



Admin UI Configuration

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

- [Introduction, on page 1](#)
- [Configuration Wizard, on page 4](#)
- [Install Threat Grid Appliance Updates, on page 14](#)
- [Test the Appliance Setup, on page 15](#)

Introduction

The Admin UI is the recommended tool for administrators to use to configure the Threat Grid 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 Admin UI Admin Password
- Review End User License Agreement
- Configure Network Settings
- Install License
- Configure NFS
- Configure Clustering
- Configure Email
- Configure Notifications
- Configure Date and Time
- Configure System Log
- Review and Install Configuration Settings



Note Not all configuration steps are completed using the configuration wizard. See the [Cisco Threat Grid Appliance Administration 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.

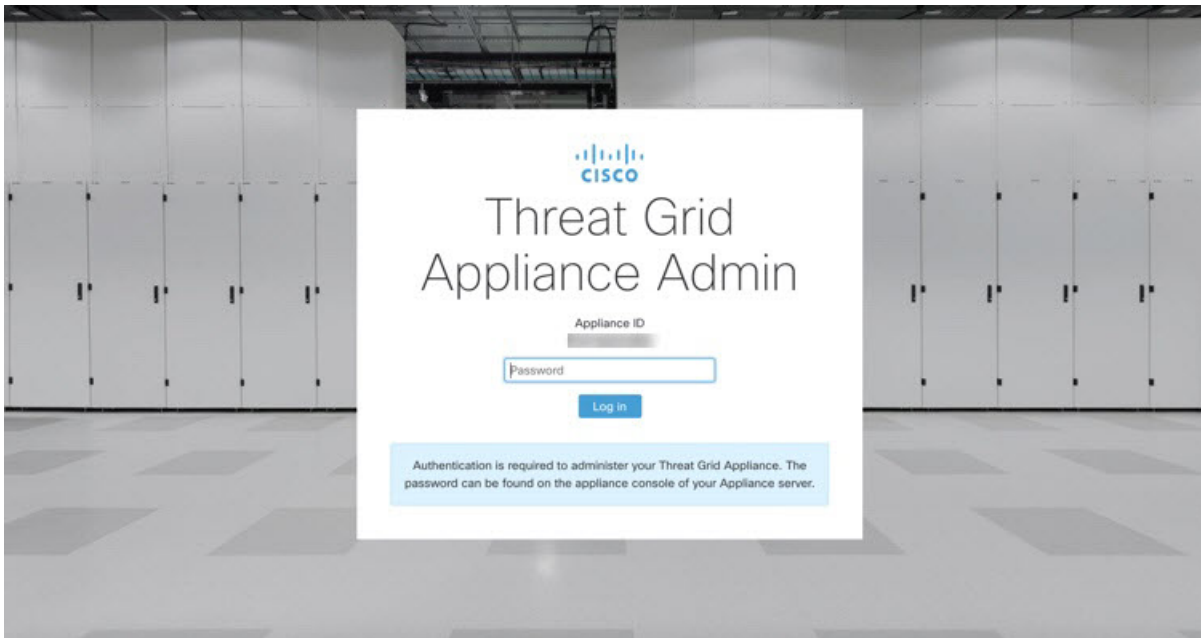
Log In to the Admin UI

Perform the following steps to log in to the Threat Grid Admin UI.

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

Note The Hostname is the appliance serial number.

Figure 1: Admin UI Login Screen



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

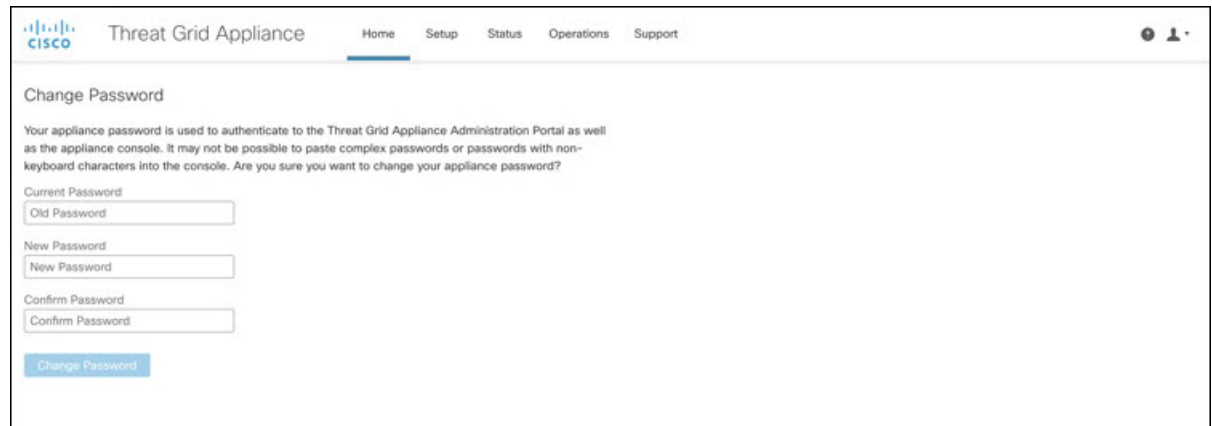
What to do next

Proceed to [Change Admin Password](#).

