



OpAdmin Portal Configuration Wizard

This chapter provides instructions for configuring your appliance using the OpAdmin Portal. It includes the following topics:

- [Introduction, on page 1](#)
- [Configuration Wizard, on page 3](#)
- [Install Updates, on page 11](#)
- [Test Appliance Setup, on page 12](#)

Introduction

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

The configuration includes the following steps:

- Change OpAdmin Admin Password
- Review End User License Agreement
- Review Network Configuration Settings (not configured using wizard)
- Install License
- Configure NFS
- Configure Email Host
- Configure Notifications
- Configure Date and Time (NTP Server)
- Configure SysLog
- Review and Install Configuration Settings



Note Not all configuration steps are completed using the configuration wizard. See the [Cisco Threat Grid Appliance Administrator Guide](#) for configuring settings not included in the wizard, such as SSL Certificates and Clustering.



Important 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.

Log In to OpAdmin Portal

Perform the following steps to log in to the Threat Grid OpAdmin portal.

Step 1 In a browser, enter the URL for the OpAdmin portal (<https://<adminIP>/> or <https://<adminHostname>/>) to open the Threat Grid OpAdmin login screen.

Note The Hostname is the appliance serial number (v2.7 or later).

Figure 1: OpAdmin Login Screen



Step 2 Enter the initial **Admin Password** that you copied from the TGSH Dialog and click **Login**.

What to do next

Proceed to [Change Admin Password](#).

Change Admin Password

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 continuing with the configuration.

Step 1 Enter the password from the TGSH Dialog in the **Old Password** field. (You should have this saved in a text file.)

Step 2 Enter a **New Password** and re-enter it in the **Confirm New Password** field.

Step 3 Click **Change Password**. The password is updated.

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

What to do next

Proceed to [Review End User License Agreement](#).

Review End User License Agreement

Review the license agreement and confirm that you agree to it.

Step 1 Review the End User License Agreement.

Step 2 Scroll to the end and click **I HAVE READ AND AGREE**.

Note We recommend that you follow the configuration workflow and configure the networks before you install the license.

What to do next

Proceed to [Configure Network Settings](#).

Configuration Wizard

The Configuration wizard takes you through configuring your Threat Grid Appliance.

Configure Network Settings

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

Step 1 Review the IP addresses and confirm they are accurate.

Step 2 If you used DHCP for your initial connection and now need to change the Clean and Dirty IP networks to static IP addresses, follow the steps in the *Using DHCP* section of the [Cisco Threat Grid Appliance Administrator Guide](#).

What to do next

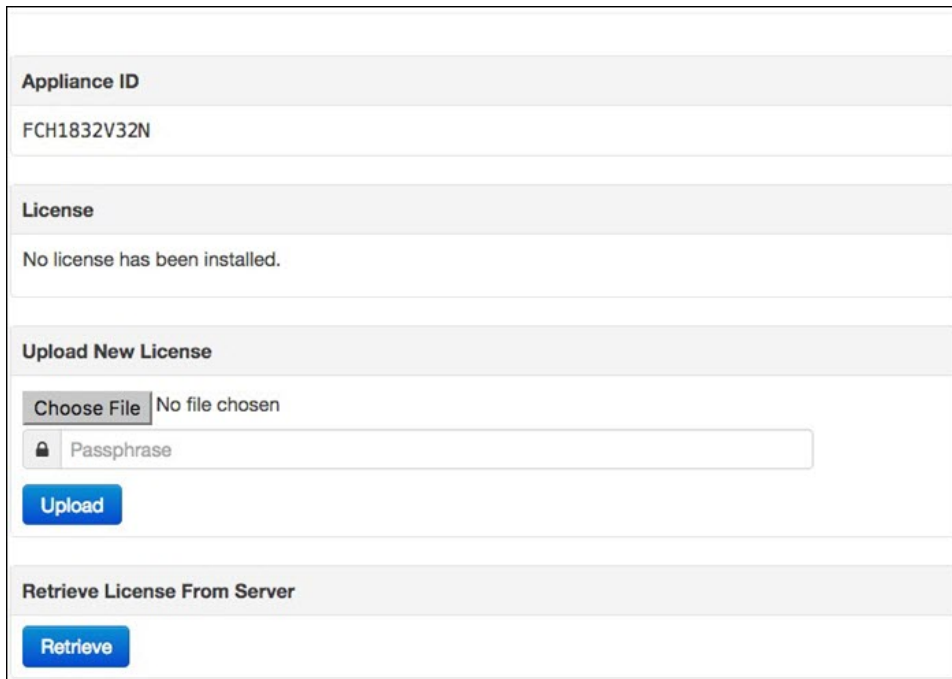
Proceed to [Install License](#).

