



Initial Network Configuration

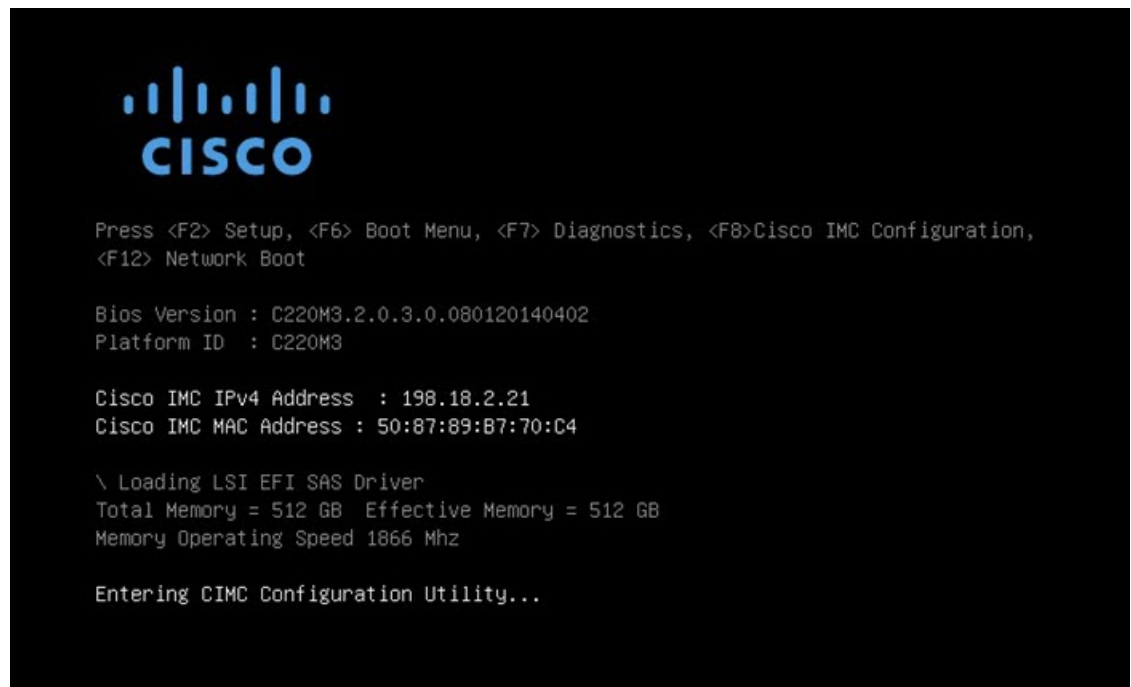
This chapter provides instructions for completing the initial network configuration using the TGS dialog. It includes the following topic:

- [Power On and Boot Up Appliance, on page 1](#)
- [Configure Network Using TGS Dialog, on page 2](#)

Power On and Boot Up Appliance

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

Figure 1: Cisco Screen During Bootup





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

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

Figure 2: TGSN Dialog

```

198.18.2.23 - KVM Console

Cisco ThreatGRID - Unified Malware Analysis and Threat Intelligence

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

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

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

< OK >

198.18.2.23 admin 0.0 fps 0.002 KB/s

```

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 **TGSN Dialog** displays the initial administrator Password, which will be needed to access and configure the OpAdmin Portal interface later in the configuration. Make a note of the Password in a separate text file (copy and paste).

