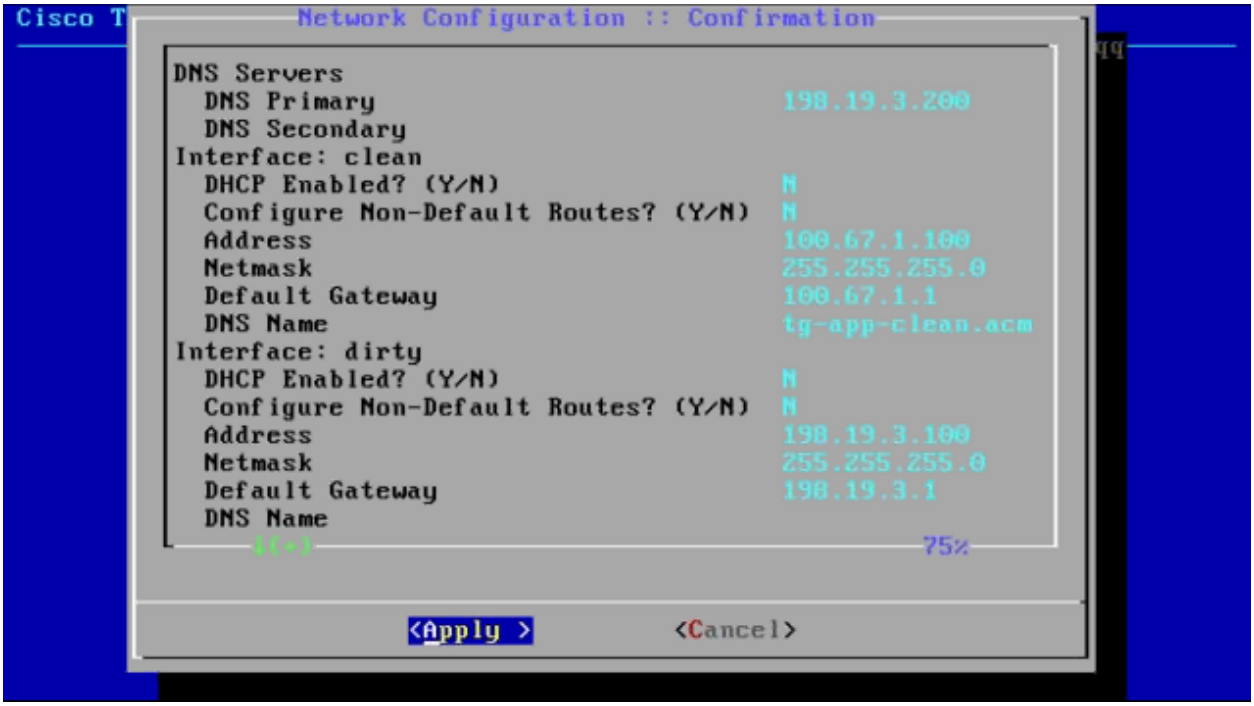


7. After you finish entering all the network settings, tab down and select **Validate** to validate your entries.

   If invalid values have been entered, you may see errors. If this is the case, then fix the errors and re-Validate.

   After validation, the Network Configuration Confirmation displays the values you've entered:

Figure 13 - Network Configuration Confirmation

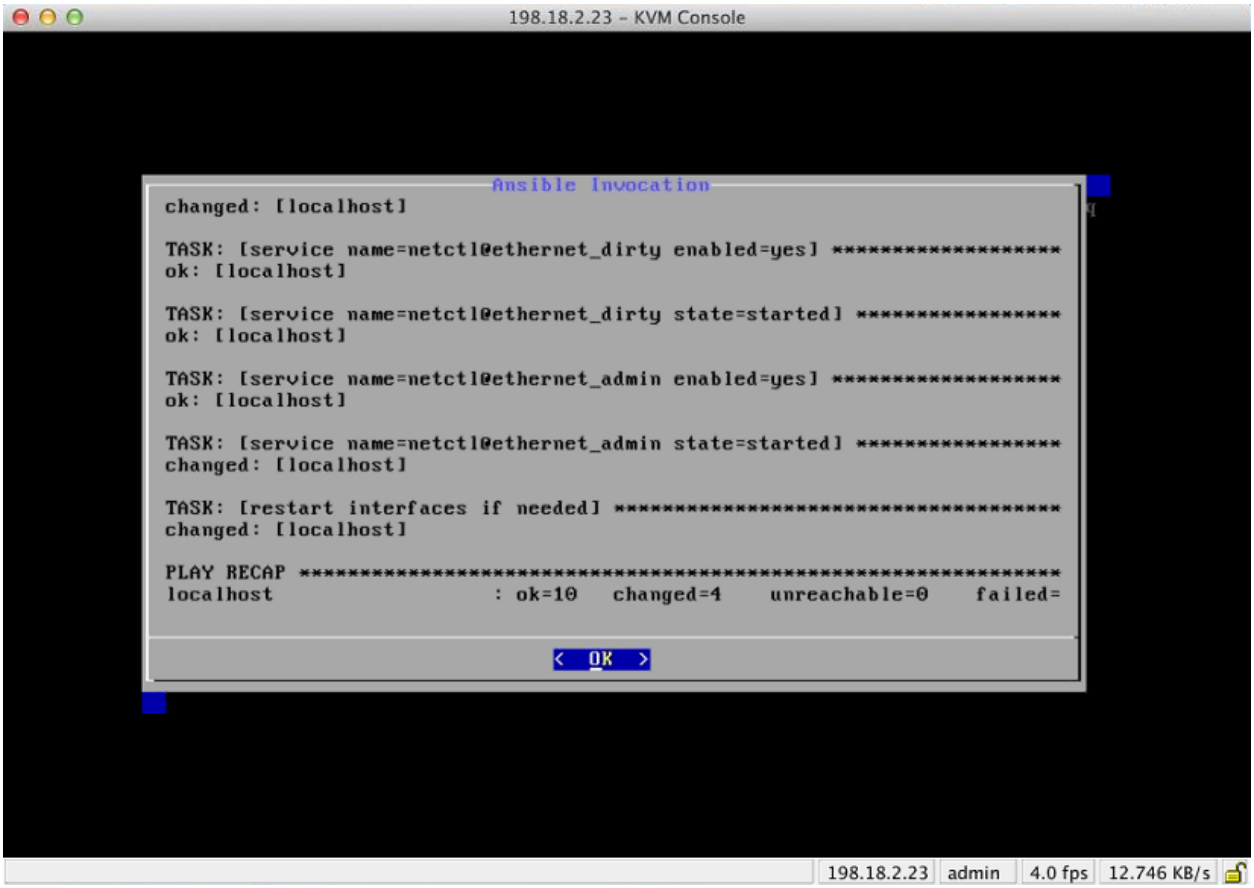


8. Select **Apply** to apply your configuration settings.

   Have patience. This step may take 10 minutes or more to complete.