Change Admin Password

The initial Admin password was generated randomly during the pre-ship Threat Grid installation and is visible as plain text in the TGS dialog. You must change the initial Admin password before continuing with the configuration.

Figure 2: Change Admin Password



The screenshot shows the 'Change Password' page in the Threat Grid Appliance administration portal. The page has a header with the Cisco logo and navigation links for Home, Setup, Status, Operations, and Support. The main content area is titled 'Change Password' and contains a warning message: 'Your appliance password is used to authenticate to the Threat Grid Appliance Administration Portal as well as the appliance console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the console. Are you sure you want to change your appliance password?'. Below the warning are three input fields: 'Current Password' (with a sub-label 'Old Password'), 'New Password', and 'Confirm Password' (with a sub-label 'Confirm Password'). A blue 'Change Password' button is located at the bottom of the form.

Step 1 Enter the old password from the TGS dialog in the **Current Password** field. (You should have this password saved in a text file.)

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

The new password must contain the following: 8 characters minimum, one number, one special character, at least one uppercase and one lowercase character.

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

Note The new password will not be displayed in visible text in the TGS 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 TGS Dialog, the IP addresses displayed on the **Network Configuration** page reflect the values you entered in the TGS Dialog during the Threat Grid Appliance network configuration.

Figure 3: Network Configuration

The screenshot displays the 'Network Configuration' page in the Threat Grid Appliance admin UI. On the left, a 'Configuration Wizard' sidebar lists steps: 1. Network (Configure Networking), 2. License (Upload license), 3. NFS (Configure NFS), 4. Clustering (Configure Clustering), 5. Email (Configure Email), 6. Notifications (Configure Notifications), 7. Date and Time (Configure Date and Time), 8. System Log (Configure Logging), and 9. Review and Install (Done!). The main content area is titled 'Network Configuration' and is divided into two sections: 'CLEAN interface' and 'DIRTY interface'. Each interface section shows a 'MAC Address' field, an 'IP Address' field (with '(DHCP)' next to it), an 'IP Assignment' dropdown menu set to 'DHCP', a 'Host Name' text input field, a 'Primary DNS Server' text input field (with 'IP' below it), and a 'Secondary DNS Server' text input field (with 'IP' below it). The 'DIRTY interface' section also includes a warning icon next to the 'IP Address' field, indicating it is 'Unassigned (DHCP)'.

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 Administration Guide](#).

What to do next

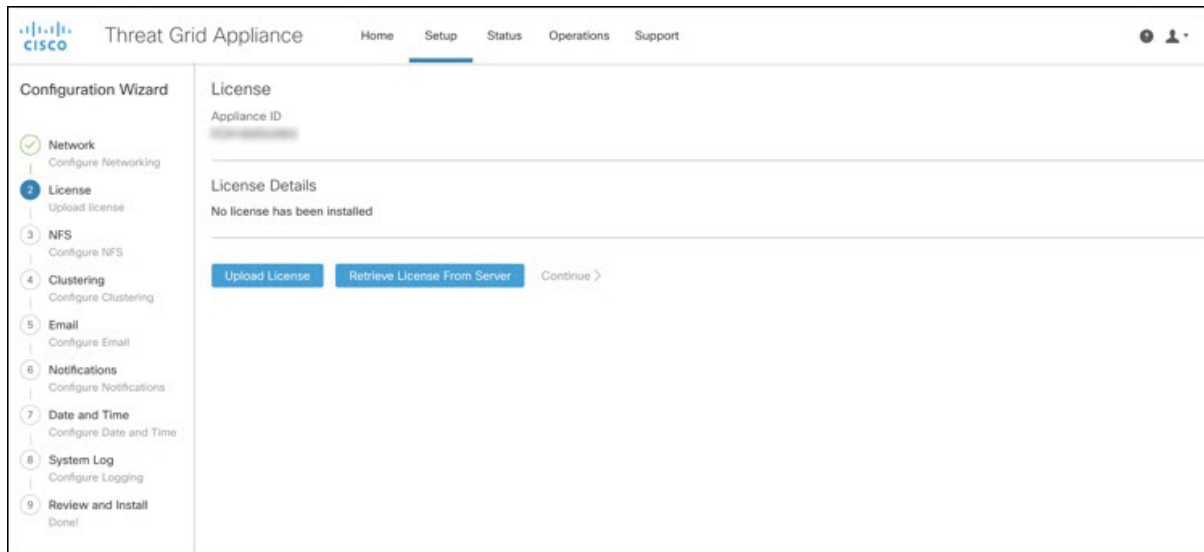
Proceed to [Install License](#).