Install License

After the networks are configured, you are ready to install the Threat Grid license.

Step 1 Click **License** in the navigation pane to open the License page.

Figure 2: License Page Prior to Installation



The screenshot displays the License page interface. It features a section for 'Appliance ID' with the value 'FCH1832V32N'. Below this is a 'License' section with the message 'No license has been installed.' The 'Upload New License' section includes a 'Choose File' button (currently showing 'No file chosen'), a 'Passphrase' input field with a lock icon, and an 'Upload' button. At the bottom, there is a 'Retrieve License From Server' section with a 'Retrieve' button.

Step 2 In the Upload New License pane, click **Choose File** and select the license from your file manager.

Alternatively, you can retrieve the license from the server (v2.3 or later). If the appliance has network access when being installed, click **Retrieve** to get the license over the network.

Step 3 Enter your license password in the **Passphrase** field.

Step 4 Click **Upload** to install the license. The page refreshes and your license information is displayed.

Figure 3: License Information After Successful Installation

Appliance ID	
FCH1832V32N	
License	
Licensee	No Name Provided provision@threatgrid.com
Business	2f518e6d-dd45-4397-9533-3c6d38239c32
Validity	Fri, 22 Sep 2017 14:47:46 +0000 - Mon, 21 Sep 2020 14:47:46 +0000
Product SKU	
Daily Submissions	1500
Upload New License	
<input type="button" value="Choose File"/>	No file chosen
<input type="password" value="Passphrase"/>	
<input type="button" value="Upload"/>	
Retrieve License From Server	
<input type="button" value="Retrieve"/>	
<input type="button" value="Next >"/>	

Step 5 Click **Next** to continue.

What to do next

Proceed to [Configure NFS](#).

Configure NFS

The next step in the workflow is NFS configuration. This task is required for backups and clustering. See *NFS Requirements* in the *Backups* section of the [Cisco Threat Grid Appliance Administrator Guide](#) for more information.

The configuration process includes mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

Step 1 Click **NFS** in the navigation pane to open the NFS configuration page.

Figure 4: NFS Configuration

The screenshot shows the ThreatGRID Appliance Administration Portal interface. At the top, there are links for Support and Help, and a Logout button. Below the navigation bar, the left sidebar lists various configuration categories: Configuration (with sub-items Network, License, NFS, Clustering, Email, Notifications, Date and Time, Syslog), and Other (with sub-item Review and Install). A 'Start Installation' button is visible in the sidebar. The main content area is titled 'NFS' and contains a form titled 'NFS Configuration'. The form has four rows: 'Host' with a text input field and a refresh icon; 'Path' with a text input field and a folder icon; 'Opts' with a text input field and a list icon; and 'Status' with a dropdown menu currently showing 'Disabled'. A 'Next >' button is located at the bottom right of the form. At the bottom of the page, there are links for 'Visit the Cisco Threat Grid homepage', 'Documentation', 'Support', and 'License', along with the ThreatGRID logo.

Step 2 Enter the following information:

- **Host** - The NFSv4 host server. We recommend using the IP address.
- **Path** - The absolute path to the location on the NFS host server under which files will be stored.
- **Opts** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.
- **Status** - Choose **Enabled** from the drop-down list (Pending Key).

Step 3 Click **Next**. The page refreshes and a FS Encryption Password Key ID is displayed.