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

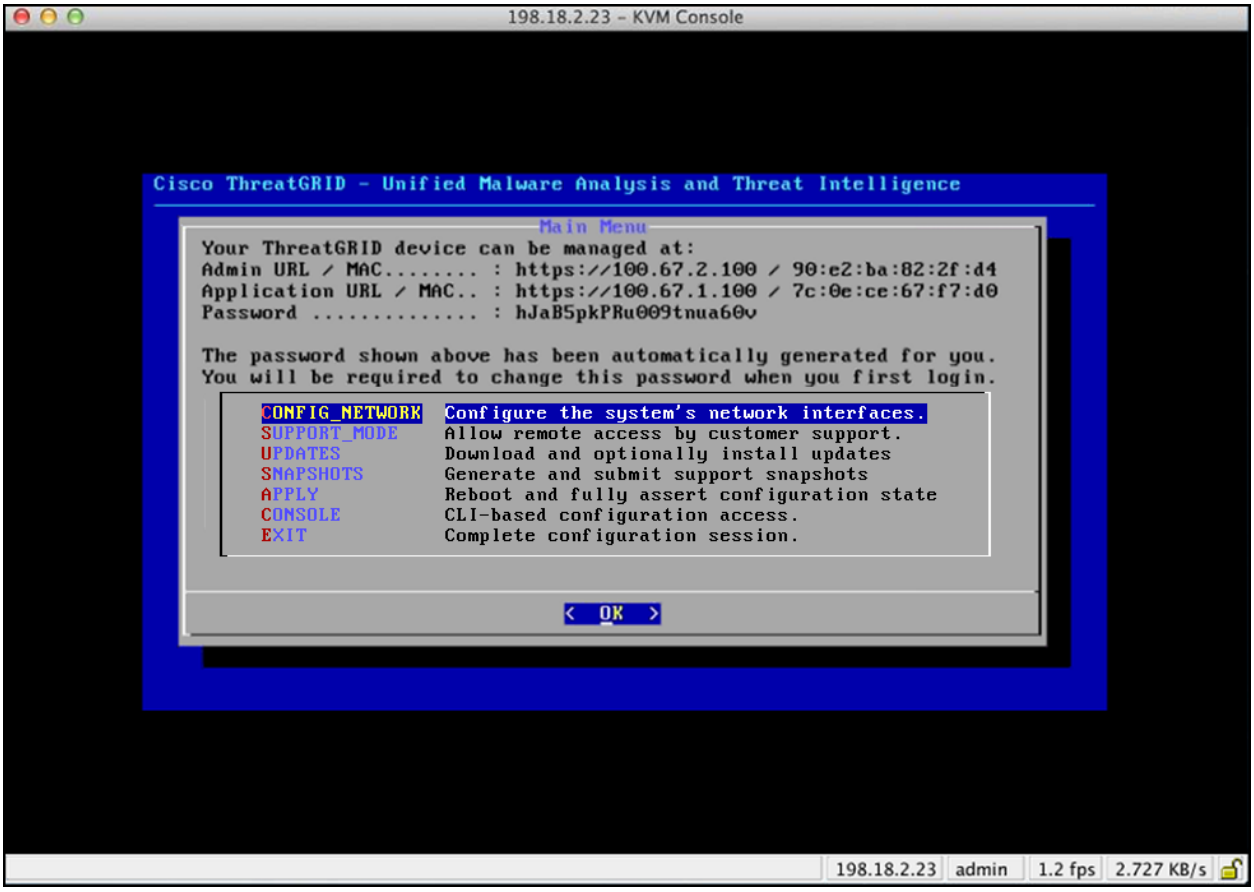
Figure 14 - Network Configuration - List of Changes Made



9. Select **OK**.

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

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.

Next Setup Step:

The next step in the appliance setup is to complete the remaining configuration tasks using the workflow in the OpAdmin portal, as described in the following section, OPADMIN PORTAL CONFIGURATION WIZARD.

CONFIGURATION WIZARD - OPADMIN PORTAL

The OpAdmin Portal is the Threat Grid administrator's portal on the appliance. It is a Web user interface that can be used once an IP address has been configured on the Admin interface.

The OpAdmin Portal is the recommended tool for configuring your appliance, and in fact, much of the appliance configuration can only be done via the OpAdmin portal interface, including:

- OpAdmin Portal administrator's password
- Email servers
- DNS servers
- NTP servers
- SSL Certificates
- Other server settings
- https://<adminIP>/ OR https://<adminHostname>/

Note: Not all of these settings are completed in the initial OpAdmin portal configuration wizard workflow. Some, such as SSL Certificates, are configured in separate steps, as described in the *Threat Grid Appliance Administrator's Guide*.

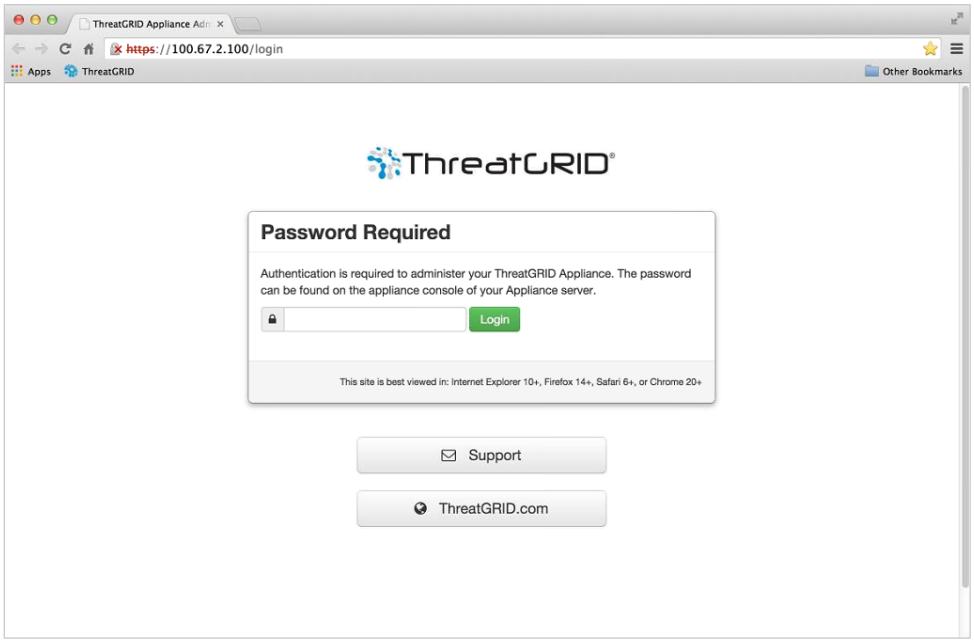
Configuration Workflow

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.

Login to the OpAdmin Portal

1. Point your browser at the OpAdmin Portal interface (the Admin URL with the "https"). The Threat Grid OpAdmin login screen opens:

