Threat Grid Appliance Administrator's Guide

Version: 2.2.4

Updated: 7/10/2017

Cisco Systems, Inc. www.cisco.com

All contents are Copyright © 2015-2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Cisco Threat Grid Appliance Administrator's Guide

CONTENTS

LIST OF FIGURES

INTRODUCTION

A Cisco Threat Grid Appliance ("TGA") provides the complete Threat Grid malware analysis platform installed on a single Cisco UCS server (UCS C220-M3 or UCS C220 M4). Threat Grid Appliances provide a safe and highly secure on-premises environment for performing advanced malware analysis, with detailed threat analytics and content.

Many organizations that handle sensitive data, such as banks, insurance companies, healthcare services, etc., must follow various regulatory compliance rules, policy restrictions, and other guidelines that prohibit certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Threat Grid Appliance on-premises, these organizations are able to send suspicious documents and files to the appliance to be analyzed without ever leaving the network.

With an Threat Grid Appliance, security teams can analyze all samples using proprietary and highly secure static and dynamic analysis techniques. The appliance correlates the analysis results with hundreds of millions of previously analyzed malware artifacts, to provide a global view of malware attacks and campaigns, and their distributions.

A single sample of observed activity and characteristics can quickly be correlated against millions of other samples to fully understand its behaviors within an historical and global context. This ability helps security teams to effectively defend the organization against threats and attacks from advanced malware.

Who This Guide Is For

This document is the TGA administrator's guide. It describes how to get started with a new Threat Grid Appliance, and how to manage the appliance for optimum malware analysis. This guide also provides information for administrators who are integrating the Threat Grid Appliance with other Cisco products and services, such as ESA and WSA appliances and AMP for Endpoints Private Cloud devices.

For information about Threat Grid Appliance setup and configuration, please see the *Threat Grid Appliance Setup and Configuration Guide*, which is available on the Threat Grid Appliance product documentation page.

GETTING STARTED

A Cisco Threat Grid Appliance is a Linux server that has been installed prior to shipping with all components necessary to analyze samples. After a new appliance is received, it must first be set up and configured for the on-premises network environment.

Once the server is up and running, the Threat Grid Appliance administrator is responsible for managing organizations and users for the Threat Grid malware analysis tool, as well as appliance updates, backups, and for performing other server administration tasks.

Updates

We recommend updating the appliance prior to use, in order to ensure that all the latest features and security updates are installed.

Check for new release updates and install them, as described in the *Installing Updates* section.

Documentation

Threat Grid Appliance documentation (including this document, the *Threat Grid Appliance Setup and Configuration Guide*, a formatted version of the Release Notes, integration guides, etc.) is available on the internal resources page on the Cisco.com website: *Threat Grid Appliance product documentation page*. This page contains links to documentation for the current and older appliance releases.

Threat Grid Appliance Setup and Configuration Guide

The *Threat Grid Appliance Setup and Configuration Guide* is the companion to the current document. It contains detailed setup information, including network interfaces, suggested firewall rules, network diagram, configuration instructions, and other tasks.

Threat Grid Appliance Release Notes

OpAdmin Portal > **Operations > Update Appliance > Release Notes**

Note: A formatted, PDF version of the Threat Grid Appliance Release Notes is also available on the **Install and Upgrade Guides** page – see link above.

Threat Grid Portal Release Notes

Portal UI Navigation bar > **Help > Release Notes**

Threat Grid Portal Online Help and API Documentation

The Threat Grid Portal's *Using Threat Grid* Online Help, API documentation, and other information is available from the main Threat Grid Portal Help page:

Threat Grid Portal user interface >Navigation bar > Help

The **Help** home page opens, with links to the documentation.

ESA/WSA Appliance Documentation

For information on connecting an ESA or WSA appliance with a Threat Grid Appliance, see Connecting ESA/WSA Appliances to a Threat Grid Appliance.

See the instructions for *"Enabling and Configuring File Reputation and Analysis Services"* in the online help or user guide for your ESA/WSA.