The first time you configure this page, options to **Remove** or **Download** the encryption key become visible. The **Upload** option is available if you have NFS enabled but do not have a key created. Once you create a key, the **Upload** button changes to **Download**. (If you delete the key, the **Download** button becomes **Upload** again.)

Note If the key correctly matches the one used to create a backup, the Key ID displayed in OpAdmin after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key.

Step 4 Click **Next** to continue.

What to do next

Proceed to [Configure Email Host](#).

Configure Email Host

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

Step 1 Click **Email** in the navigation pane to open the Email configuration page.

Figure 5: Email Configuration

The screenshot shows the ThreatGRID Appliance Administration Portal interface. The main navigation pane on the left includes 'Configuration' (with sub-items: Network, License, NFS, Clustering, Email, Notifications, Date and Time, Syslog) and 'Other' (with sub-item: Review and Install). A 'Start Installation' button is located below the navigation pane. The main content area is titled 'Email' and contains the 'SMTP Configuration' section. This section includes several rows of settings, each with a 'HELP' icon and a dropdown menu:

- Delivery Mode:** Upstream Relay
- Upstream Host:** smtp.acme.test
- Port:** 587
- SSL:** Detect from Port
- Upstream Authentication:** No Authentication
- From Address:** (empty field)

A green 'Next >' button is positioned at the bottom right of the configuration area. At the bottom of the page, there are links for 'Visit the Cisco Threat Grid homepage', 'Documentation', 'Support', and 'License', along with the ThreatGRID logo.

Step 2 Enter the name of the **Upstream Host** (email host).

Step 3 Change the port from 587 to **25**.

Step 4 Keep the defaults for the other settings.

Step 5 Click **Next** to continue.

What to do next

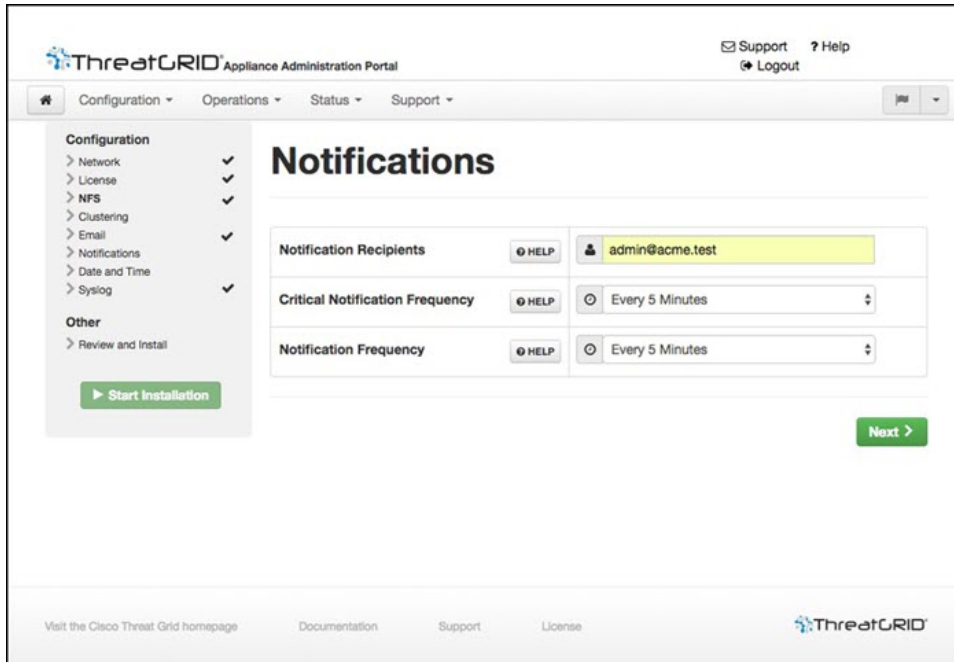
Proceed to [Configure Notifications](#).

Configure Notifications

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.

Step 1 Click **Notifications** in the navigation pane to open the Notifications configuration page.