Configure Network Using TGSN Dialog

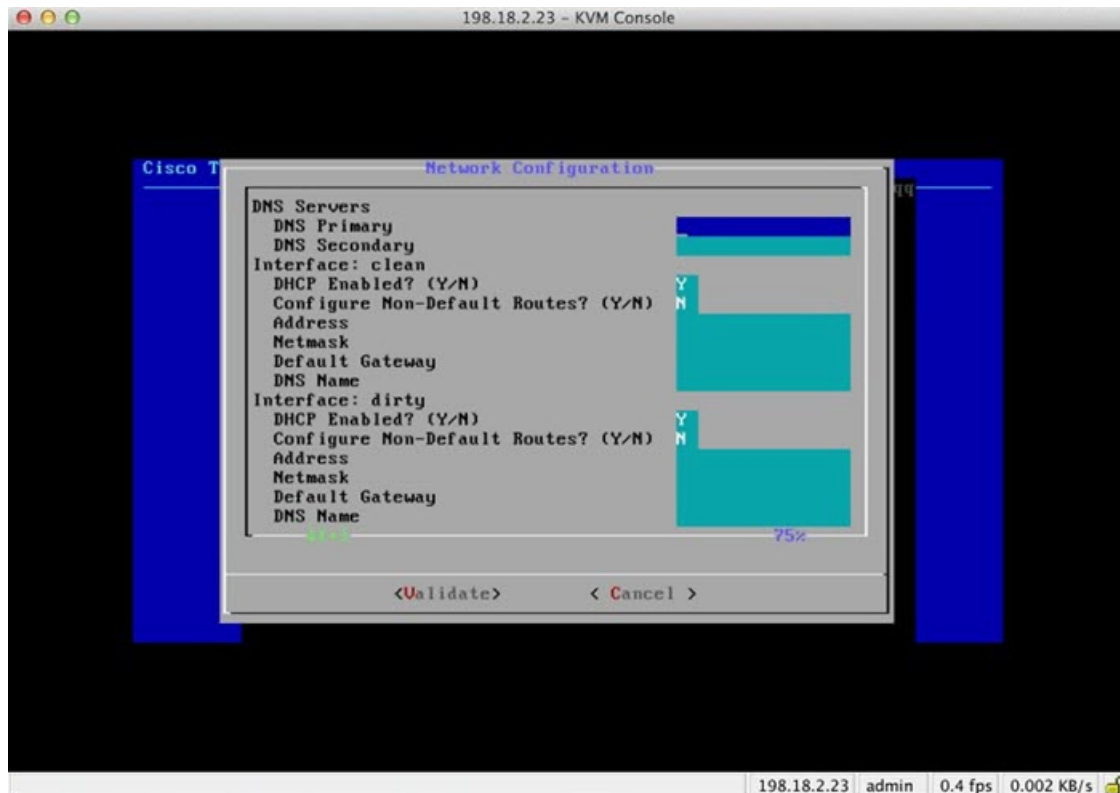
The initial network configuration is completed in the TGSN Dialog. The basic configuration, once completed, allows access to the OpAdmin portal, where you can complete additional configuration tasks.



Note For DHCP users, the following steps assume that you are using static IP addresses. If you are using DHCP to obtain your IP addresses, see the *Cisco Threat Grid Appliance Administrator Guide*.

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

Figure 3: TGSH Dialog - Network Configuration Console



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

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

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

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

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

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

Figure 4: Network Configuration In-Progress (Clean and Dirty)

