Configuration Management

This chapter describes additional information about configuring the Threat Grid Appliance after the initial configuration. It includes the following topics:

Introduction

The initial Threat Grid Appliance configuration is performed during the appliance setup, as documented in the *Cisco Threat Grid Appliance Setup and Configuration Guide*, using the TGSH Dialog and the OpAdmin portal.

Note Threat Grid organizations and user accounts are managed in the Threat Grid Portal UI (from the drop-down arrow next to your login name in the navigation bar).

Network Configuration Using TGSH Dialog

The initial network configuration is completed using the TGSH Dialog (see *Cisco Threat Grid Appliance Setup and Configuration Guide*). This section provides some additional information about using the TGSH Dialog.

Configure Network Using TGSH Dialog

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 Network Configuration and DHCP.

Step 1 Login to TGSH Dialog.

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

Step 2 In the TGSH Dialog interface, select **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 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

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

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

Step 7 Select **OK**.

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

Reconnect to TGSH Dialog

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

To reconnect to the TGSH Dialog, SSH into the Admin IP address as the user **threatgrid**. The required password is either the initial randomly generated password, which is visible initially in the TGSH Dialog, or the new Admin password you create during the first step of the OpAdmin Configuration (see the *Cisco Threat Grid Appliance Setup and Configuration Guide*.

Configure Networking 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.

Step 1 Reboot the Threat Grid Appliance 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** - static
- **IP Address** - <Clean IP Address>/<Netmask>
- **Gateway Address** - <Clean network gateway>
- **Routes** - <leave blank>
- **Final Question** - Enter **y**

Step 4 Enter **Exit** to apply the configuration.

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

Configuration Using OpAdmin Portal

The initial setup and configuration wizard is described in the Cisco Threat Grid Appliance Setup and Configuration Guide. New Threat Grid Appliances may require the administrator to complete additional configuration, and OpAdmin settings may require updates over time.

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

The OpAdmin portal is used to configure and manage various Threat Grid Appliance configuration settings, including:

- Administrator's passwords (for OpAdmin and the **threatgrid** user)
- Threat Grid License
- Rate Limits
- SMTP
- SSH
- SSL Certificates
- DNS servers (including DNS configuration for AMP for Endpoints Private Cloud integrations)
- NTP servers
- Server Notifications

- Syslog messages and Threat Grid Notifications remote server setup
- CA Certificate Management (for AMP for Endpoints Private Cloud integrations)
- LDAP Authentication
- Third-party Detection and Enrichment Services (including ClamAV, OpenDNS, Titanium Cloud, and VirusTotal)

Note

- Configuration updates in OpAdmin should be completed in one session to reduce the chance of an interruption to the IP address during configuration.
- OpAdmin does not validate the gateway entries. If you enter the wrong gateway and save it, the OpAdmin interface will not be accessible. You will need to use the console to fix the networking configuration if that was done on the Admin interface. If Admin is still valid, you can fix it in OpAdmin and reboot.
- Threat Grid Appliances (v2.7 or later) use the serial number as the hostname to improve interoperability with some NFS v4 servers.

Important OpAdmin uses HTTPS and you must enter this in the browser address bar; pointing to only the Admin IP is not sufficient. Enter the following address in your browser:

https://adminIP/

OR

https://adminHostname/

Configure SSH Keys

Setting up SSH keys provides the Threat Grid Appliance administrator with access to the TGSH Dialog via SSH (`threatgrid@<host>`).

It does not provide root access or a command shell. Multiple keys may be added in **Configuration > SSH**.

Configuring a SSH public key for access to the Threat Grid Appliances disables password-based authentication via SSH (v2.7.2 and later); this makes SSH authentication methods one or the other, not both. After a successful SSH connection using key-based authentication, the TGSH Dialog prompts for a password, such that both tokens are required.

Configure Remote Syslog Server for Notifications

In addition to the periodic notifications that can be set up to deliver system notifications via email (in OpAdmin under **Configuration** > **Notifications**), you can configure a remote syslog server to receive syslog messages and Threat Grid notifications.