- The ESA user guides are located here: http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
- The WSA user guides are located here: http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

Licensing

The Threat Grid license is managed in the *OpAdmin Configuration License* page:

Configuration > License

For questions about licenses, please contact support@threatgrid.com.

Rate Limits

The API rate limit is global for the appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions.

Rate limits are based on a window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error, plus a message about how long to wait before retrying. See the Threat Grid portal UI FAQ entry on rate limits for a more detailed description.

Assumptions

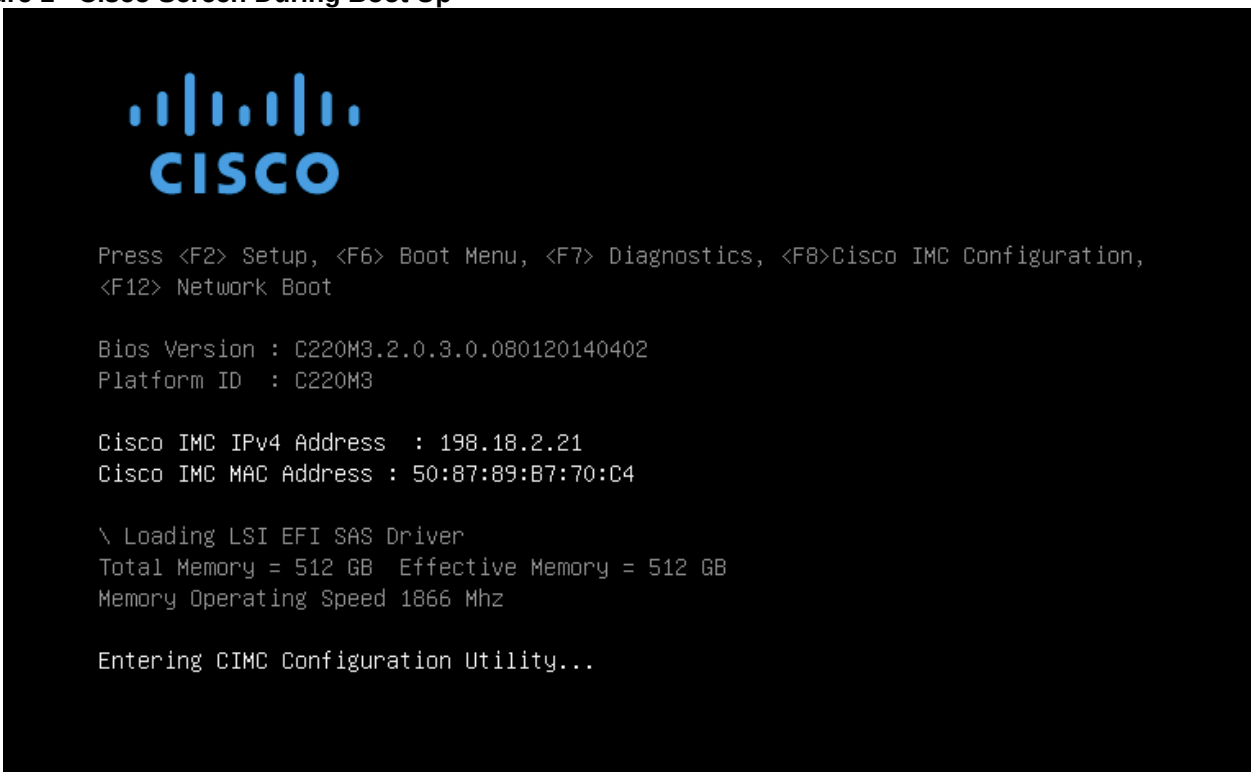
This guide assumes that the initial setup and configuration steps have been completed as described in the *Threat Grid Appliance Setup and Configuration Guide,* and that an initial test malware sample has been successfully submitted and analyzed.