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 4: License Page Prior to Installation



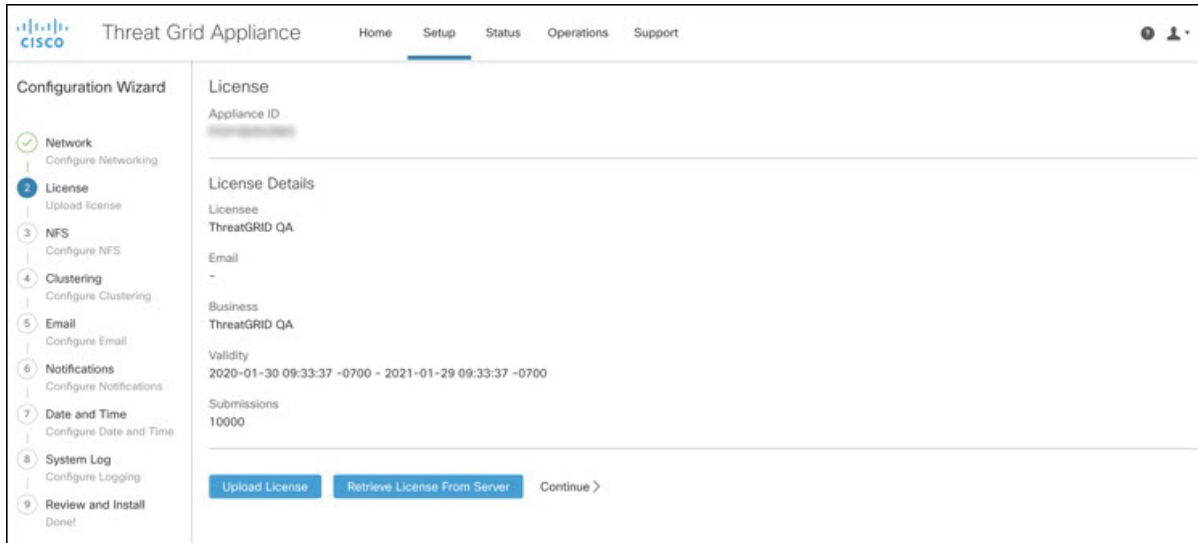
Step 2 Click **Upload License** and select the license file from your file manager.

Alternatively, you can retrieve the license from the server. If the appliance has network access when being installed, click **Retrieve License From Server** to get the license over the network.

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

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

Figure 5: License Information After Successful Installation



Step 5 Click **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 the NFS Requirements section in the *Cisco Threat Grid Appliance Administration Guide* for more information.

The configuration process includes mounting the NFS store, mounting the encrypted data, and initializing the Threat Grid Appliance local datastores from the contents of the NFS store.

If you would like to skip this step or continue and return later, click **Continue without NFS**.

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

Figure 6: NFS Configuration

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.
- **Options** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4. The default is **rw**.
- **FS Encryption Key Hash** - Click **Generate Key** to generate a new encryption key. You will need this key to restore backups later. (At that time, click **Upload** and upload the key required for the backup.)

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

The first time you configure this page, options to **Delete** 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 Admin UI after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key.

Step 4 Click **Activate** to activate the key. The Activating Key dialog is displayed.

Step 5 When activation has succeeded, click **Continue**.

What to do next

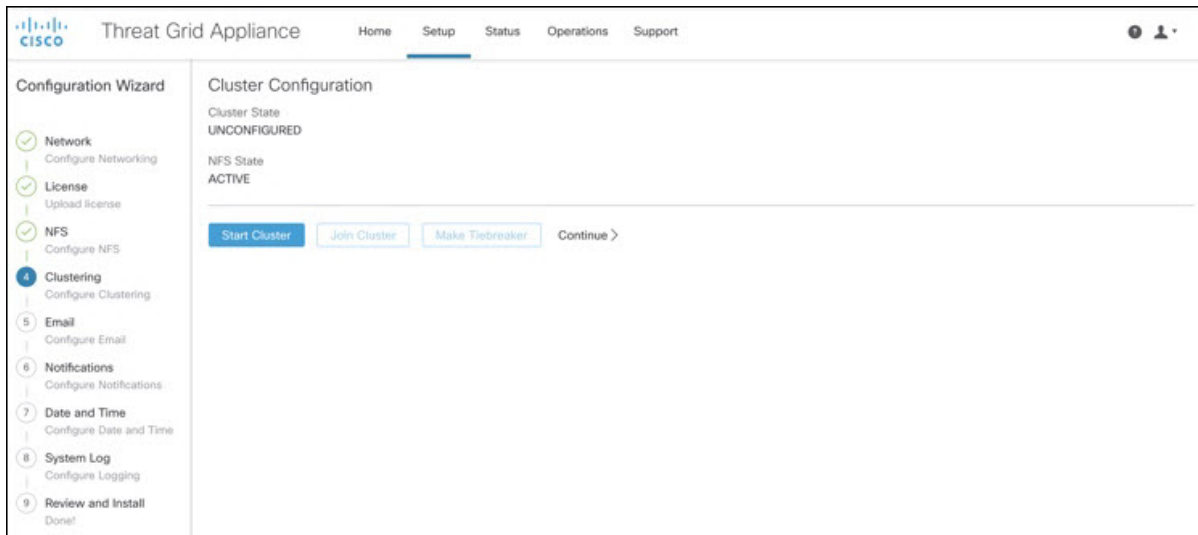
Proceed to [Configure Clustering](#).

