

Network

The initial Secure Malware Analytics Appliance network configuration is completed during the appliance setup using the Admin UI, as documented in the *Cisco Threat Grid Appliance Getting Started Guide*. This chapter provides additional information about using the Admin TUI to make changes to your initial network configuration:

- Modifying Network Configuration, on page 1
- Reconnecting to Admin TUI, on page 2
- Configuring Network in Recovery Mode, on page 2

Modifying Network Configuration

The initial network configuration is completed using the Admin TUI. If you want to make changes to your initial network configuration, perform the following steps.

Note If you are using DHCP to obtain IPs, see the Network section.

Procedure

Step 1 Login to Admin TUI.

Note
If you are configured for **LDAP Only** authentication, you can only log into Admin TUI using LDAP. If authentication mode is set to **System Password or LDAP**, the Admin TUI login only allows the **System** login.

Step 2 In the Admin TUI interface, choose **CONFIG_NETWORK**.

The **Network Configuration** console opens and displays the current network settings.

Step 3 Make any necessary changes (you need to backspace over the old entry before you can enter the new one).

Step 4 Leave the Dirty network **DNS Name** blank.

Step 5 After you finish updating the network settings, tab down and choose **Validate** to verify your entries.

If errors occur, fix the invalid values and choose **Validate** again.

After validation, the **Network Configuration Confirmation** page displays the entered values

Step 6 Choose **Apply** to apply your configuration settings.

Detailed information about the configuration changes that have been made are displayed.

Step 7 Choose **OK**.

The **Network Configuration** console refreshes again and displays the IP addresses. Network configuration is now complete.

Reconnecting to Admin TUI

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

To reconnect to the Admin TUI, SSH into the Admin IP address as the user **threatgrid**. The required password is either the initial randomly generated password, which is visible initially in the Admin TUI, or the new Admin password you created during the first step of the Admin UI configuration. For more information, refer to the latest Cisco Secure Malware Analytics Appliance Getting Started Guide in Configuration Guides.

Configuring Network in Recovery Mode

Network configuration in recovery mode mirrors the full system (v2.7 and later):

- All interfaces are brought up.
- Firewall rules and policy routing restricts which processes can communicate on which interfaces.

Note Support mode traffic on port 19791 is allow-listed across all three interfaces.

Perform the following steps to set up networking in recovery mode.

Procedure

Step 1 Reboot the Secure Malware Analytics Appliance (**Operations > Power > Reboot**) and then choose **Recovery Mode** in the boot menu.

Step 2 Once the system is up, press **Enter** several times to get a clean command prompt.

Step 3 Enter **netctl clean** and provide the following information:

- **Configuration type (dhcp|static)[Current: DHCP]**: static
- **IP Address (ipaddr)** - <Clean IP Address>
- **Netmask (ipaddr)** -<Netmask>

- **Gateway Address** - <Clean network gateway>
- **DNS name of this interface's address** - Enter DNS name of this interface's address
- **Primary DNS server for LAN addresses** - Enter primary DNS server address
- **Secondary DNS server for LAN addresses** - Enter secondary DNS server address
- **Save this profile? (Yes|No)** - Enter **Yes**

Step 4 Enter **netconfig-apply** to apply the configuration.

The appliance will attempt to open an outbound support connection on the Clean interface on port 19791/tcp.