Figure 16 - OpAdmin Login



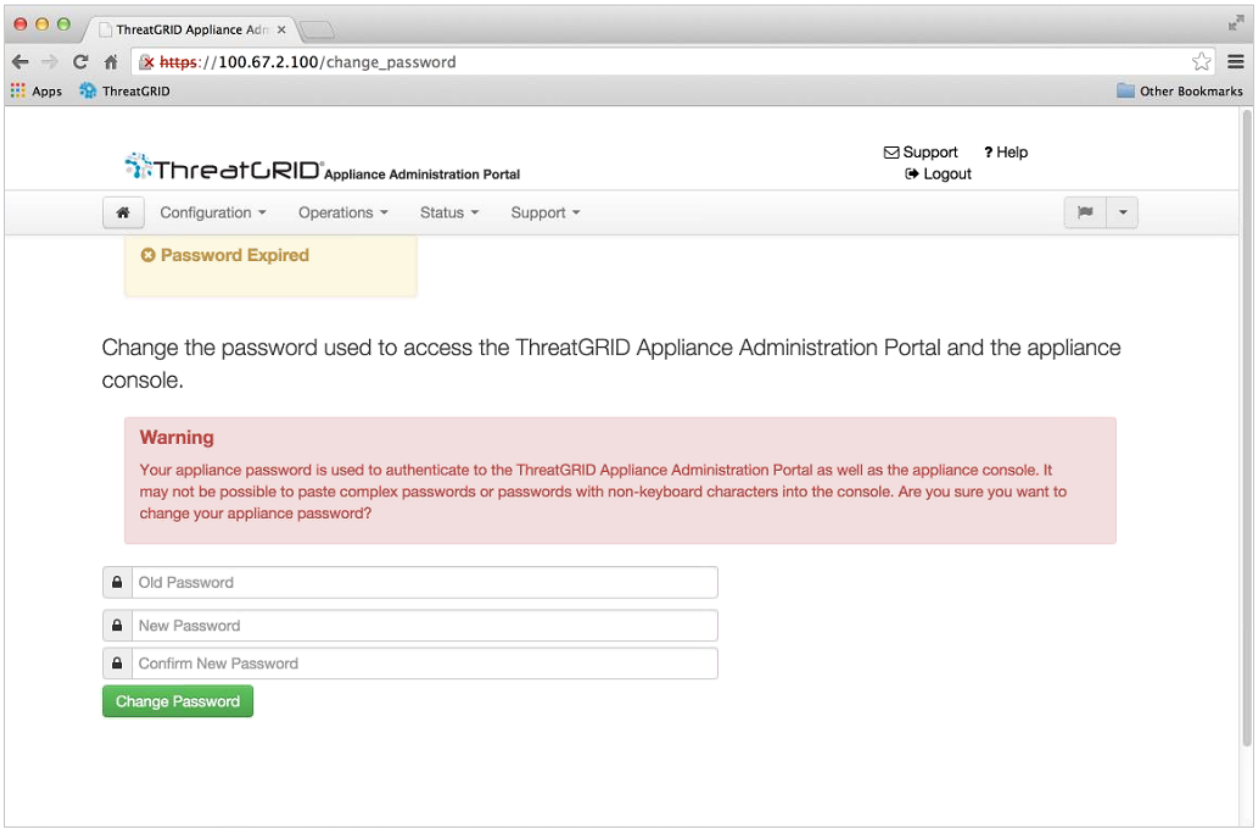
2. Enter the default Admin Password that you copied from the TGSH Dialog and click **Login**. The *Change Password* page opens.

Continue with the next section:

Admin Password Change

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 you may continue with the configuration workflow.

Figure 17 - OpAdmin Change Password



1. Enter the password from the TGSH Dialog into the **Old Password** field. (You should have this in a text file for use at this moment.)
2. Enter and confirm a new password.
3. Click **Change Password**.

   The password is updated. The *End User License Agreement* page opens.

   Note: The new password will NOT be displayed in visible text in the TGSH Dialog, so be sure to note it down somewhere.

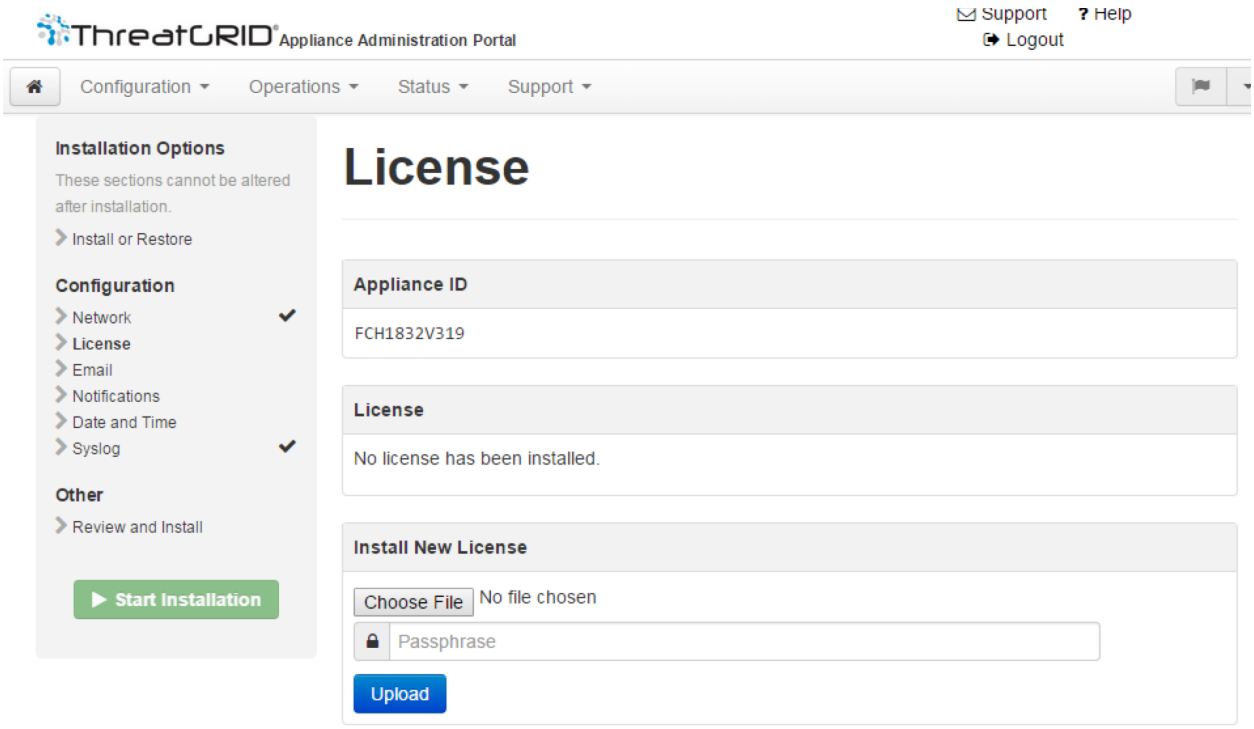
   If you lose the password, follow the **Lost Password** instructions located in the *Support* section of the *Threat Grid Appliance Administrator's Guide*.

Continue with the next section:

End User License Agreement

1. Review the End User License Agreement.
2. Scroll down to the end, and click **I HAVE READ AND AGREE**. The *License* page opens:

Figure 18 - License Page



We recommend that you follow the configuration workflow, and *configure the networks before you install the license*, as described in the next section, Network Configuration Settings.

Network Configuration Settings

If you configured your static network settings in the TGSH Dialog, the IP addresses displayed in the Network Configuration page will reflect the values you entered in the TGSH Dialog during the appliance network configuration.

Network Configuration and DHCP

If you used DHCP for your initial connection and now need to change the Clean and Dirty IP networks to static IP addresses, then follow the steps in the section: ***Networking > Using DHCP***, located in the *Threat Grid Appliance Administrator's Guide*.

