Configuration Management

This chapter describes additional information about configuring the Threat Grid Appliance after the initial configuration.

Note The initial configuration is described in the *Cisco Threat Grid Appliance Setup and Configuration Guide*. Refer to this guide for configuring the TGSH Dialog Interface and using the OpAdmin Configuration Wizard.

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 validate your entries.

If invalid values have been entered, you may see errors. Correct the entries and then select **Validate** again.

After validation, the Network Configuration Confirmation 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 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.

OpAdmin is the recommended tool for configuring your appliance, and in fact, much of the appliance configuration can only be done via OpAdmin. OpAdmin is used to configure and manage a number of important Threat Grid Appliance configuration settings, including:

- The 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. Pointing a browser at the Admin IP is not sufficient; you must point to:

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**.

On Threat Grid Appliances (v2.7 and later), configuring a SSH public key for access to the appliance disables password-based authentication via SSH; this makes SSH authentication methods one or the other, not both. After a successful SSH connection using key-based authentication, 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** and 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 reviewed:

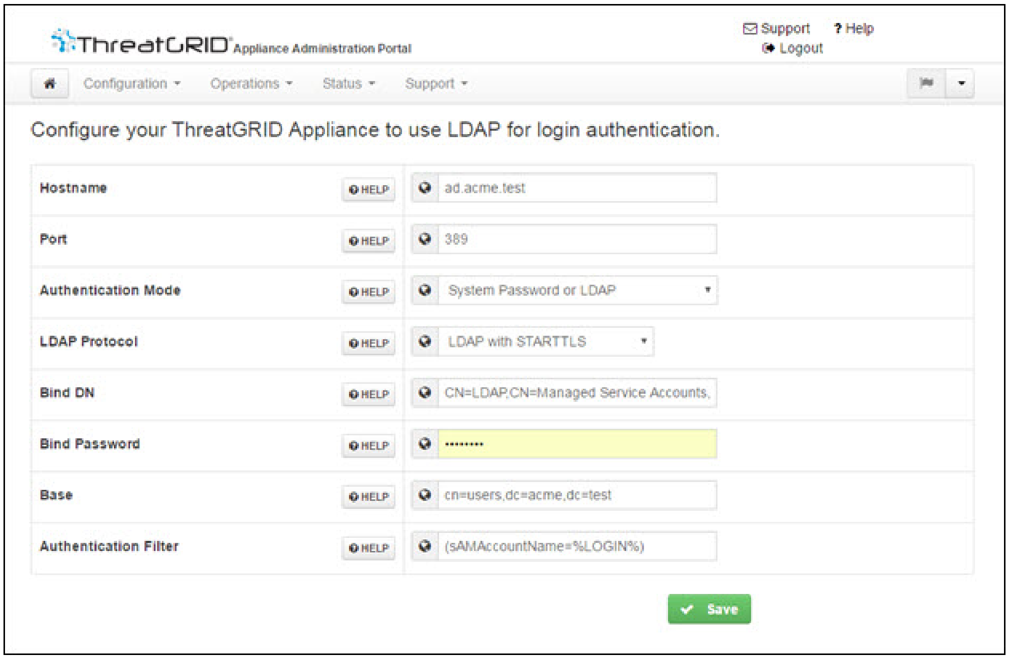
- The dual authentication mode (**System Password or LDAP**) is required to avoid accidentally locking yourself out of the appliance when setting up LDAP. Selecting **LDAP Only** is not allowed initially; you must first go through dual mode to make sure it works. You will need to log out of OpAdmin after the initial configuration, and then log back in using LDAP credentials in order to toggle to **LDAP Only**.
- You can only log into TGSH Dialog using LDAP if you are configured for LDAP Only authentication. If authentication mode is set to System Password or LDAP, then the TGSH Dialog login will only allow the System login.
- If the appliance is configured for LDAP authentication only (**LDAP Only**), then resetting the password in recovery mode will reconfigure the authentication mode to allow login with system password as well.
- Make sure that the authentication filter is set up to restrict membership.
- TGSH Dialog and OpAdmin require LDAP credentials only in **LDAP Only** mode: if **LDAP only** is configured, TGSH Dialog will not ask for the system password but for an LDAP user/password.
- If authentication is configured for **System Password or LDAP**, TGSH Dialog will continue to ask for the system pw only, it'll not have both.
- Troubleshooting LDAP: If it breaks, disable it by doing a password reset in Recovery Mode.
- TGSH Dialog access via SSH: A system password or a configured SSH key is required **in addition to** LDAP credentials for tgsh-dialog access via ssh 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



Configure your ThreatGRID Appliance to use LDAP for login authentication.