Step 1 Log in to the OpAdmin portal and click **Configuration > Syslog**.

Step 2 Enter the **server DNS** and then choose a protocol from the drop-down list (TCP is the default, the other is UDP).

Step 3 Check the **Verification** check box to perform a DNS lookup after you save the configuration.

If the host cannot resolve the name, it will print an error and will not save (until you enter a valid hostname). If you do not check the **Verification** check box, the appliance will accept any name, whether valid in DNS or not.

Step 4 Click **Save**.

To edit or delete the Syslog DNS, open **Configuration > Syslog**, make your modifications, and then click **Save**.

Configure LDAP Authentication

The Threat Grid Applicance supports LDAP authentication and authorization for OpAdmin and TGSH Dialog login.

You can authenticate multiple appliance administrators with different credentials that are managed on the domain controller or the LDAP server. Authentication modes include: System Password Only, System Password or LDAP, and LDAP Only.

There are three LDAP Protocol options: LDAP, LDAPS, and LDAP with STARTLS.

The following considerations should be observed:

- The dual authentication mode (**System Password or LDAP**) is required to avoid accidentally locking yourself out of the Threat Grid Appliance when setting up LDAP.

  Selecting **LDAP Only** is not allowed initially; you must first go through dual mode to make sure it works. You must log out of OpAdmin after the initial configuration, and then log back in using LDAP credentials to toggle to **LDAP Only**.

- You can only log into the TGSH Dialog using LDAP if you are configured for **LDAP Only** authentication. If authentication mode is set to **System Password or LDAP**, the TGSH Dialog login only allows the System login.

- If the Threat Grid Appliance is configured for LDAP authentication only (**LDAP Only**), you can reset the password in recovery mode to reconfigure the authentication mode to also allow login with a system password.

- Make sure that the authentication filter is set up to restrict membership.

- The TGSH Dialog and OpAdmin portal require LDAP credentials only in **LDAP Only** mode/ if **LDAP only** is configured, the TGSH Dialog only prompts for the LDAP user/password; not the system password.

- If authentication is configured for **System Password or LDAP**, the TGSH Dialog prompts for for only the system password; not both.

- To troubleshoot LDAP issues, disable it by resetting the password in Recovery Mode.

- To access the TGSH Dialog via SSH, a system password or a configured SSH key is required in addition to LDAP credentials when in **LDAP Only** mode.

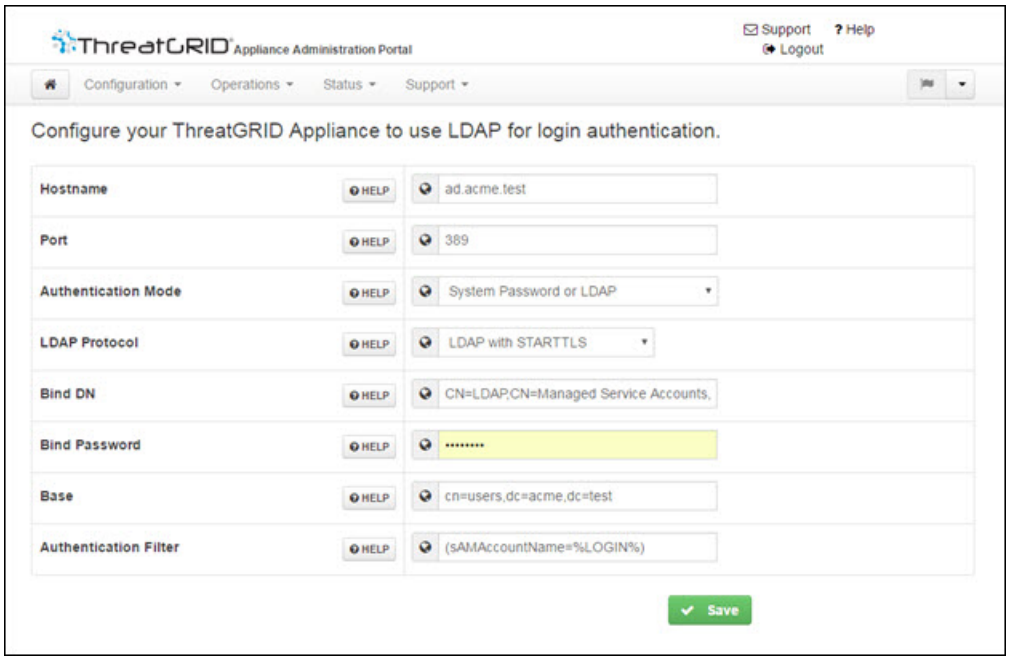
- LDAP is outbound from the Clean interface.