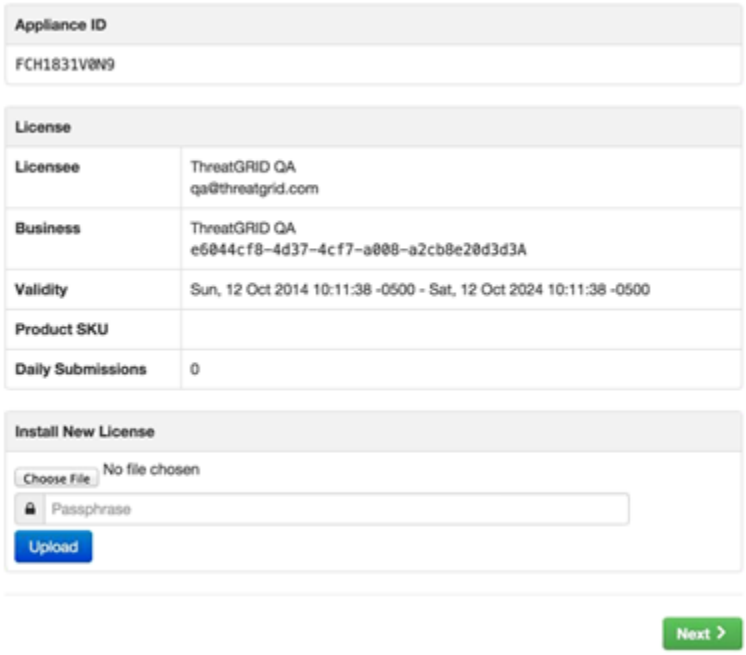
Continue with the next section:

License Installation

After the networks are configured, you are ready to install the Threat Grid license. (In versions older than v1.4.4, you will need to start Support Mode in order for your license to be accepted. See Start Support Mode - License Workaround Prior to Version 1.4.4 for more information.

1. Click on **License** in the left column. The *License* page opens. No license has been installed.
2. Under **Install New License**, click **Browse**, and select the license from your file manager.
3. Enter the license password you were given into the Passphrase field.
4. Click **Upload** to install. The page refreshes, and you should see your license information:

Figure 19 - License Information After Successful Installation



5. Click **Next** to continue. The *Email* page opens.

Continue with the next section:

Email Host Configuration

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

1. Click on **Email** in the left column. The *Email* page opens.
2. Enter the name of the **Upstream Host** (email host).
3. Change the port from 587 to **25**.

4. Leave the other settings at the defaults.
5. Click **Next**. The *Notifications* page opens.

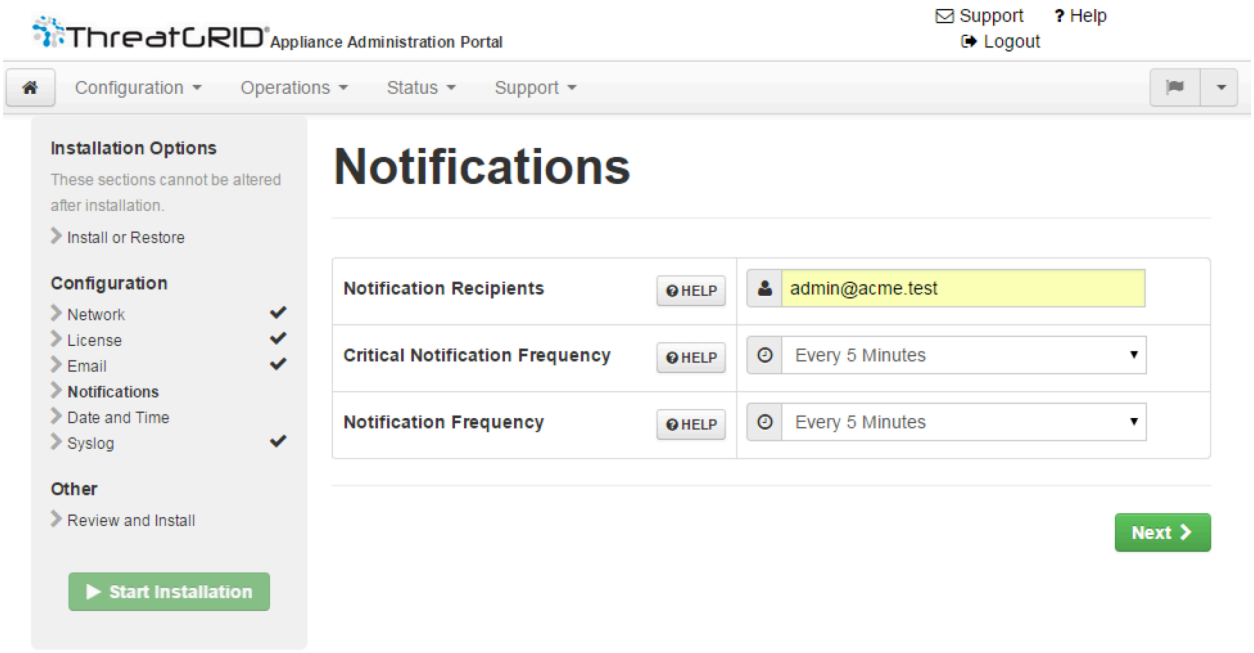
Continue with the next section:

Server Notifications Configuration

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.

Note: Update v1.3 includes a page to configure a Syslog server to receive syslog messages and Thread Grid notifications. See the *Threat Grid Appliance Admin Guide* for more information.

Figure 20 - Notifications Configuration



1. First, set the **Critical Notification Frequency** and the **Notification Frequency** by selecting them from the dropdown lists.
2. Next, in **Notification Recipients**, enter one or more email addresses separated by commas.
3. Click **Next**. The *Date and Time* page opens.

Continue with the next section:

NTP Server Configuration

This is where you identify the NTP ("Network Time Protocol") servers.

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

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

2. Ignore Current System Time and Synchronize with Browser.

3. Click **Next**.

   The *Review and Install* page opens with checkboxes next to all of the Configuration steps.

Continue with the next section:

Review and Install Configuration Settings

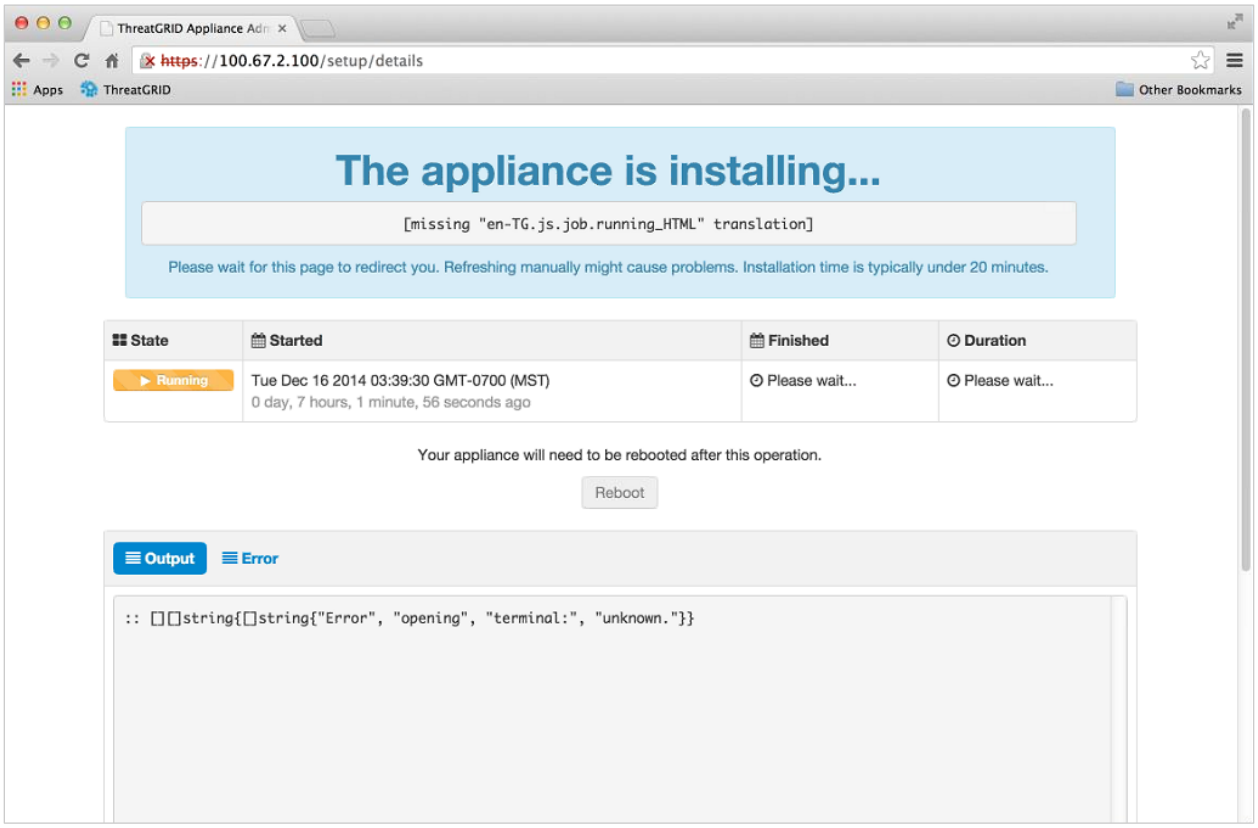
Now that you have entered your network configuration settings, you must install them as described below.