Figure 6: Notifications Configuration



Step 2 In the **Notification Recipients** field, enter one or more email addresses separated by commas.

Step 3 Choose the **Critical Notification Frequency** and the **Notification Frequency** from the drop-down menus.

Step 4 Click **Next** to continue.

What to do next

Proceed to [Configure Date and Time \(NTP Server\)](#).

Configure Date and Time (NTP Server)

The next step is to identify the Network Time Protocol (NTP) servers.

Step 1 Click **Date and Time** in the navigation pane.

Step 2 Enter the **NTP Server(s)** IP or NTP name.

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

Step 3 Ignore the **Current System Time** and **Synchronize with Browser** fields.

Step 4 Click **Next** to continue.

What to do next

Proceed to [Configure Syslog](#).

Configure Syslog

The Syslog page is used to configure a Syslog server to receive syslog messages and Thread Grid notifications.

Step 1 Click **Syslog** in the navigation pane.

Step 2 Complete the information on page and click **Next** to continue.

See the [Cisco Threat Grid Appliance Administrator Guide](#) for more information.

What to do next

Proceed to [Review and Install Configuration Settings](#).

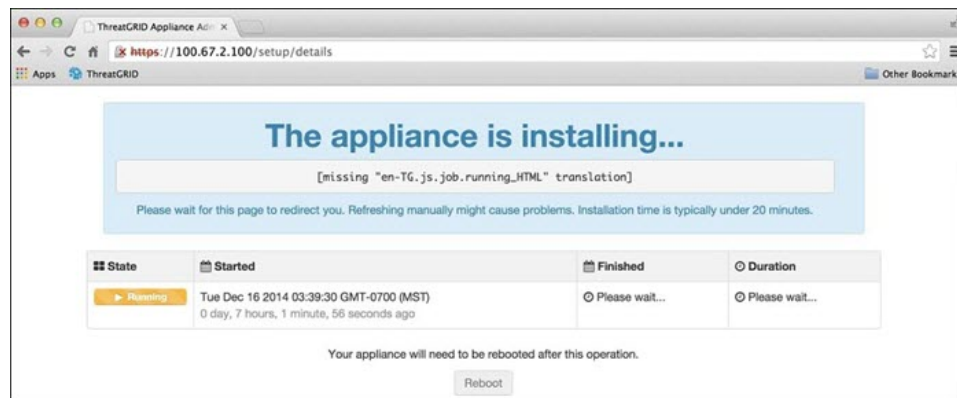
Review and Install Configuration Settings

The final step in the workflow is to review and install your network configuration settings.

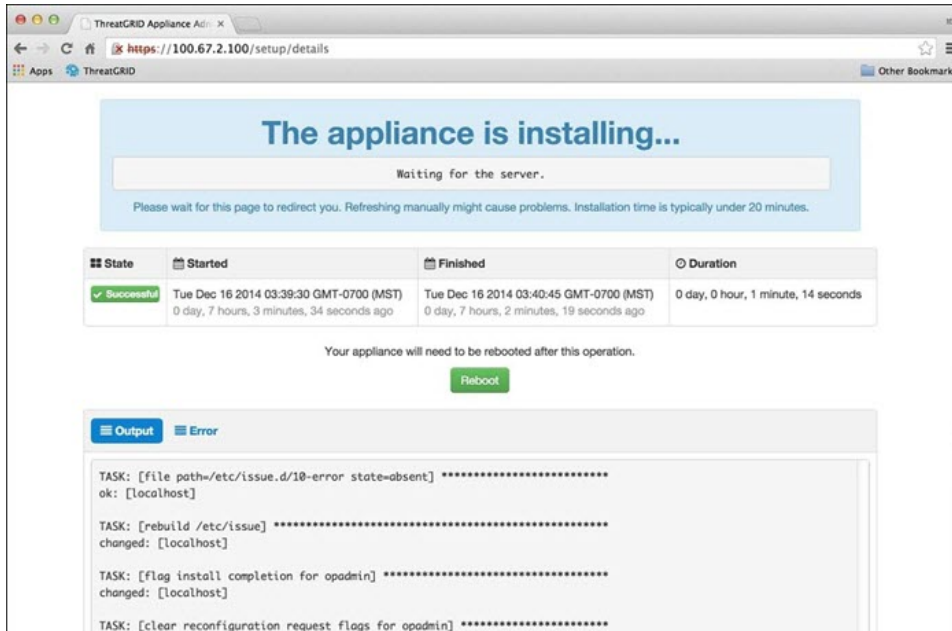
Step 1 Click **Review and Install** in the navigation pane and then click **Start Installation** to begin installing the configuration scripts.