Configure Clustering

The next step in the wizard workflow is to configure clustering.

Step 1 Click **Clustering** in the navigation pane to open the **Cluster Configuration** page.

Figure 7: Cluster Configuration



Step 2 See Clustering in the *Threat Grid Appliance Administration Guide* for more information. We recommend that you skip this step during the initial configuration, and return once configuration is completed.

Step 3 Click **Continue** to move to the next step in the workflow.

What to do next

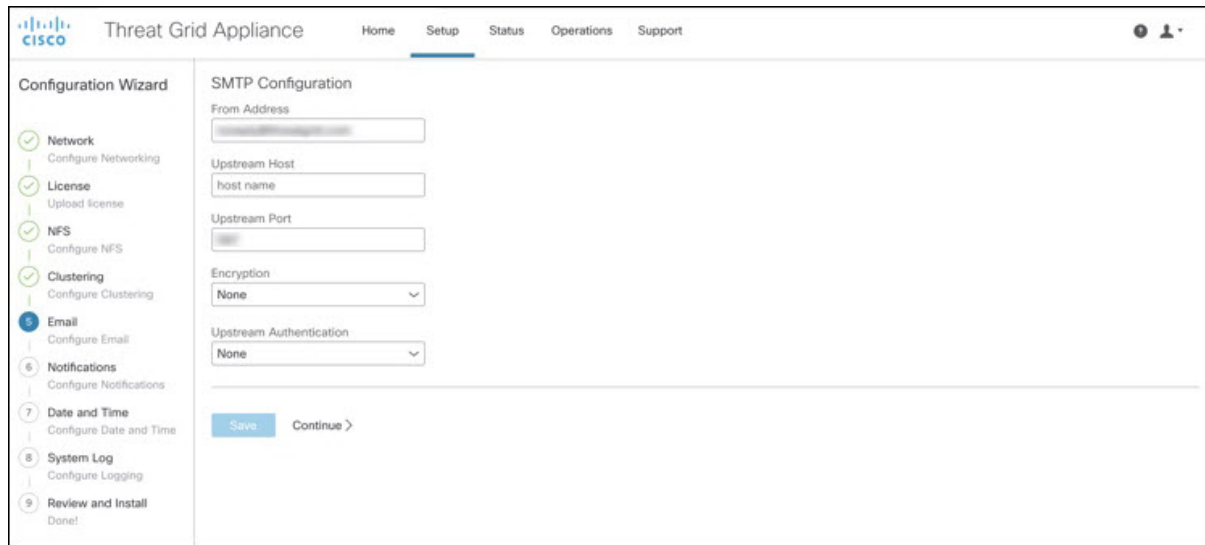
Proceed to [Configure Email](#).

Configure Email

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

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

Figure 8: SMTP Configuration



The screenshot shows the Threat Grid Appliance configuration wizard. The navigation pane on the left lists the following steps: Network (Configure Networking), License (Upload license), NFS (Configure NFS), Clustering (Configure Clustering), Email (Configure Email), Notifications (Configure Notifications), Date and Time (Configure Date and Time), System Log (Configure Logging), and Review and Install (Done!). The main content area is titled "SMTP Configuration" and contains the following fields: "From Address" (text input), "Upstream Host" (text input with "host name" as a placeholder), "Upstream Port" (text input), "Encryption" (dropdown menu set to "None"), and "Upstream Authentication" (dropdown menu set to "None"). At the bottom of the main content area, there are "Save" and "Continue >" buttons.

- Step 2** Enter the email From Address.
- Step 3** Enter the name of the Upstream Host (email host).
- Step 4** Change the port from **587** to **25**.
- Step 5** Keep the defaults for the other settings.
- Step 6** Click **Save** to save your settings.
- Step 7** Click **Continue** to move to the next step in the workflow.

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** page.

Figure 9: Notifications

- Step 2** Under **Recipients**, enter the **Email Address** for at least one notifications recipient. If you need to add multiple email addresses, click the + icon to add another field; repeat as needed.
- Step 3** Under **Notification Frequency**, choose the settings for **Critical** and **Non-critical** from the drop-down lists.
- Step 4** Click **Save**.
- Step 5** Click **Continue** to move to the next step in the workflow.