Configure LDAP Authentication in OpAdmin

Perform the following steps to configure LDAP authentication in the OpAdmin portal.

Step 1 Log in to the OpAdmin portal and choose **Configuration > LDAP** to open the LDAP configuration page.

Figure 1: LDAP Authentication Configuration



Step 2 Complete the fields on the page. You can click the **Help** icon next to each field for a detailed description and more information.

Note The first time you configure LDAP authentication, you must select **System Password** or **LDAP**, log out of OpAdmin, and then log back in using your LDAP credentials. You can then change the setting to implement **LDAP Only**.

Step 3 Click **Save**.

When users log in to OpAdmin or TGSH Dialog, they will now see one of the following screens:

Figure 2: LDAP Only

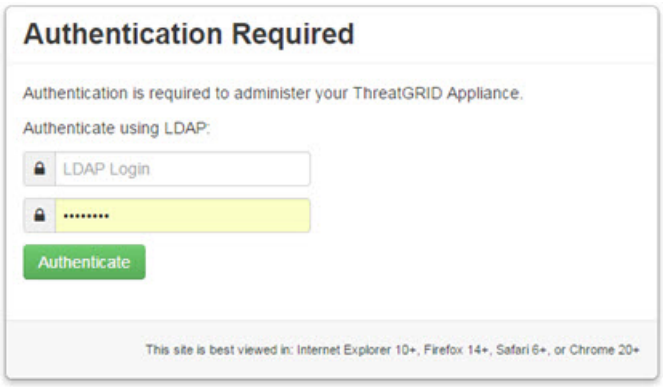
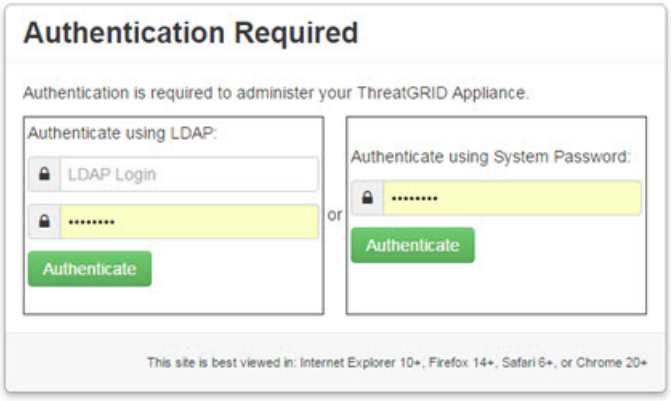