ADMINISTRATION

Power On

Turn on the Appliance and wait for it to boot up. The Cisco screen is displayed briefly:

Figure 1 - Cisco Screen During Boot Up

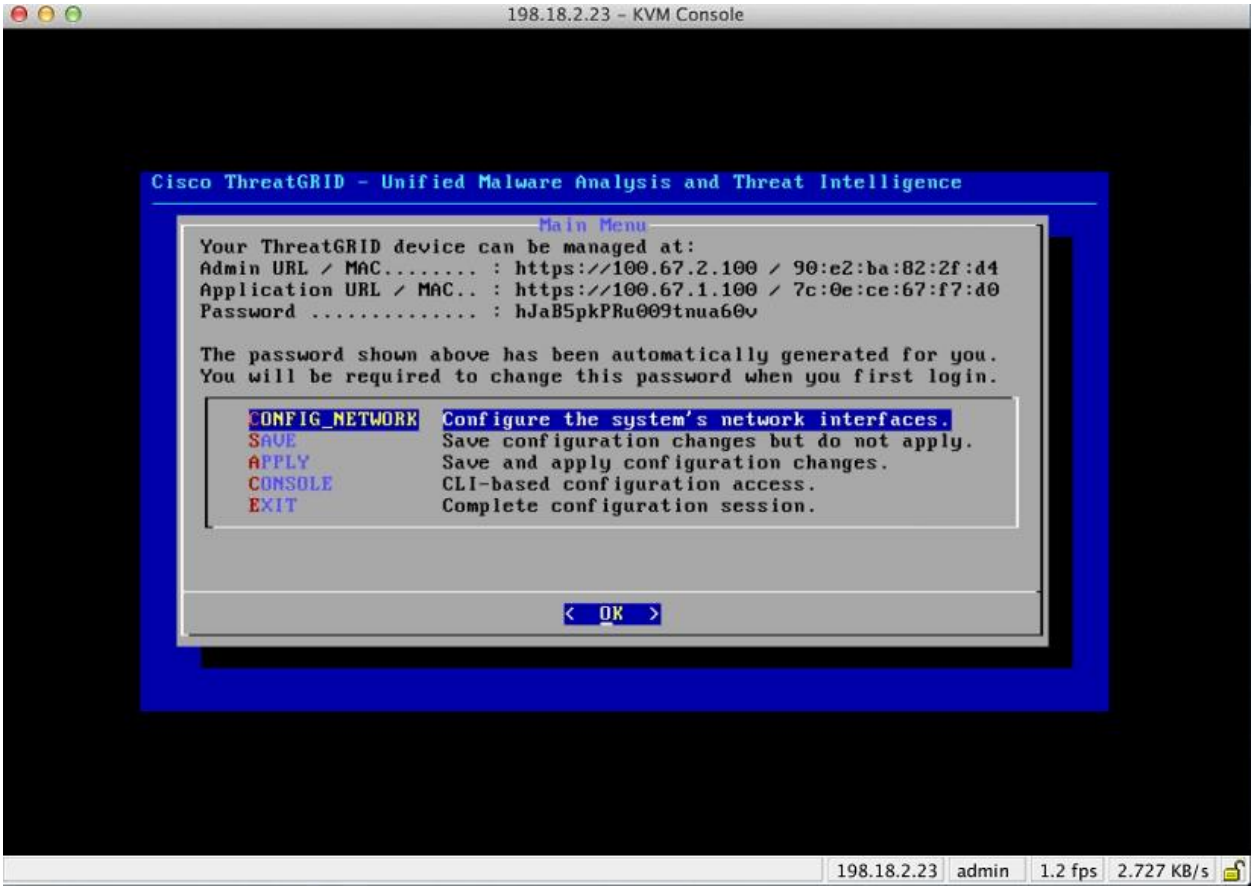


Note: If you want to configure the CIMC interface, press **F8** after the memory check is completed.

For more information, see the section, *Configuring CIMC*, located in the Threat Grid Appliance Setup and Configuration Guide.

The **TGSH Dialog** is displayed on the console when the server has successfully booted up and connected.

Figure 2 - TGSH Dialog



Note: After the TG appliance has been setup and configured, the TGSH Dialog will no longer display the Password, which you need in order to access and configure the OpAdmin interface.

Lost Password: If you lose this password in the future, see Lost Password Recovery for instructions.