Hostname	ad.acme.test
Port	389
Authentication Mode	System Password or LDAP
LDAP Protocol	LDAP with STARTTLS
Bind DN	CN=LDAP,CN=Managed Service Accounts,
Bind Password	••••••••
Base	cn=users,dc=acme,dc=test
Authentication Filter	(sAMAccountName=%LOGIN%)

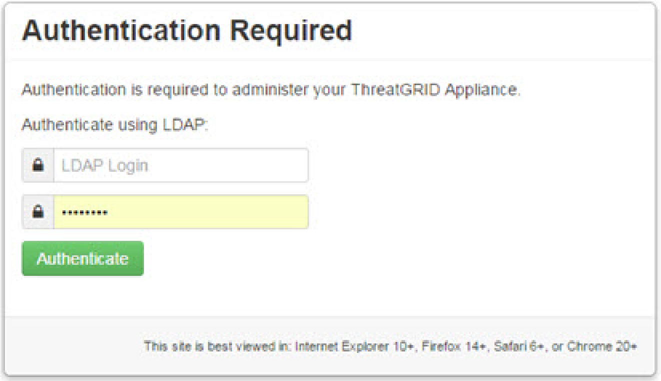
Step 2 Complete the fields on the page. You can click the **Help** icon next to each field for a detailed description and more information.

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



Authentication Required

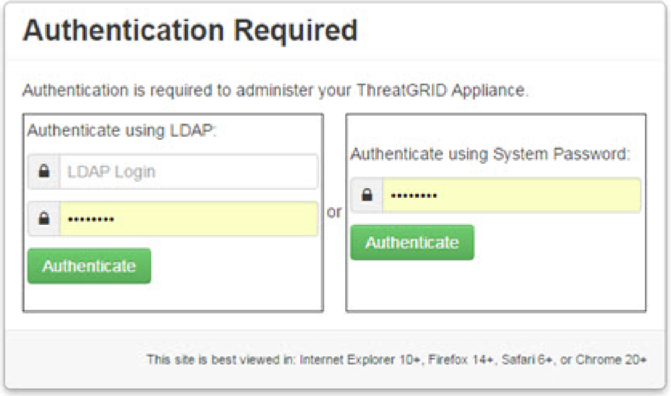
Authentication is required to administer your ThreatGRID Appliance.

Authenticate using LDAP:

••••••••

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

Figure 3: System Password or LDAP



Authentication Required

Authentication is required to administer your ThreatGRID Appliance.

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

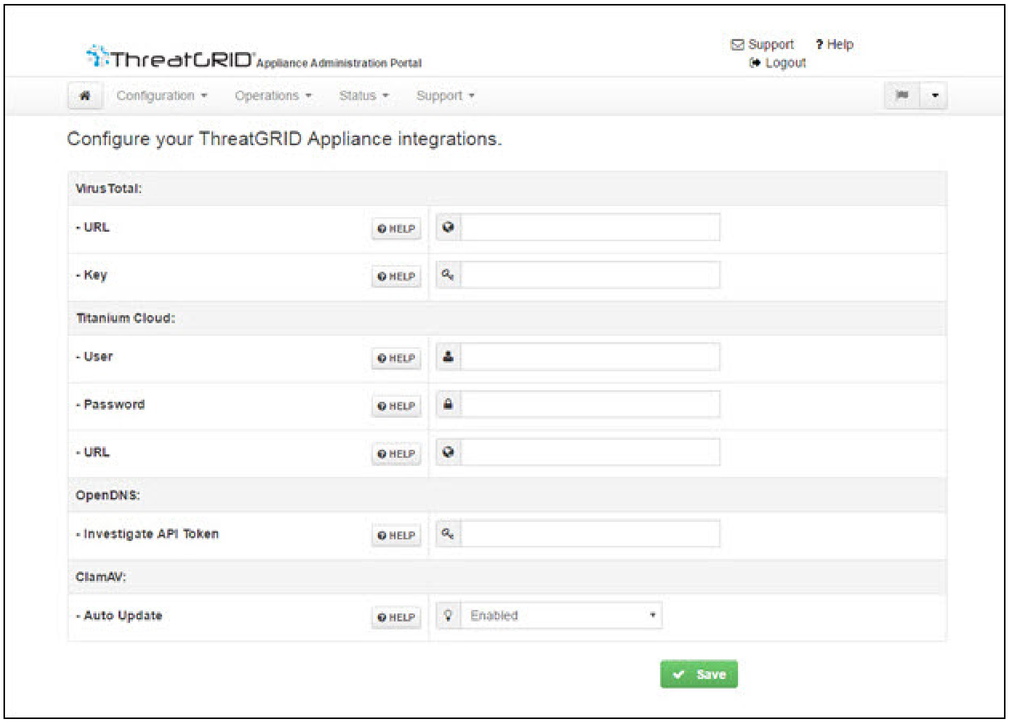
Configure Third-party Detection and Enrichment Services