Figure 3: System Password or LDAP



Configure Third-Party Detection and Enrichment Services

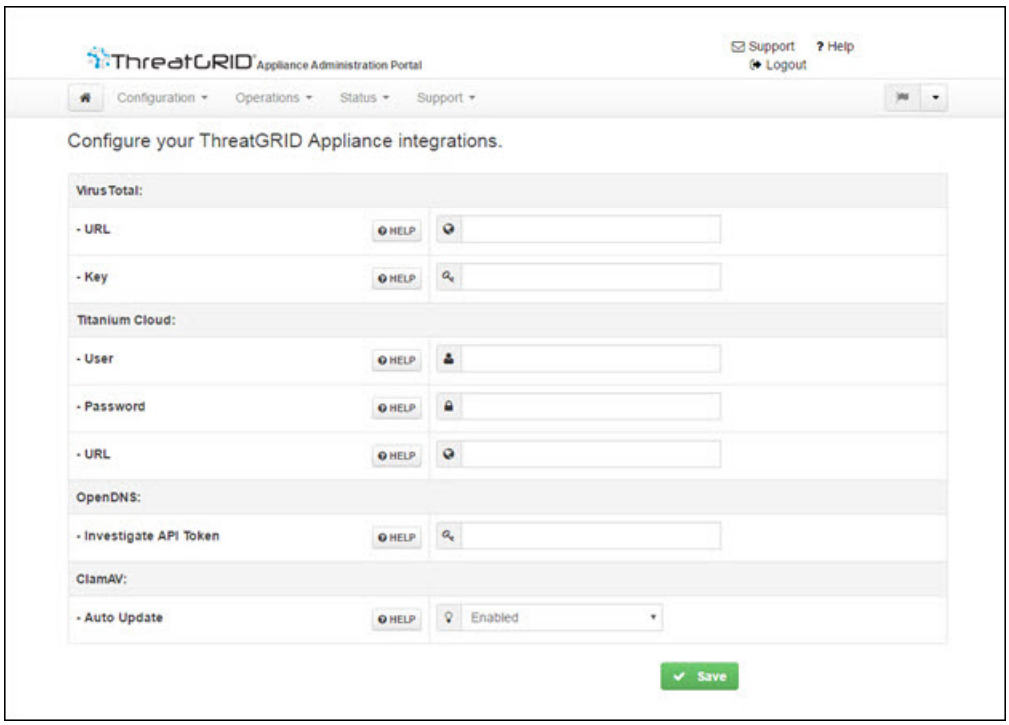
Integrations with several third-party detection and enrichment services, including OpenDNS, TitaniumCloud, and VirusTotal, can be configured on the appliance using the **Integration** page (v2.2 and later).

The Cloud Search Federation feature (available in v2.8 and later), provides users with an option in the portal application UI to rerun a search query against the Threat Grid cloud instance, if a cloud endpoint is configured (on the **Integrations** page in the administrative interface).

Note If OpenDNS is not configured, the **whois** information on the Domains entity page in the analysis report (in the Mask version of the UI) will not be rendered.

Step 1 Log in to the OpAdmin portal and click **Configuration** > **Integrations** to open the **Integrations** page.

Figure 4: Integrations Configuration



Step 2 Enter the authentication or other values required.

Note ClamAV signatures can be automatically updated on a daily basis. This is enabled by default, and can be disabled in the **ClaimAV** field.

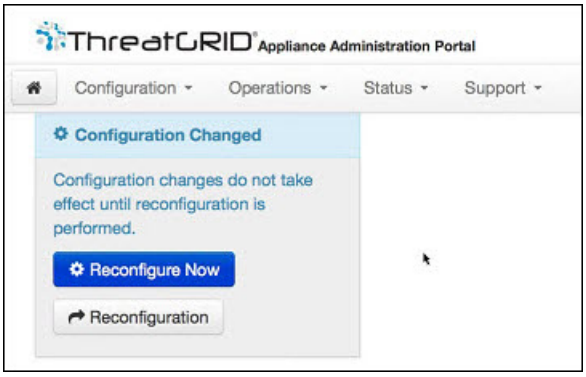
Step 3 Click **Save**.

Apply Configuration Change

Any time changes are made to configuration settings, a light blue **Configuration Changed** alert appears below the **Configuration** menu. When you are done updating any OpAdmin configuration settings, you must save the new configuration in a separate step.

Step 1 Click **Configuration Changed** to open the dialog.

Figure 5: Configuration Changed Dialog



Step 2 Click **Reconfigure Now** to apply your changes to the appliance.