Login Names and Passwords - Defaults

Threat Grid Portal UI Administrator

- **Login:** "admin"
- **Password:** "changeme"

TGA Administrator - OpAdmin and threatgrid User

The OpAdmin administrator's password is the same as the "threatgrid" user password. It is maintained in the OpAdmin interface. The default administrator's password was changed during the initial TGA setup, and is not displayed in visible text once that step is completed. If the password is lost and you are unable to login to OpAdmin, follow the **Lost Password Recovery** instructions below.

CIMC (Cisco Integrated Management Controller)

- **Login:** "admin"
- **Password:** "password"

Lost Password Recovery

The default administrator's password is only visible in the TGSH Dialog during the initial appliance setup and configuration. Once the initial configuration is completed the password is no longer displayed in visible text.

Note: LDAP authentication is available for TGSH Dialog and OpAdmin login when you have multiple administrators. If the appliance is configured for LDAP authentication only, resetting the password in recovery mode will reconfigure the authentication mode to allow login with system password as well.

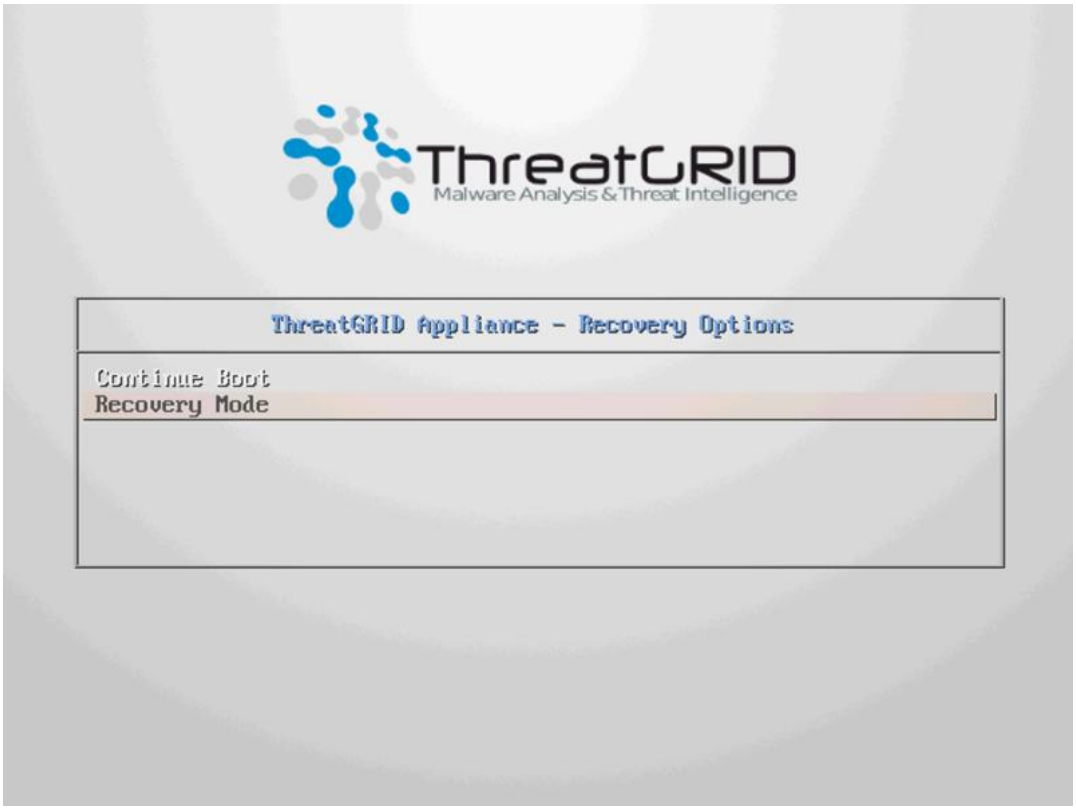
If you lose the administrator's password and are unable to login to OpAdmin, complete the following steps:

Resetting a Lost Administrator's Password

1. Reboot your Appliance.

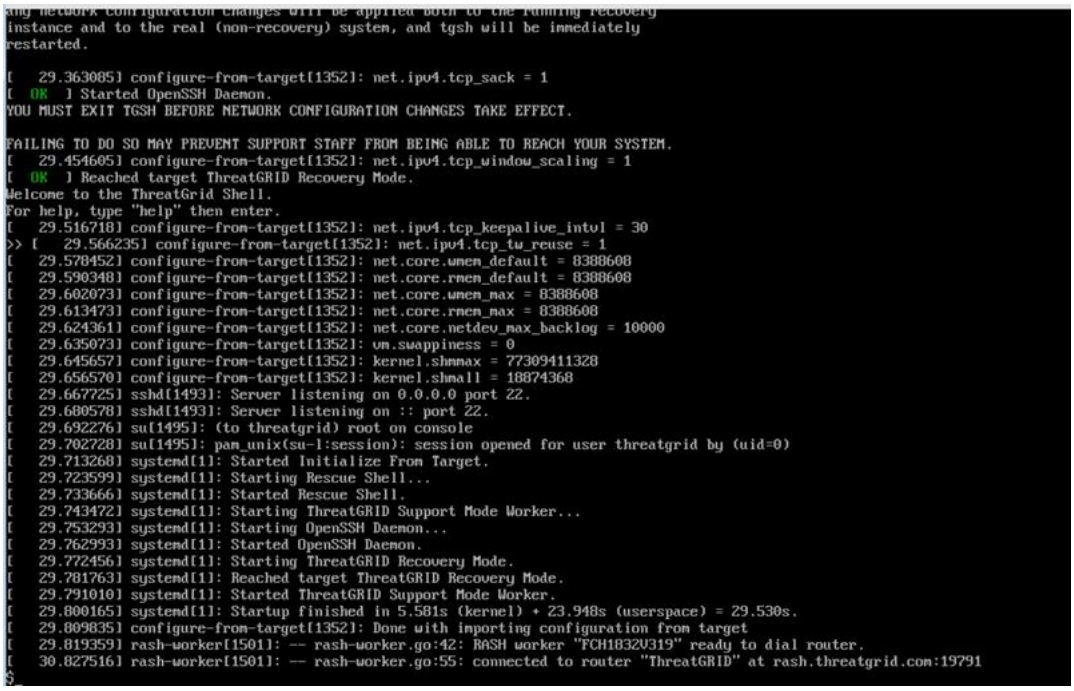
   During the boot, there will be a brief window of time in which you can select Recovery Mode, as shown below:

Figure 3 - Boot Menu - Recovery Mode



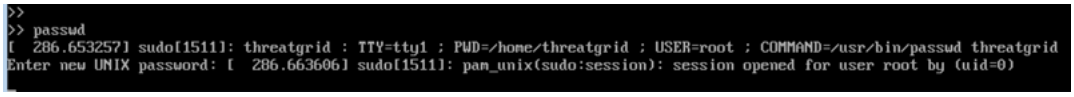
The Threat Grid Shell opens:

Figure 4 - The Threat Grid Shell in Recovery Mode



2. Run `passwd` to change the password:

Figure 5 - Enter a New Password



Note: The command prompt is not always visible in this mode and logging output may be displayed at any point on top of your input. This does not affect input; you can keep typing "blindly".

3. Ignore the 2 lines of logging output. Blindly enter the password, press enter, and then retype the password and enter again. The password will not be displayed.

4. You **MUST** type `exit` from the command line in order for the new password to be saved.

   Rebooting will not save the new password. If you do not `exit` - even though everything appears to be OK - the password change will be quietly discarded.

5. Next, type the command `reboot` and press Enter to start the appliance in normal mode.

Installing Updates

Before you can update the Threat Grid Appliance with newer versions, you must have completed the initial setup and configuration steps as described in the *Threat Grid Appliance Setup and Configuration Guide .*

New Appliances: If you have a new Appliance that shipped with an older version and wish to install updates, you must complete the initial configuration first. Do Not apply the updates until all Appliance configuration is done.

Appliance updates will not download unless the license is installed, and may not apply correctly if the Appliance has not been fully configured, including the database.