Note The installation may take over 10 minutes to complete. The screen displays configuration information as it is applied.

Figure 7: Appliance Is Installing



After successful installation, the **State** changes from *Running* to *Successful*, and the **Reboot** button becomes enabled (green). The configuration output is also displayed.

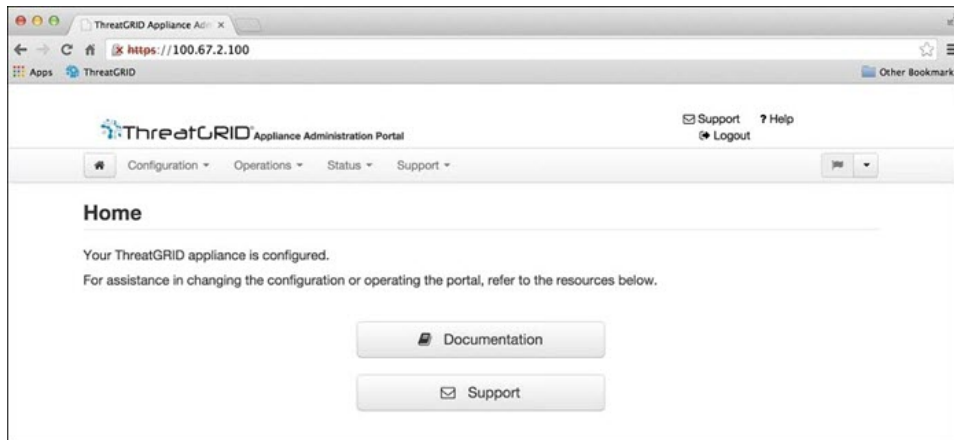
Figure 8: Successful Appliance Installation**Step 2** Click **Reboot**.

Note Rebooting may take up to 5 minutes. Do not make any changes while the appliance is rebooting.

Figure 9: Appliance Is Rebooting

Once the appliance has successfully rebooted, a message is displayed on the Home page indicating that your appliance is configured.

Figure 10: Appliance Successfully Configured



The appliance configuration is complete.

Install 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.