What to do next

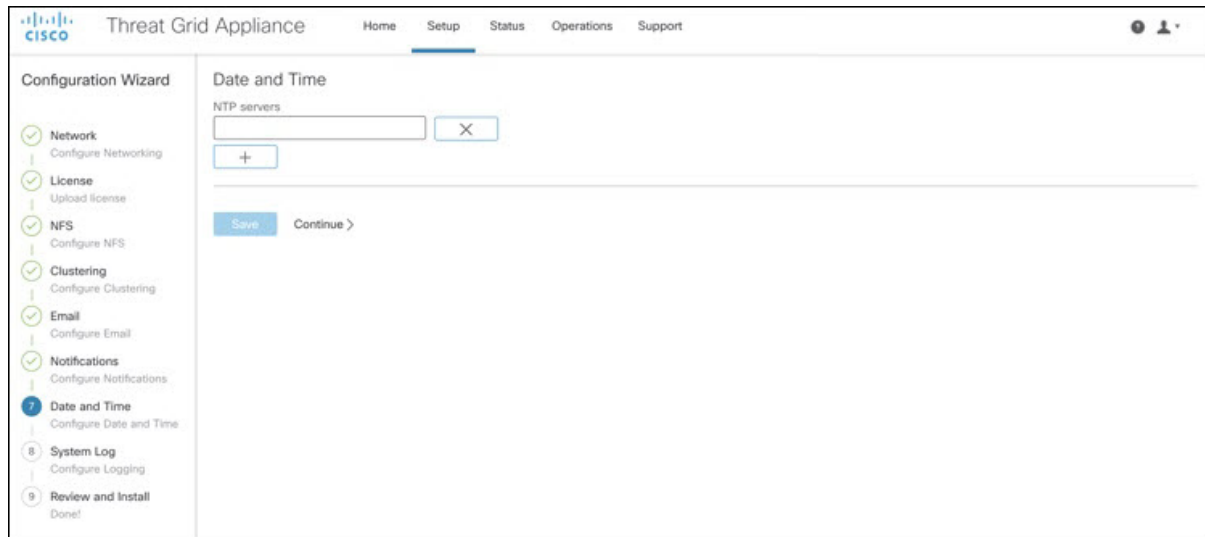
Proceed to [Configure Date and Time](#).

Configure Date and Time

The next step is to specify the Network Time Protocol (NTP) servers to configure the date and time.

- Step 1** Click **Date and Time** in the navigation pane to open the **Date and Time** page.

Figure 10: Date and Time



The screenshot shows the Cisco Threat Grid Appliance configuration wizard. The left sidebar lists the configuration steps: Network, License, NFS, Clustering, Email, Notifications, Date and Time (highlighted with a blue circle), System Log, and Review and Install. The main content area is titled "Date and Time" and contains a section for "NTP servers". There is a text input field, a clear button (X), and an add button (+). Below the input field are "Save" and "Continue >" buttons.

- Step 2** Enter the **NTP Server(s)** IP or NTP name.
If there are multiple NTP servers, click the + icon to add another field; repeat as needed.
- Step 3** Click **Save**.
- Step 4** Click **Continue** to move to the next step in the workflow.
-

What to do next

Proceed to [Configure System Log](#).

Configure System Log

The **System Log Server Information** page is used to configure a system log server to receive syslog messages and Thread Grid notifications.

- Step 1** Click **System Log** in the navigation pane to open the **System Log Server Information** page.

Figure 11: System Log Server Information

The screenshot shows the Cisco Threat Grid Appliance Admin UI. The top navigation bar includes 'Home', 'Setup', 'Status', 'Operations', and 'Support'. The 'Setup' tab is active. On the left, a 'Configuration Wizard' sidebar lists steps: Network, License, NFS, Clustering, Email, Notifications, Date and Time, System Log (highlighted with a blue circle), and Review and Install. The main content area is titled 'System Log Server Information' and contains three input fields: 'Host URL' (empty), 'Host Port' (531), and 'Protocol' (TCP). Below these fields are 'Save' and 'Continue >' buttons.

Step 2 Complete the Host URL, Host Port, and Protocol fields and click **Save**.

Step 3 Click **Continue** to move to the final step in the workflow.

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

What to do next

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

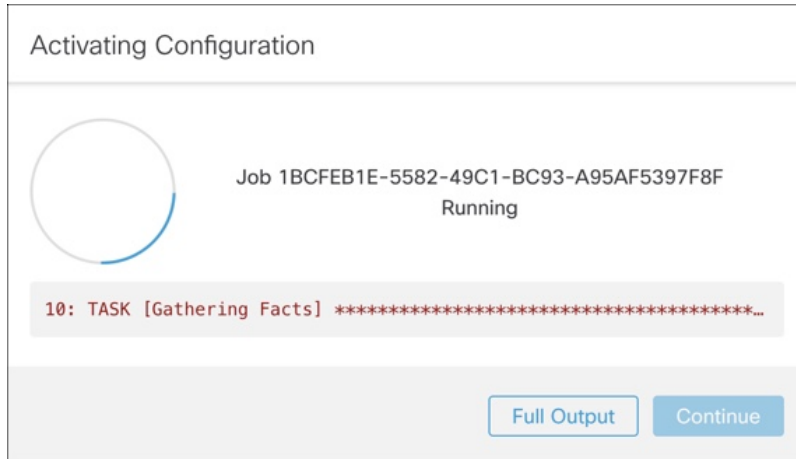
Review and Install Configuration Settings

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.