1. In the *Review and Install* page, click **Start Installation**.

   Configuration scripts are installed and you see the message: "*The appliance is installing...*".

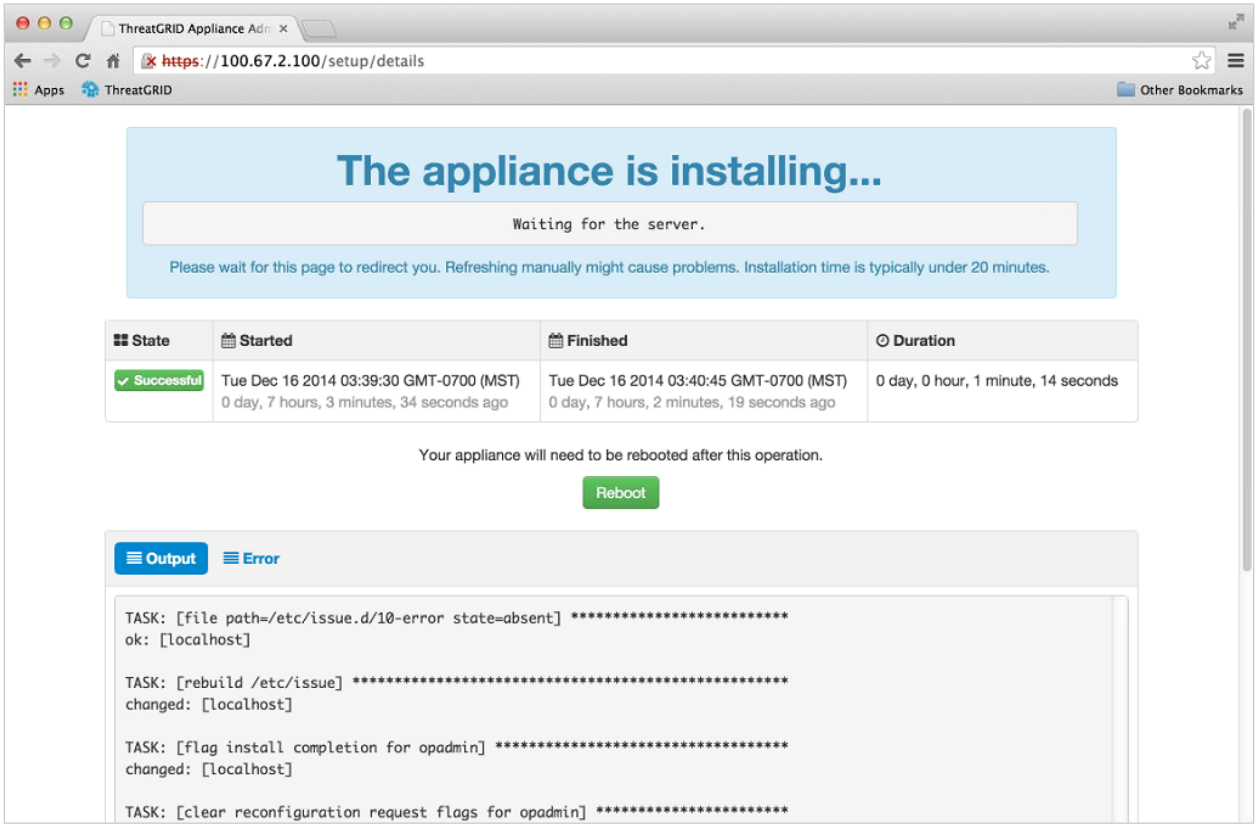
Note: Have patience. Please allow 10+ minutes for this step to complete. The screen will display configuration information as it is applied.

Figure 21 - Appliance is Installing



2. After successful installation, the State changes from the orange **Running** to a green **Successful** message confirming success. The **Reboot** button changes to green, and the configuration output is displayed:

Figure 22 - Successful Appliance Installation

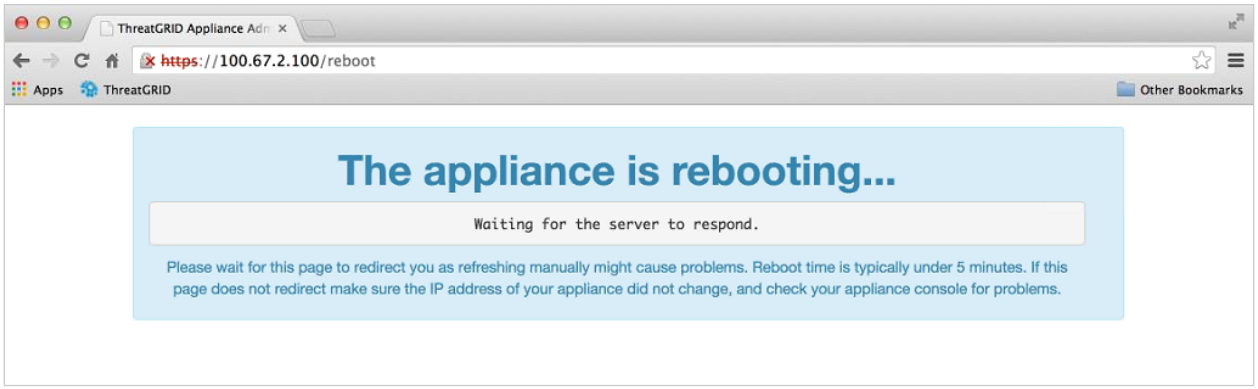


3. Click **Reboot** after the successful installation. You will see the message that "*The appliance is rebooting*".

   Rebooting may take up to 5 minutes.