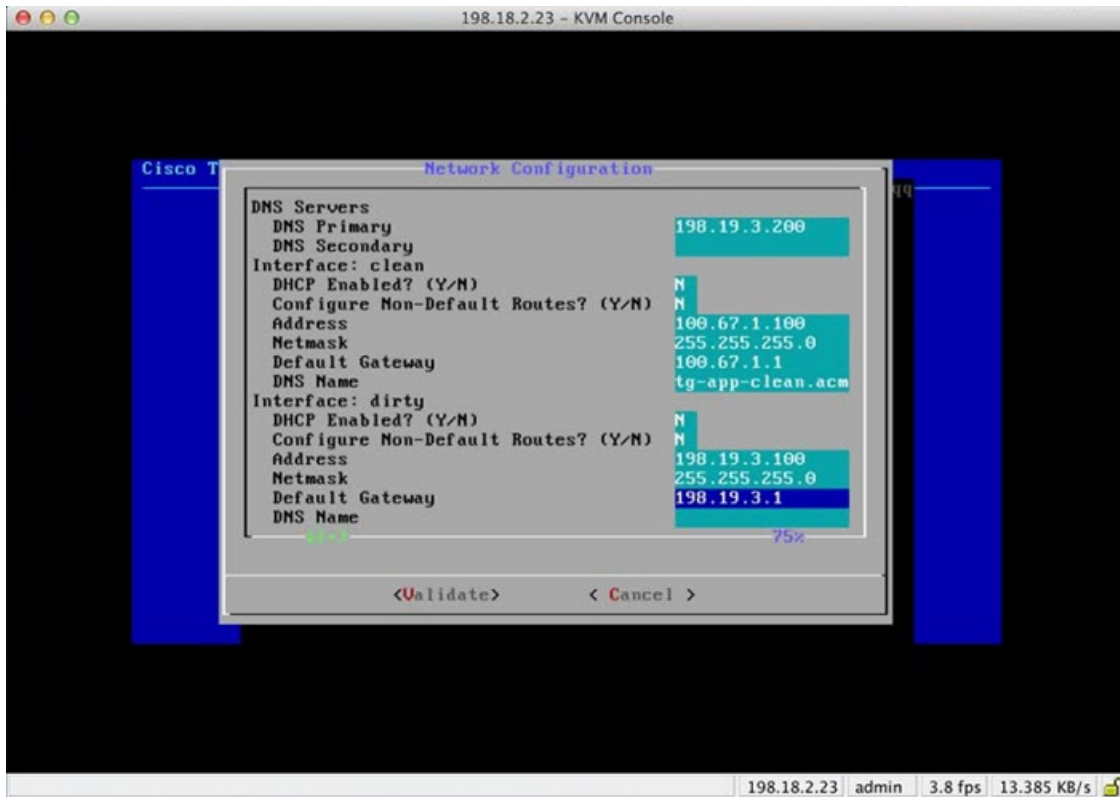
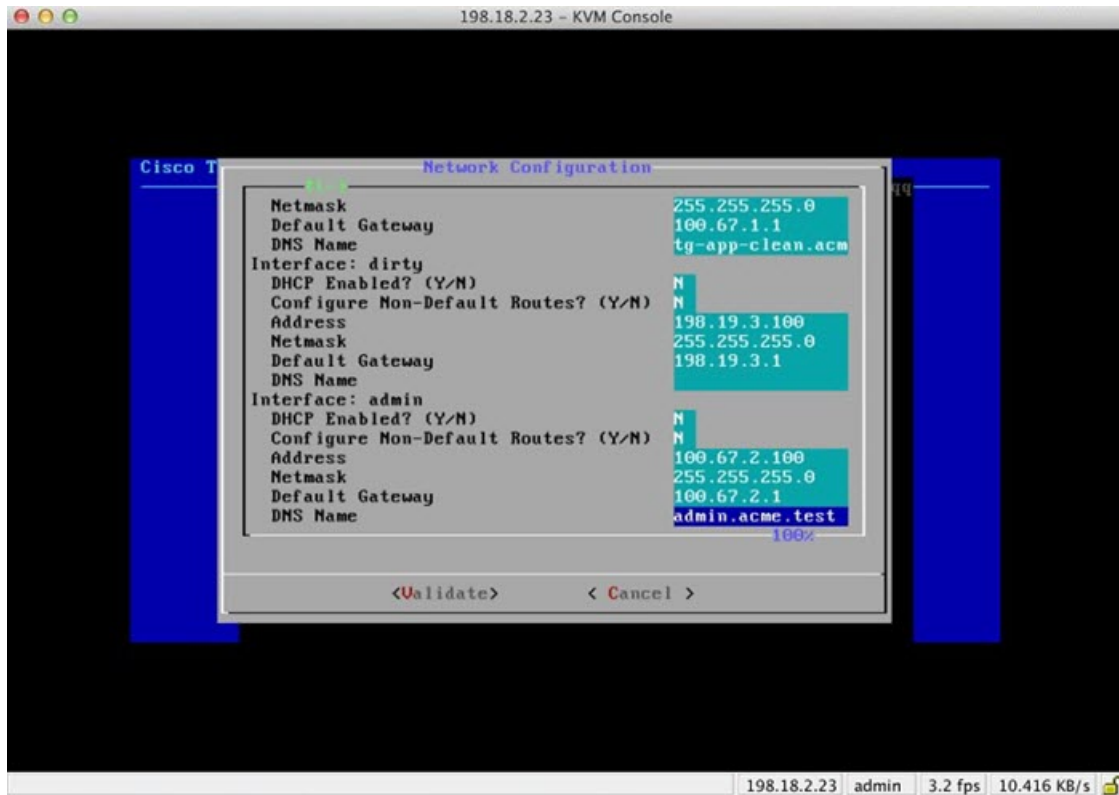
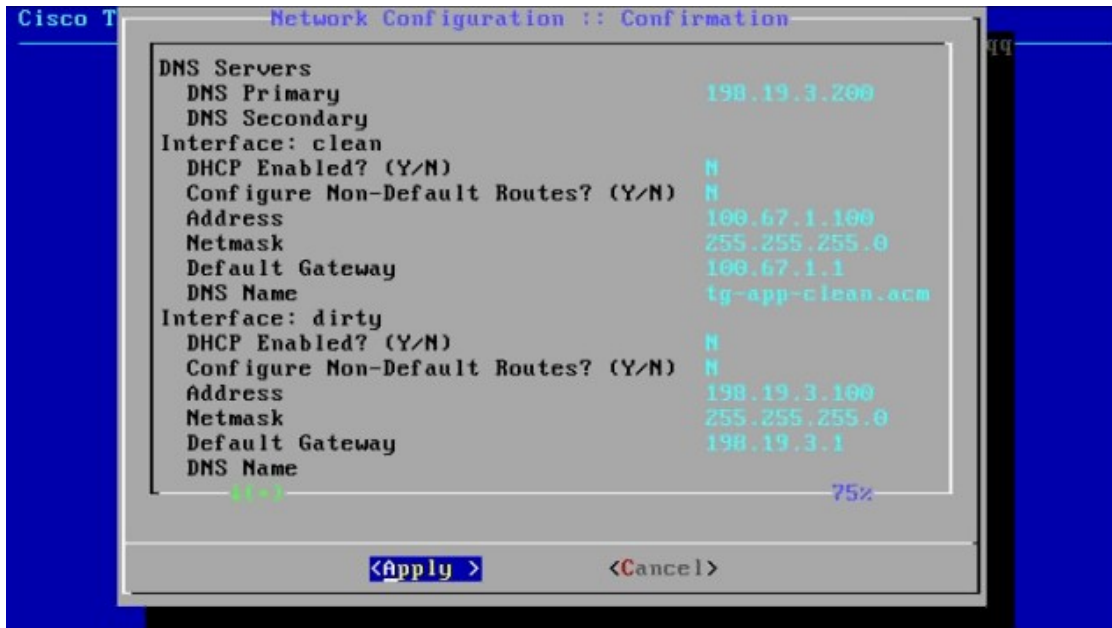