Using DHCP

Most Threat Grid Appliance users do not use a network configured with DHCP. However, if you are connected to a network configured to use DHCP, it is important that you read this section to understand the requirements.

Note If the initial appliance network configuration used DHCP and you now need to switch to static IP addresses, see Network Configuration and DHCP.

TGSH Dialog displays the information you will need to access and configure the OpAdmin portal interface. It may take some time for the IP addresses for DHCP to display after your appliance boots.

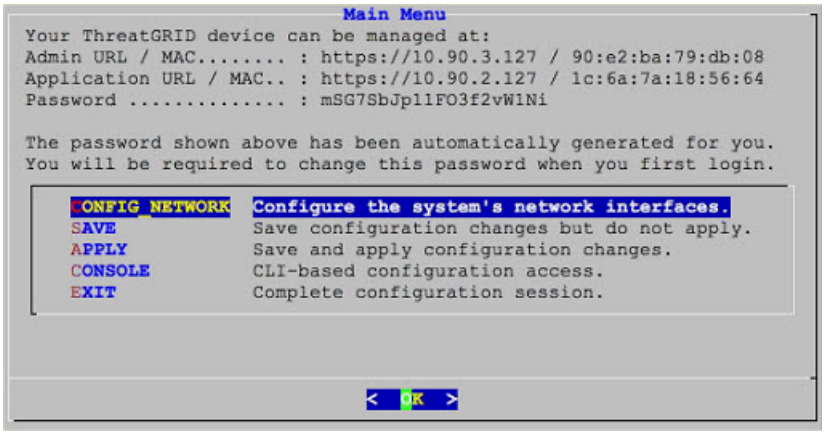
Explicit DNS for DHCP

Threat Grid Appliances that use DHCP need to explicitly specify DNS.

Warning An upgrade of a system without a DNS server explicitly specified will fail.

Open the TGSH Dialog and note the following information:

Figure 6: TGSH Dialog (Connected to a Network Configured to Use DHCP)



- **Admin URL** - The Admin network. You will need this address in order to continue the remaining configuration tasks with OpAdmin.
- **Application URL** - The Clean network. This is the address to use after completing the configuration with OpAdmin to access the Threat Grid application.

  The Dirty network is not shown.
- **Password** - The initial Admin password that is randomly generated during the Threat Grid Appliance installation. You will need to change this password later as the first step the OpAdmin configuration process.

If you plan to use DHCP on a permanent basis, no additional network configuration is necessary, unless you need to change the Admin IP address to static.

Network Configuration and DHCP

If you used DHCP for the initial configuration, and you need to adjust the IP assignment from DHCP to your permanent static IP addresses for all three networks, perform the following steps.

Note OpAdmin does not validate the gateway entries. If you enter the wrong gateway and save it, the OpAdmin interface will not be accessible. You will need to use the console to fix the networking configuration if that was done on the admin interface. If Admin is still valid, you can fix it in OpAdmin and reboot.

Step 1 In the OpAdmin portal, click **Network** in the navigation pane (although **Configuration** > **Network** is checked in the License window, the DHCP network configuration has not yet been done).

The **Network** page opens.

Step 2 Complete the following fields:

Note The Admin network settings were configured using the **TGSH Dialog** during the initial Threat Grid Appliance setup and configuration.

- **IP Assignment** - Choose **Static** from the drop-down list for both Clean and Dirty network interface.
- **IP Address** - Enter a static IP address for the Clean or Dirty network interface.
- **Subnet mask** - Complete as appropriate for the type of network interface.
- **Validate DNS Name** - For the Clean network interface, check the **Validate DNS Name** check box to verify that the DNS resolves to the IP address.
- **Primary and Secondary DNS** - Enter the primary and secondary DNS server information.

Step 3 Click **Next (Applies Configuration)** to save your network configuration settings.

Note Email configuration is managed from the **Email** page and Time NTP servers are managed on the **Date and Time** page.

Step 4 Click **Configuration Changed** and choose **Reconfigure Now** to apply your DHCP settings.