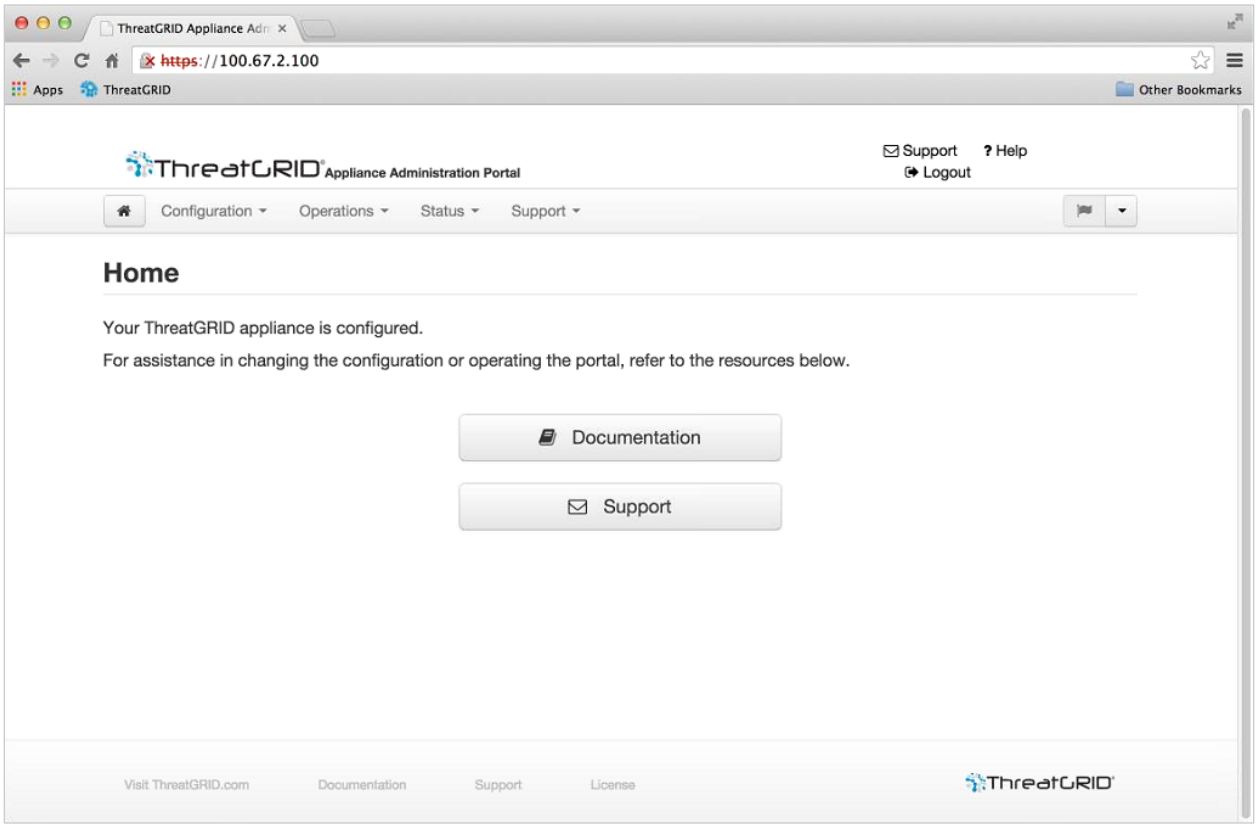
Please do not make any changes while the Appliance is rebooting.

Figure 23 - Appliance is Rebooting



Once the appliance has successfully rebooted, you will see the following confirmation that the Appliance is configured:

Figure 24 - Appliance Is Configured



Your appliance is now setup and the initial configuration is complete.

INSTALLING 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.

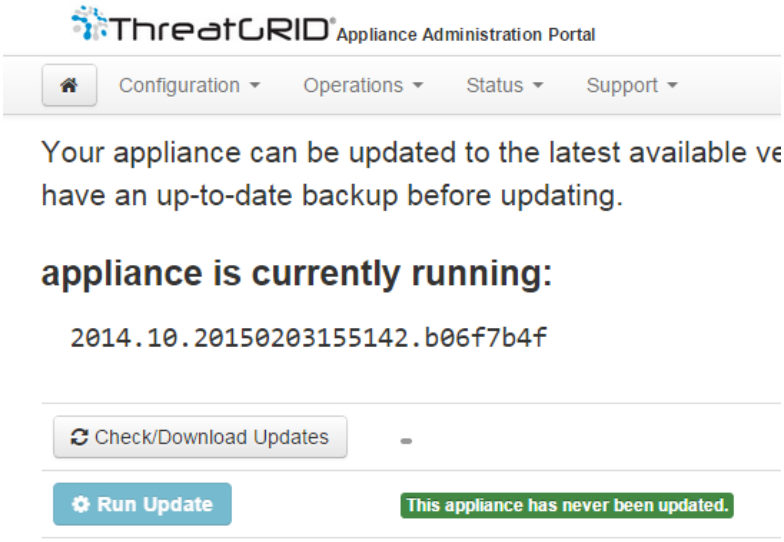
1. From the **Operations** menu, select **Update Appliance**. The updates page opens, displaying the current build of the appliance.
2. Click **Check/Download Updates**. The software checks to see if there is a more recent update/version of the Threat Grid Appliance software, and if so, it is downloaded. This may take some time.
3. Once the updates have been downloaded, click **Run Update** to install them.

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

Appliance Build Number

The build number of an appliance can be viewed on the Updates page: OpAdmin **Operations** > **Update Appliance**:

Figure 25 - Appliance Build Number



Appliance Build Number/Version Lookup Table

The build number of an Appliance can be viewed on the Updates page (OpAdmin **Operations** > **Update Appliance**), as illustrated above. Appliance build numbers correspond to the following version numbers:

Build Number	Release Version	Release Date	Notes
2016.05.20160905202824.f7792890.rel	2.1.4	9/5/2016	Primarily of interest to Manufacturing
2016.05.20160811044721.6af0fa61.rel	2.1.3	8/11/2016	Offline update support key, M4 wipe support
2016.05.20160715165510.baed88a3.rel	2.1.2	7/15/2016	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	7/6/2016	
2016.05.20160621044600.092b23fc	2.1	6/21/2016	
2015.08.20160501161850.56631ccd	2.0.4	5/1/2016	Starting point for the 2.1 update. You must be at 2.0.4 before you can update to 2.1.
2015.08.20160315165529.599f2056	2.0.3	3/15/2016	Introduces AMP integration, CA mgmt., and split DNS
2015.08.20160217173404.ec264f73	2.0.2	2/18/2016	
2015.08.20160211192648.7e3d2e3a	2.0.1	2/12/2016	
2015.08.20160131061029.8b6bc1d6	2.0	2/11/2016	Force update to 2.0.1 from here
2014.10.20160115122111.1f09cb5f	1.4.6 **NOTE:** This is the starting point for the 2.0 upgrade.	1/27/2016	Starting point for the 2.0.4 update
2014.10.20151123133427.898f70c2	v1.4.5	11/25/2015	
2014.10.20151116154826.9af96403	v1.4.4		

Build Number	Release Version	Release Date	Notes
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1+hotfix1		
2014.10.20150203155142.b06f7b4f	v1.1		
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0+hotfix2 **NOTE:** The 1.0+hotfix2 is a mandatory update that fixes the update system itself to be able to handle large files without breaking.		
2014.10.20141125162158.8afc5e2f	v1.0		

Note: For release versions 1.0-1.2 a reboot may be needed if an interface was not plugged in at boot time. This is a pre-v1.3 issue, except for any interface requiring an SFP, which will still needs to be plugged in at boot time post v1.3. The network cable plugged into the SFP may be hot-plugged safely.