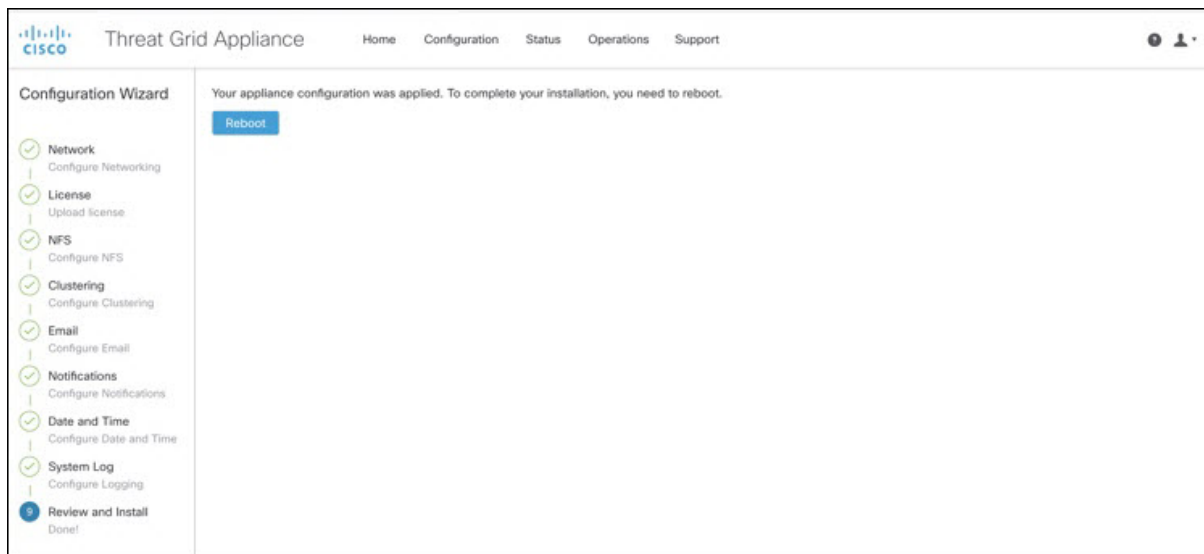
Note The installation may take over 10 minutes to complete. The screen displays configuration information as it is applied.

Figure 12: Activating Configuration



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

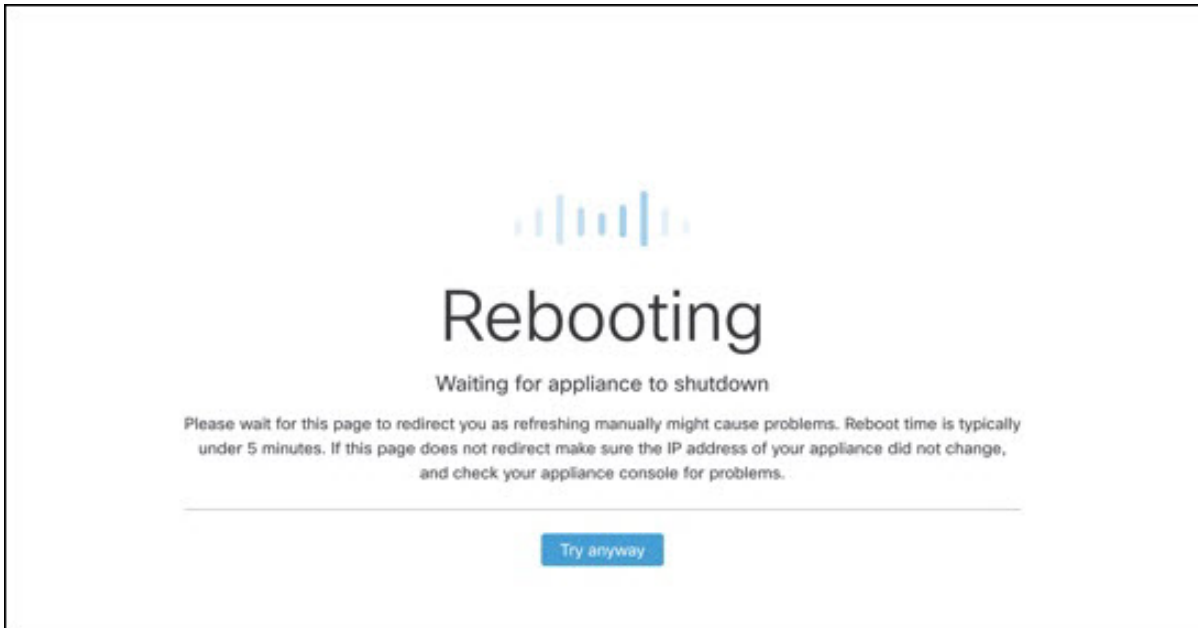
Figure 13: Successful Appliance Installation



Step 2 Click **Reboot**.

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

Figure 14: Appliance is Rebooting



After reboot, the appliance opens to the Admin UI **Home** page. This completes the configuration process.

Install Threat Grid Appliance 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 Admin UI.

Users with air-gapped implementations may contact [Threat Grid Support](#) and request a downloadable update boot image.