Figure 5: Network Configuration In-Progress (Admin)



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

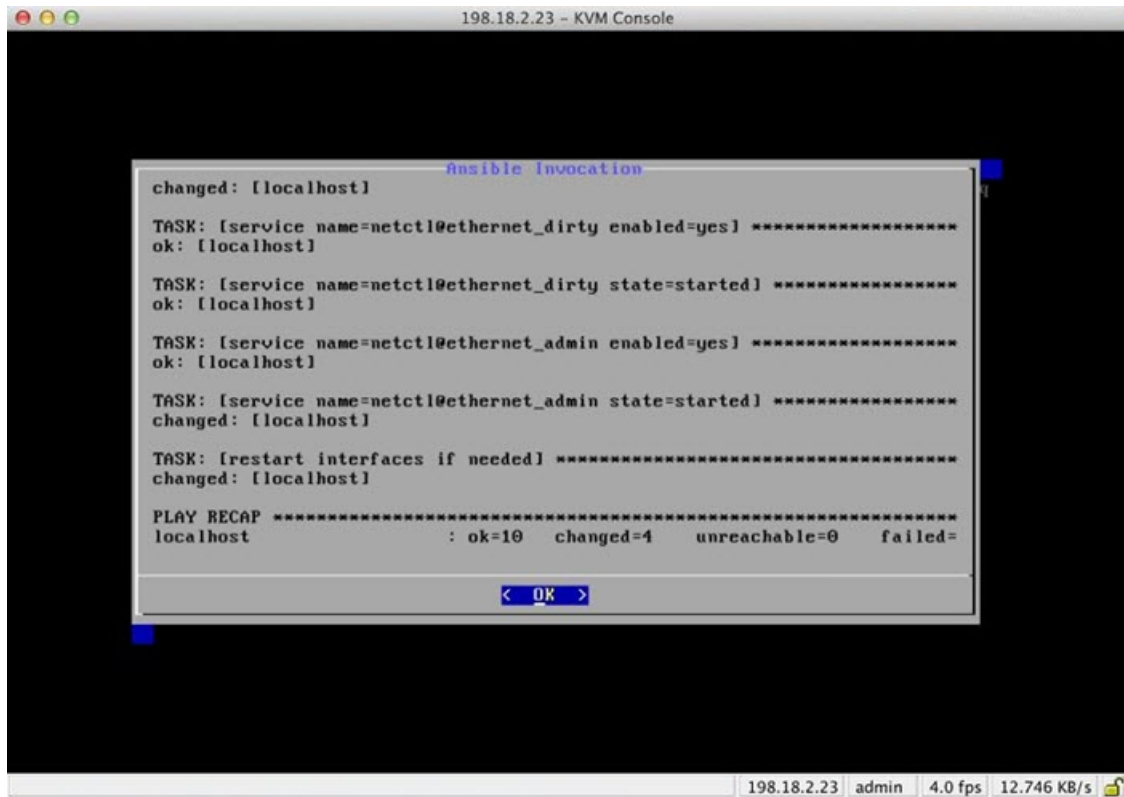
Figure 6: Network Configuration Confirmation