Integrations with several third-party detection and enrichment services, including OpenDNS, TitaniumCloud, and VirusTotal, can be configured on the appliance using the Integration Configuration page. This applies to Version 2.2 and later.

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

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

Figure 4: Integrations Configuration



Configure your ThreatGRID Appliance integrations.

VirusTotal:

- URL
- Key

Titanium Cloud:

- User
- Password
- URL

OpenDNS:

- Investigate API Token

ClamAV:

- Auto Update: Enabled

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 on the Integrations Configuration page (**ClaimAV** field).

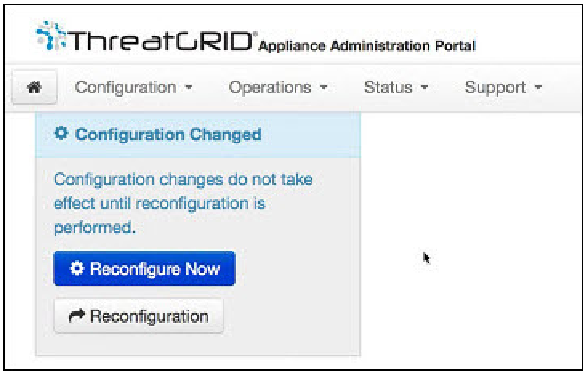
Step 3 Click **Save**.

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



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

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, then read this section.

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.

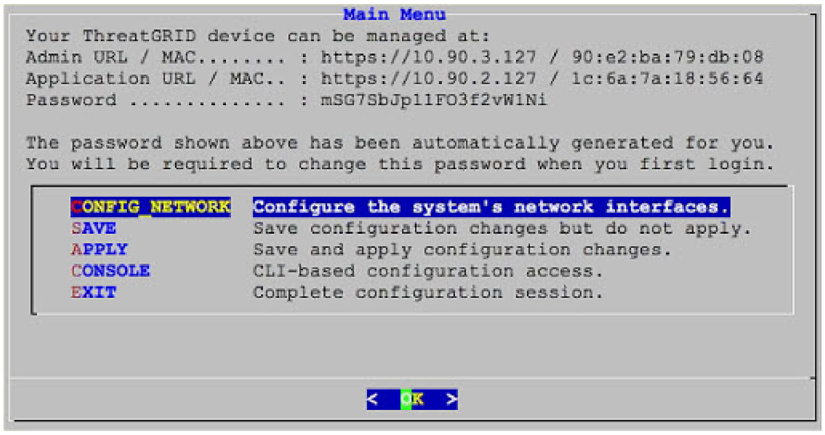
Explicit DNS for DHCP

Threat Grid Appliances (v1.3 and later) that use DHCP need to explicitly specify DNS.

Warning An upgrade of a system without a DNS server explicitly specified to v1.3 will fail.

Open the TGSH Dialog and note the following information.

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



```
                          Main Menu
Your ThreatGRID device can be managed at:
Admin URL / MAC........ : https://10.90.3.127 / 90:e2:ba:79:db:08
Application URL / MAC.. : https://10.90.2.127 / 1c:6a:7a:18:56:64
Password .............. : mSG7SbJp11FO3f2vW1Ni

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.
    SAVE               Save configuration changes but do not apply.
    APPLY              Save and apply configuration changes.
    CONSOLE            CLI-based configuration access.
    EXIT               Complete configuration session.

                         <  OK  >
```

- **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. Note: This is the address to use after completing the configuration with OpAdmin, in order to access the Threat Grid application.

  The Dirty network is not shown.
- **Password** - The initial administrator's password, which is randomly generated during the 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, then 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 initial configuration, and you now need to adjust the IP assignment from DHCP to your permanent static IP addresses for all three networks, perform the following steps.

Note OpAdmin will not validate the gateway entries. If you enter the wrong gateway and save it, the OpAdmin interface will be inaccessible. 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 configuration page opens.

Step 2 Complete the following fields:

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

- **IP Assignment** - Choose **Static** from the drop-down menu 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 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 configuration settings.