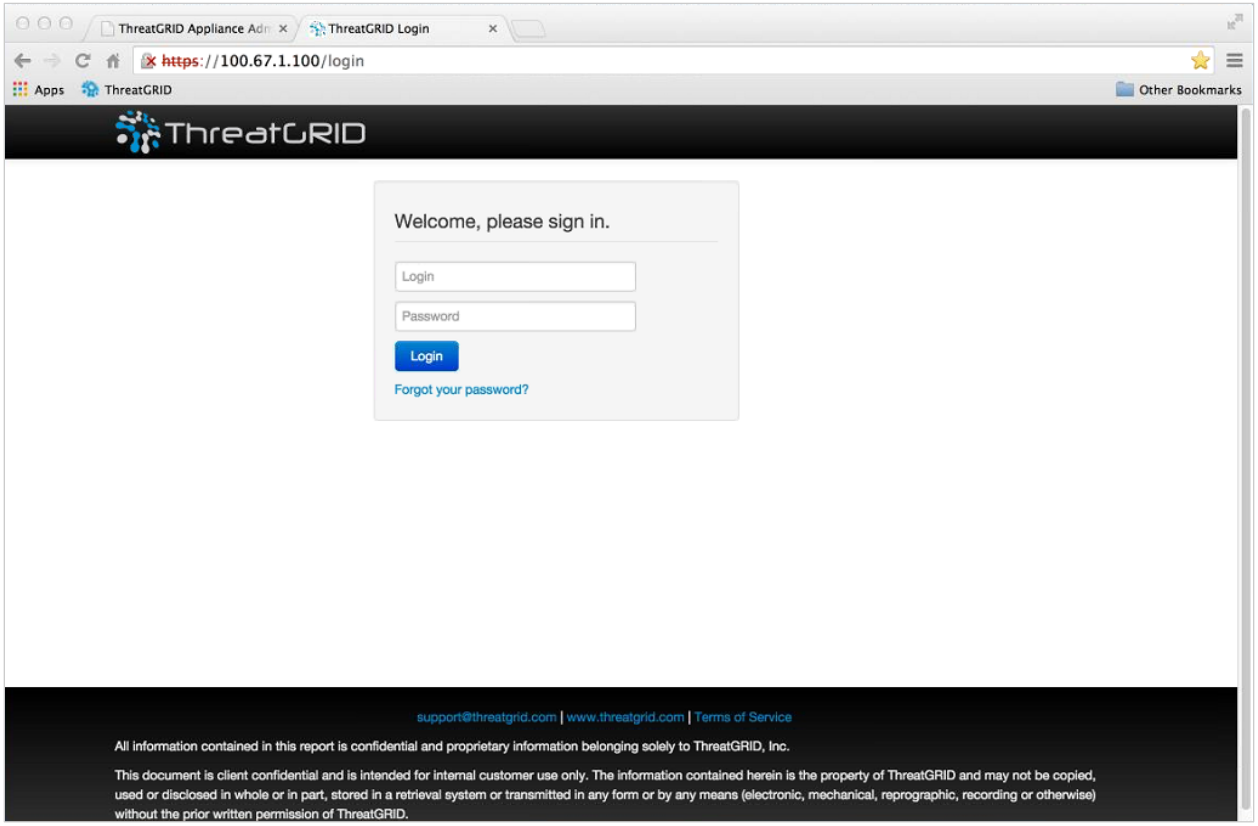
Note: Updating from 1.0 to 1.0+hotfix2 takes approximately 15 minutes. Applying a full update from 1.0 to 1.3 (without data migration) takes about 30 minutes.

TEST THE APPLIANCE SETUP - SUBMIT A SAMPLE

Once the Threat Grid Appliance is updated to the current version, the final test that your appliance has been configured properly is to submit a malware sample using the Threat Grid software.

1. Sign into the AMP Threat Grid Portal by visiting the address you configured as the Clean interface. The Threat Grid login page opens:

Figure 26 - Threat Grid Portal Login Page



2. Enter the default Login and Password: **admin/changeme**
3. Click **Login**. The main Threat Grid *Sample Analysis* page opens.
4. In the **Submit a Sample** box located in the upper-right corner, to select a sample file or enter *a URL* to submit for malware analysis.
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.

APPLIANCE ADMINISTRATION

Once the Threat Grid Appliance has been setup and initial configuration is completed, it is ready for the appliance administrator.

Release notes, Updates, SSL Certificates, adding users, and other administrator tasks and topics are documented in the *Threat Grid Appliance Administrator's Guide*.

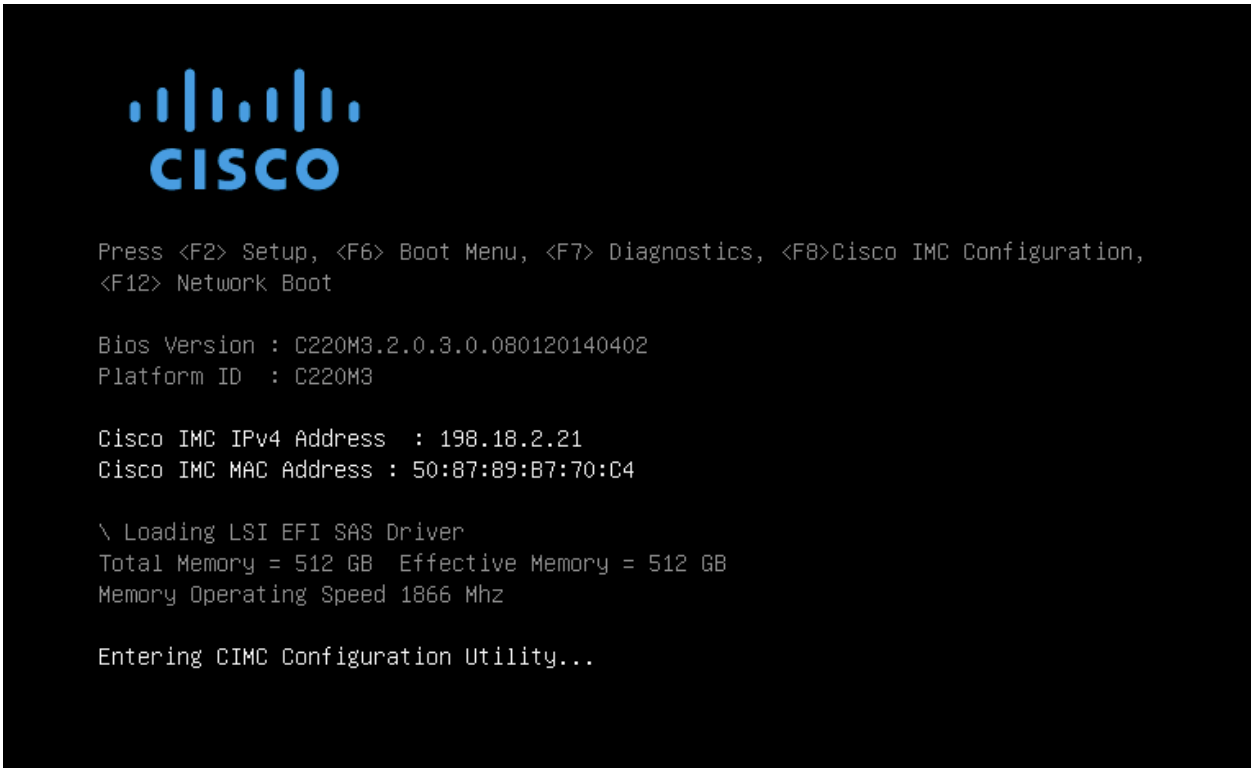
APPENDIX A – CIMC CONFIGURATION (RECOMMENDED)

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

You will need a monitor and keyboard attached directly to the appliance.