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

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

Figure 7: Network Configuration - List of Changes Made



The screenshot shows a KVM console window titled "198.18.2.23 - KVM Console". Inside the console, a terminal window displays the output of an Ansible invocation. The output shows several tasks being executed on the localhost, including enabling and starting services like netctl@ethernet_dirty and netctl@ethernet_admin, and restarting interfaces if needed. A play recap at the bottom shows 10 OK, 4 changed, 0 unreachable, and 0 failed. At the bottom of the terminal window, there is a blue button labeled "< OK >".

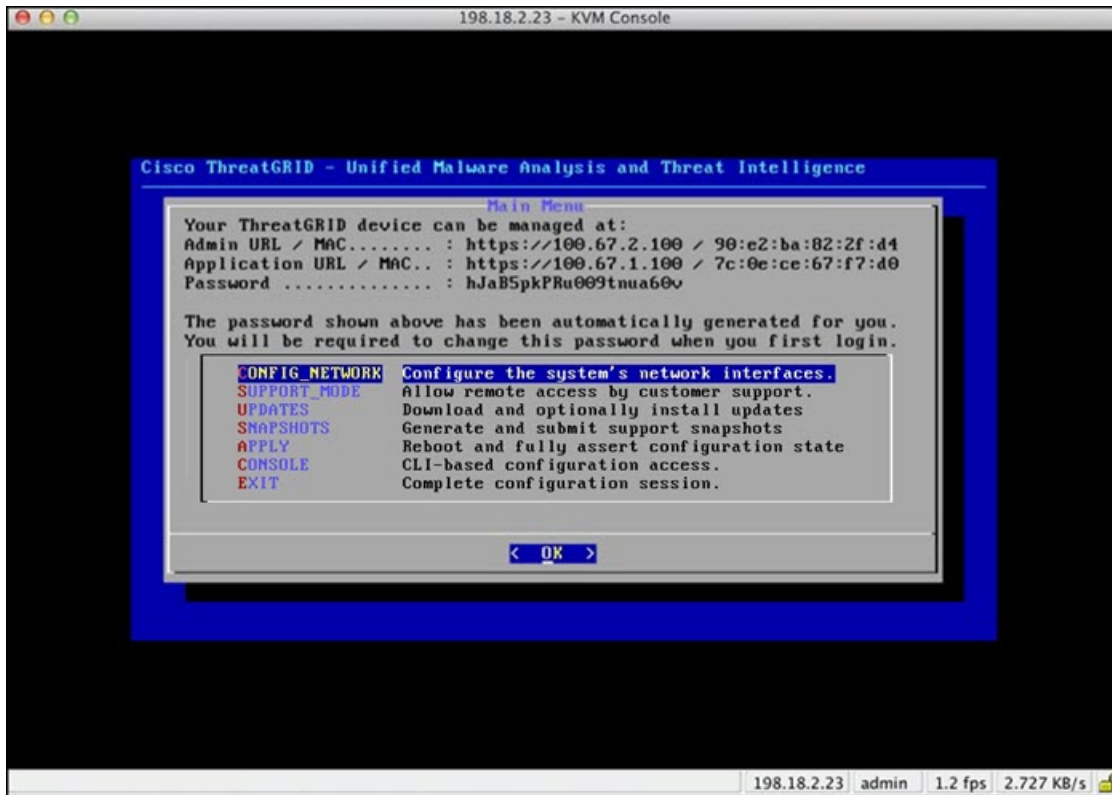
```
changed: [localhost]
Ansible Invocation
TASK: [service name=netctl@ethernet_dirty enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_dirty state=started] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin enabled=yes] *****
ok: [localhost]
TASK: [service name=netctl@ethernet_admin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

198.18.2.23 admin 4.0 fps 12.746 KB/s

Step 9 Select OK.

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

Figure 8: IP Addresses



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

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

What to do next

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