Threat Grid Appliance updates are applied through the OpAdmin Portal.

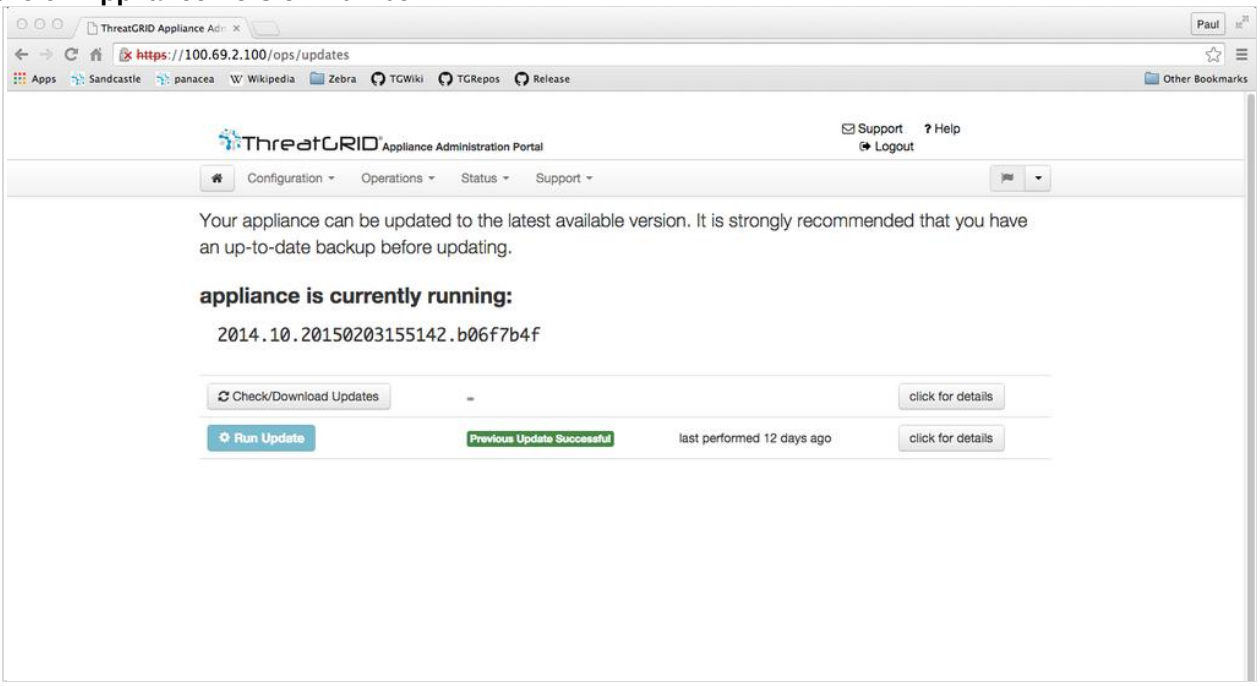
Updates are one-directional: you cannot revert to a previous version after you upgrade to a more recent version.

To test the update, submit a sample for analysis.

1. From the **Operations** menu, select **Update Appliance**.

   The updates page opens, displaying the current build of the Appliance:

Figure 6 - Appliance Version Number



2. Click **Check/Download Updates**. The software checks to see if there is a more recent update/version of the Appliance software, and if so, it is downloaded.

   Note: The download can take some time:

   - Updating from 1.0 to 1.0+hotfix2 takes approximately15 minutes.
   - Applying a full update from 1.0 to 1.3 (without data migration) takes about 30 minutes.

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

Appliance Build Number/Version Lookup Table

The build number of an Appliance can be viewed on the Updates page (OpAdmin **Operations** > **Update Appliance**), as illustrated above.