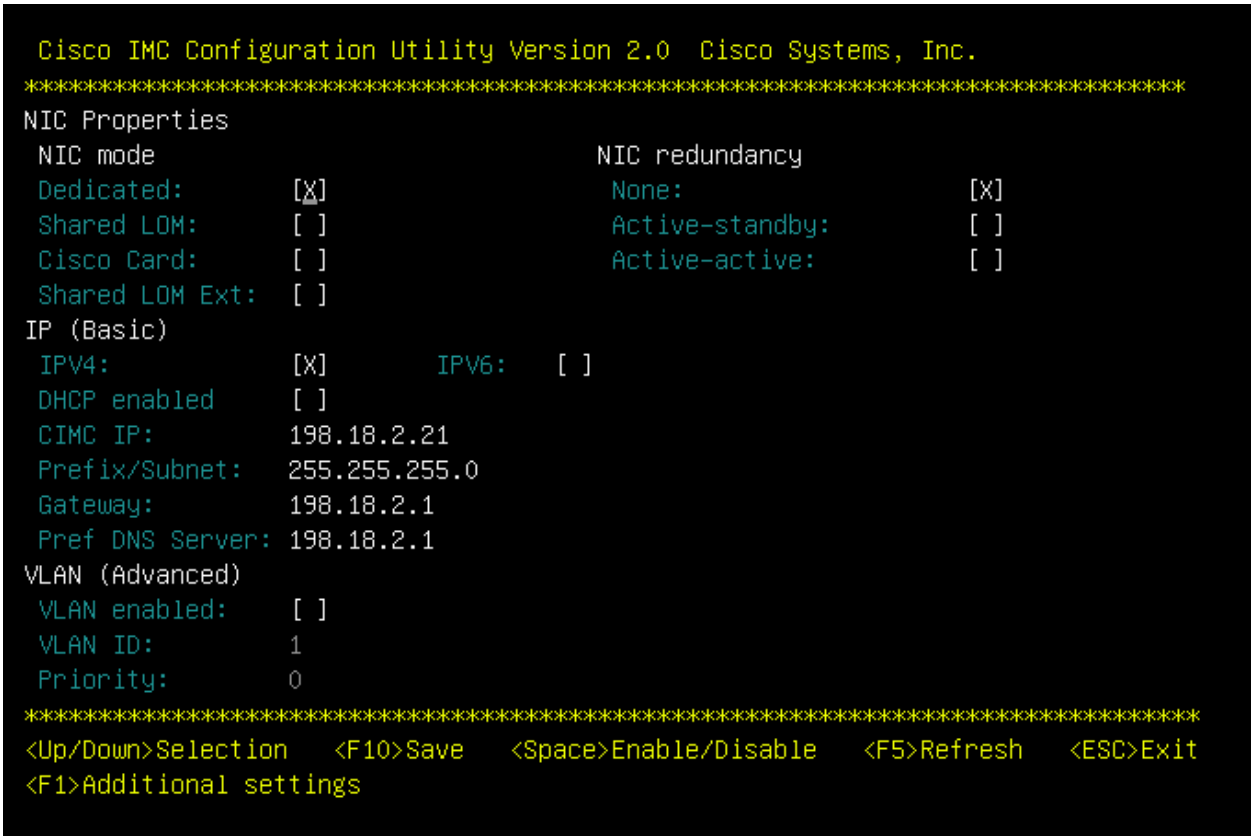
1. Power on the server. The Cisco screen opens:

Figure 27 - The Cisco screen – F8 to enter the CIMC Configuration Utility



2. After the memory check is completed press **F8** to enter the CIMC configuration utility:

Figure 28 - CIMC Configuration Utility

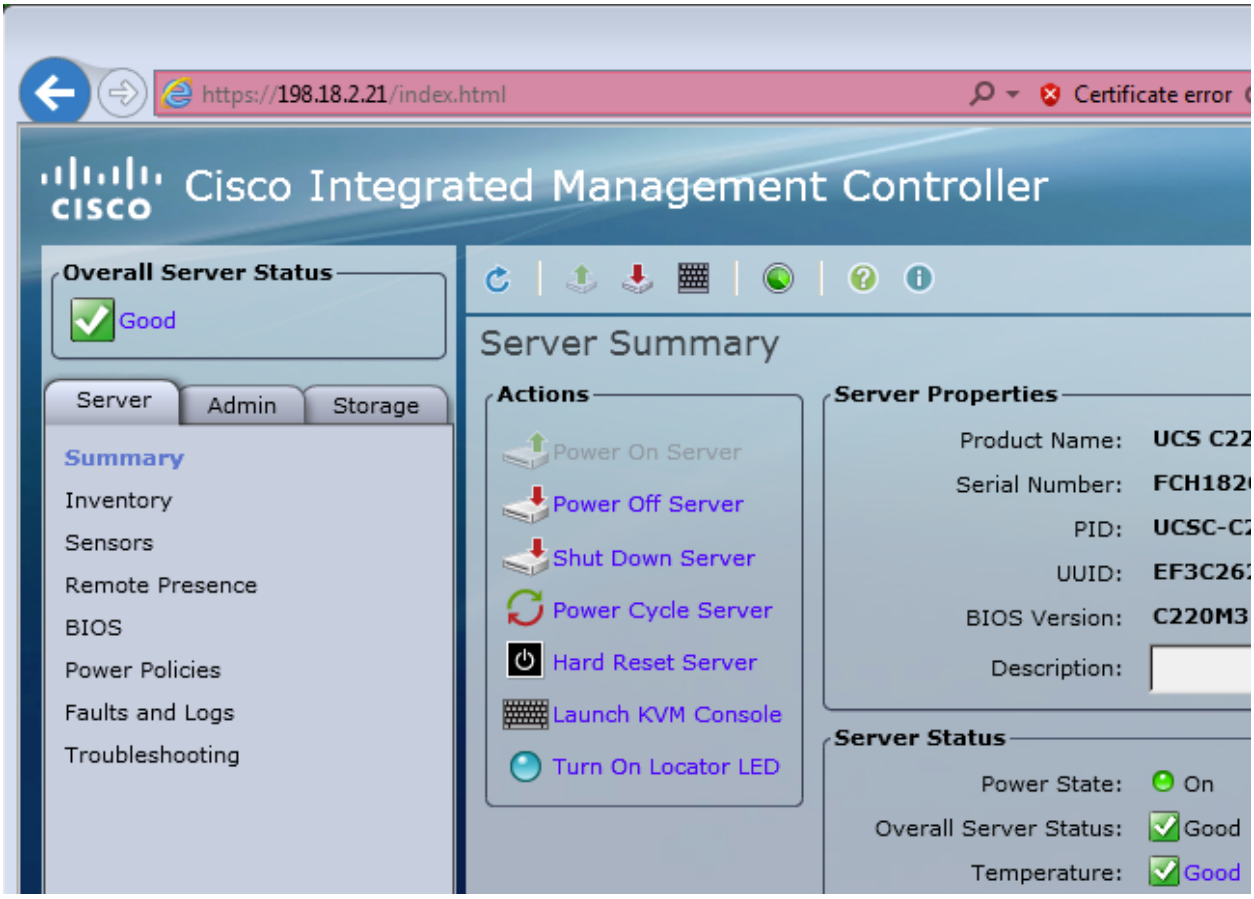


3. In the CIMC configuration utility, set up an IP address that will be used for remote server management.

4. When complete, Save, and then Exit.
   At this point the server can be managed remotely by using a Web browser to https://<*CIMC-IP address*>/

5. The initial user name is "**admin**", with a password of "**password**".

Figure 29 - Cisco Integrated Management Controller (CIMC) Interface



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