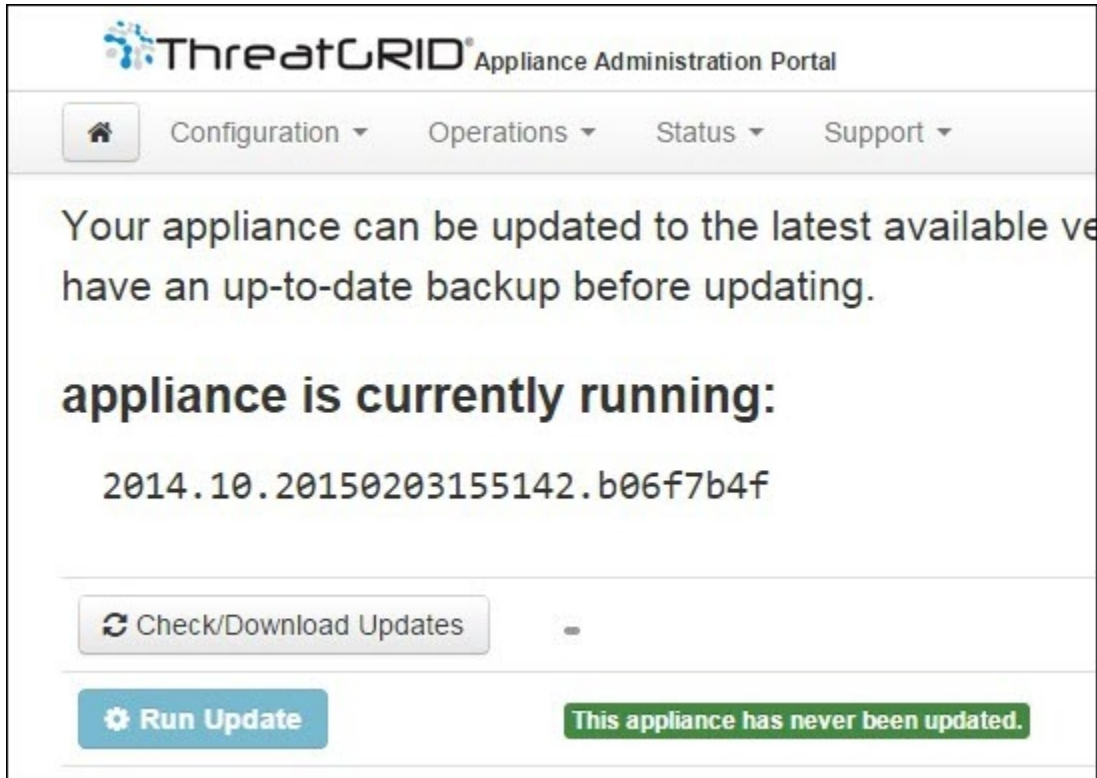


Note For more information about installing updates, see the [Cisco Threat Grid Appliance Administrator Guide](#).

Step 1 If you are not already in the OpAdmin portal, log in to the portal.

Step 2 From the **Operations** menu, choose **Update Appliance** to open the Updates page, which displays the current build of the appliance.

Figure 11: Appliance Build Number



Note See the [Cisco Threat Grid Appliance Version Lookup Table](#) for the corresponding release version.

Step 3 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, downloads it. This may take some time.

Step 4 Once the updates have been downloaded, click **Run Update** to install them.

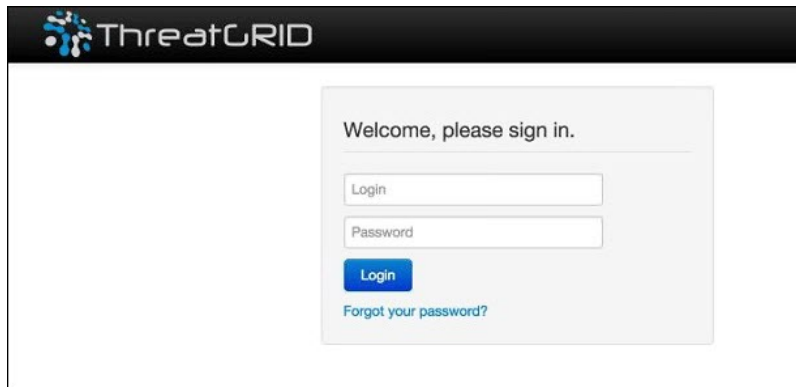
Test Appliance Setup

Once the Threat Grid Appliance is updated to the current version, you should test that it has been configured properly by submitting a malware sample to Threat Grid.

Step 1 Sign in to the Threat Grid Portal using the address you configured as the Clean interface.

The Threat Grid login page opens.

Figure 12: Threat Grid Portal Login



Step 2 Enter the default **Login** (admin) and **Password** (changeme).

Step 3 Click **Login** to open the main Threat Grid Sample Analysis page.

Step 4 In the **Submit a Sample** box located in the upper-right corner, select a sample file or enter a URL to submit for malware analysis.

Step 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.

What to do next

Once the Threat Grid Appliance has been set up and initial configuration is completed, additional tasks can be performed by the appliance administrator, such as managing SSL certificates and adding users. See the [Cisco Threat Grid Appliance Administrator Guide](#) for information about administrator tasks.