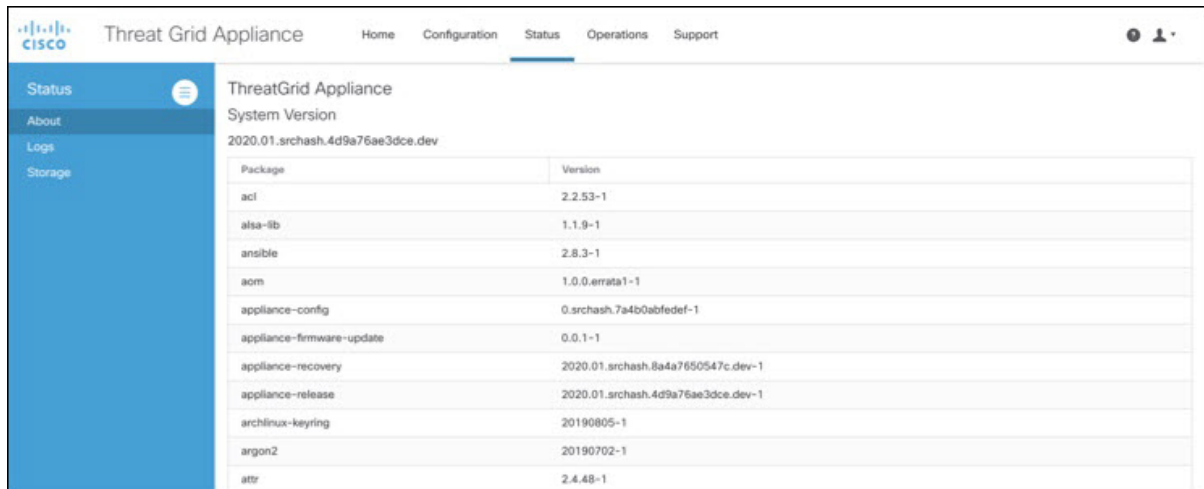


Note For more information about installing updates, see the [Cisco Threat Grid Appliance Administration Guide](#).

Step 1 Log in to the Admin UI, if you are not already logged in.

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

Figure 15: Appliance Build Number



The screenshot shows the Threat Grid Appliance Status page. The page title is "ThreatGrid Appliance" and the system version is "2020.01.srchash.4d9a76ae3dce.dev". A table lists installed packages and their versions.

Package	Version
acl	2.2.53-1
alsa-lib	1.1.9-1
ansible	2.8.3-1
aom	1.0.0.errata1-1
appliance-config	0.srchash.7a4b0abfedef-1
appliance-firmware-update	0.0.1-1
appliance-recovery	2020.01.srchash.8a4a7650547c.dev-1
appliance-release	2020.01.srchash.4d9a76ae3dce.dev-1
archlinux-keyring	20190805-1
argon2	20190702-1
attr	2.4.48-1

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

Step 3 Click **Check for Updates**.

A check is run 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 **Apply Update** to install them.

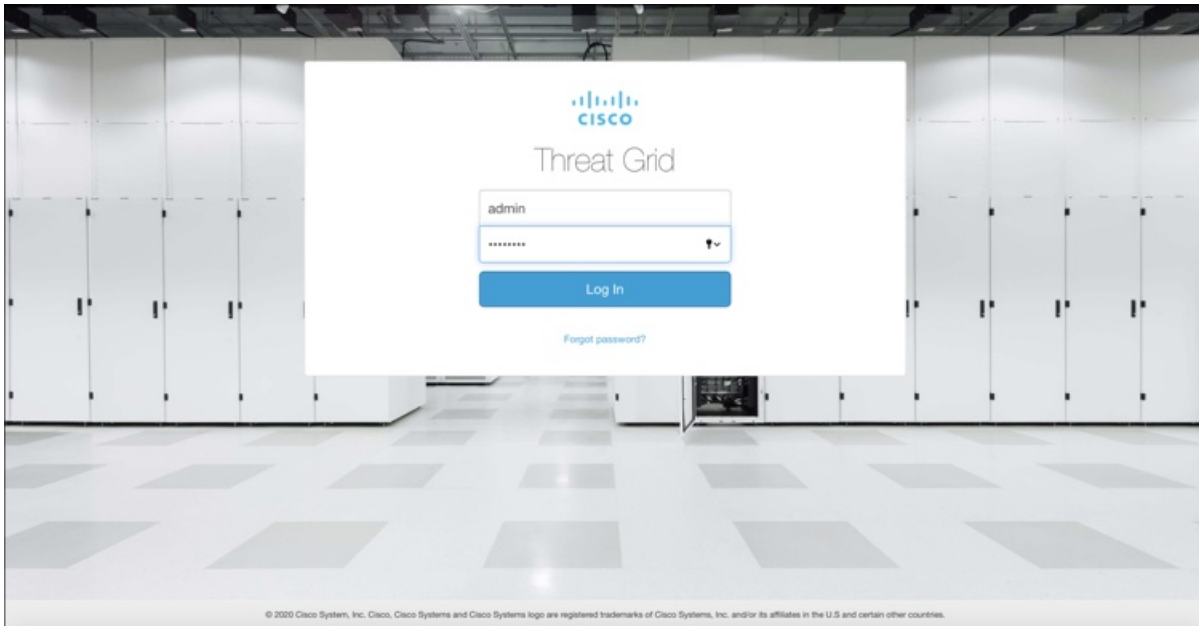
Test the Appliance Setup

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 In a browser, open Threat Grid using the address you configured as the Clean interface.

The Threat Grid login page opens.

Figure 16: Threat Grid Login

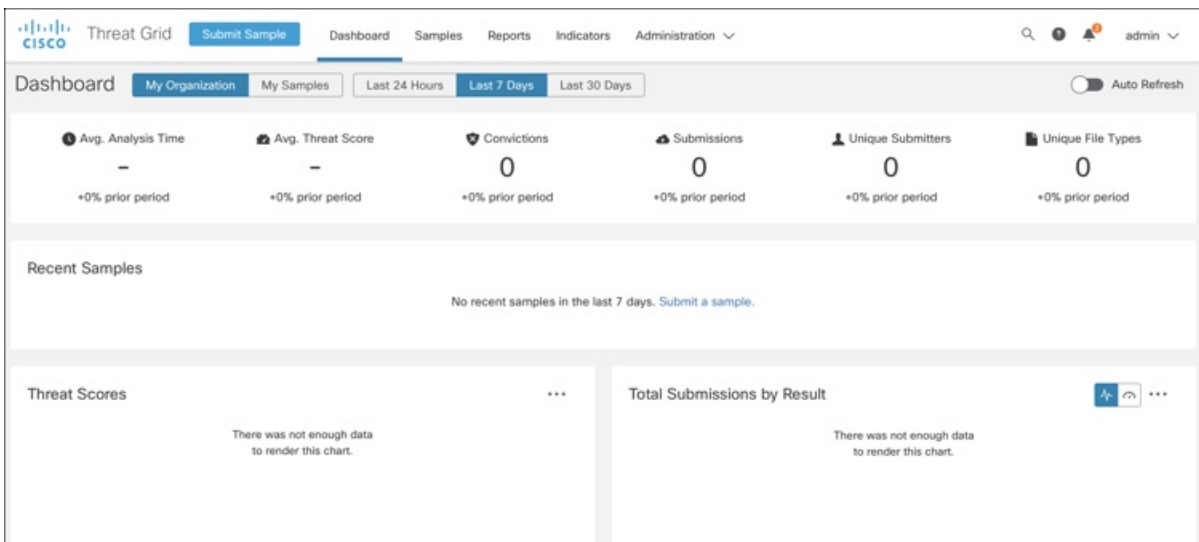


Step 2 Enter the default credentials:

- **Login** - admin
- **Password** - Use the new password entered during the first step of the Admin UI configuration workflow. We encourage you to change it for the portal when you have a chance.

Step 3 Click **Log In** to open the main **Threat Grid** dashboard. There will be no sample data available yet.

Figure 17: Threat Grid Dashboard



Step 4 Click **Submit a Sample** to open the sample submission dialog.

Figure 18: Submit Sample

Submit Sample

Submission Type

URL

Sample Name

Options

Tags
zeus, spy-eye, etc...

Access Mark private

Notification Email me when analysis is complete

Virtual Machine

Playbook

> Description

Network Simulation

No network traffic will be simulated.

Note There is help available at the bottom of this form, describing sample submission file types, size, and other information. You can also click the ? icon located in the upper-right corner to view the Threat Grid Release Notes and online help, including complete documentation on how to submit a sample and review the analysis results.

Step 5 Upload a file or enter a URL to submit for malware analysis. Leave the other options set at the defaults if you are not yet sure what they mean.

Step 6 Click **Submit**.

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 **Samples** page. Once analysis is completed, the results should be available in the Analysis Report.

Figure 19: Analysis Report

The screenshot shows the Cisco Threat Grid interface for an analysis report. The top navigation bar includes 'Threat Grid', 'Submit Sample', 'Dashboard', 'Samples', 'Reports', 'Indicators', and 'Administration'. The user is logged in as 'admin'. The report title is 'Report / Samples / Burning Daylight.pdf'. The main content area is divided into sections: Metrics, Metadata, and Behavioral Indicators. The Metrics section shows a Threat Score of 56. The Metadata section is split into two columns of key-value pairs.

Metadata	
Sample ID	81dfa29471f3edc0b360c1b312db2f1b
Submitted By	admin
OS	Windows 7 64-bit
Started	4/30/20 11:49:47 am
Ended	4/30/20 11:56:55 am
Duration	0:07:08
Sandbox	FCH1825V2W3
Playbook	No Playbook Applied
Network Exit	LO - Local - Dirty Network Interface
Localization	
Filename	Burning Daylight.pdf
Magic Type	PDF document, version 1.5
File Type	pdf
First Seen	4/30/20 11:49:40 am
Last Seen	4/30/20 11:49:40 am
SHA-256	c3ed5099be47d523b34ab502f49392d2fd4e...
SHA-1	73ec32bc9e15ab2d750ca422796ba056a662db9c
MD5	c9b22fcf4e8704833b069d9451d7eaa6
Tags	

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 Administration Guide](#) for information about administrator tasks.