Appliance build numbers correspond to the following release version numbers:

Build Number	Release Version	Release Date	Notes
2016.05.20170710175041.77c0b12f.rel	2.2.4	7/10/2017	This release introduces Backup functionality.
2016.05.20170519231807.db2f167e.rel	2.2.3	5/20/2017	This minor release allows new factory installations to be run without Windows XP.
2016.05.20170508195308.b8dc88ed.rel	2.2.2	5/8/2017	Minor release of changes to network configuration and operating-system components to support upcoming features.
2016.05.20170323020633.f82e66fe.rel	2.2.1	3/24/2017	Disables SSLv3, fixes a resource issue
2016.05.20170308211223.c92516ee.rel	2.2mfg	3/8/2017	Manufacturing-only changes. No customer impact. Not deployed via update server.
2016.05.20170303034712.1b205359.rel	2.2	3/3/2017	Storage migration, Pruning, Mask UI, Multi-disposition update
2016.05.20170105200233.32f70432.rel	2.1.6	1/5/2017	Adds LDAP Authentication
2016.05.20161121134140.489f130d.rel	2.1.5	11/21/2016	ElasticSearch5; CSA performance fix
2016.05.20160905202824.f7792890.rel	2.1.4	9/5/2016	Primarily of interest to Manufacturing.

Build Number	Release Version	Release Date	Notes
2016.05.20160811044721.6af0fa61.rel	2.1.3	8/11/2016	Offline update support key, M4 wipe support
2016.05.20160715165510.baed88a3.rel	2.1.2	7/15/2016	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	7/6/2016	
2016.05.20160621044600.092b23fc	2.1	6/21/2016	
2015.08.20160501161850.56631ccd	2.0.4	5/1/2016	Starting point for the 2.1 update. You must be at 2.0.4 before you can update to 2.1.
2015.08.20160315165529.599f2056	2.0.3	3/15/2016	Introduces AMP integration, CA mgmt., and split DNS
2015.08.20160217173404.ec264f73	2.0.2	2/18/2016	
2015.08.20160211192648.7e3d2e3a	2.0.1	2/12/2016	
2015.08.20160131061029.8b6bc1d6	2.0	2/11/2016	Force update to 2.0.1 from here
2014.10.20160115122111.1f09cb5f	1.4.6 **NOTE:** This is the starting point for the 2.0 upgrade.	1/27/2016	Starting point for the 2.0.4 update
2014.10.20151123133427.898f70c2	v1.4.5	11/25/2015	
2014.10.20151116154826.9af96403	v1.4.4		
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		
2014.10.20150709144003.b4d4171c	v1.2.1		

Build Number	Release Version	Release Date	Notes
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1+hotfix1		
2014.10.20150203155142.b06f7b4f	v1.1		
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0+hotfix2 **NOTE:** The 1.0+hotfix2 is a mandatory update that fixes the update system itself to be able to handle large files without breaking.		
2014.10.20141125162158.8afc5e2f	v1.0		

Updates Port

The Threat Grid Appliance downloads release updates over SSH, port 22.

- Starting with the appliance version 1.1, release updates can also be applied from the textual (curses) interface, not just from the web-based administrative interface (OpAdmin), which is described below.
- As of 1.3, systems using DHCP need to explicitly specify DNS. Previously, they did not. An upgrade of a system without a DNS server explicitly specified to 1.3 will fail.

Updates Troubleshooting

A "*database upgrade not successful*" message means that a new appliance is running an older version of PostgreSQL than it's supposed to.

This is a critical thing to fix prior to any upgrade to 2.0 as it means the automated database migration process didn't succeed.

Please see the Release Notes for v2.0.1 for more information.

Support - Contacting Threat Grid

If you need any assistance, there are several ways to request support from a Threat Grid engineer:

- **Email.** Send email to support@threatgrid.com with your query.
- **Open a Support Case.** You will need your Cisco.com ID (or to generate one) to open a support case. You will also need your service contract number, which was included on the order invoice. To open a Cisco Support Case Manager: https://mycase.cloudapps.cisco.com/case
- **Call.** Cisco contact information: https://cisco.com/cisco/web/siteassets/contacts/index.html

When requesting support from Threat Grid, please send the following information with your request:

- Appliance version: OpAdmin > Operations > Update Appliance)
- Full service status (service status from the shell)
- Network diagram or description (if applicable)
- Support Mode (Shell or Web interface)
- Support Request Details

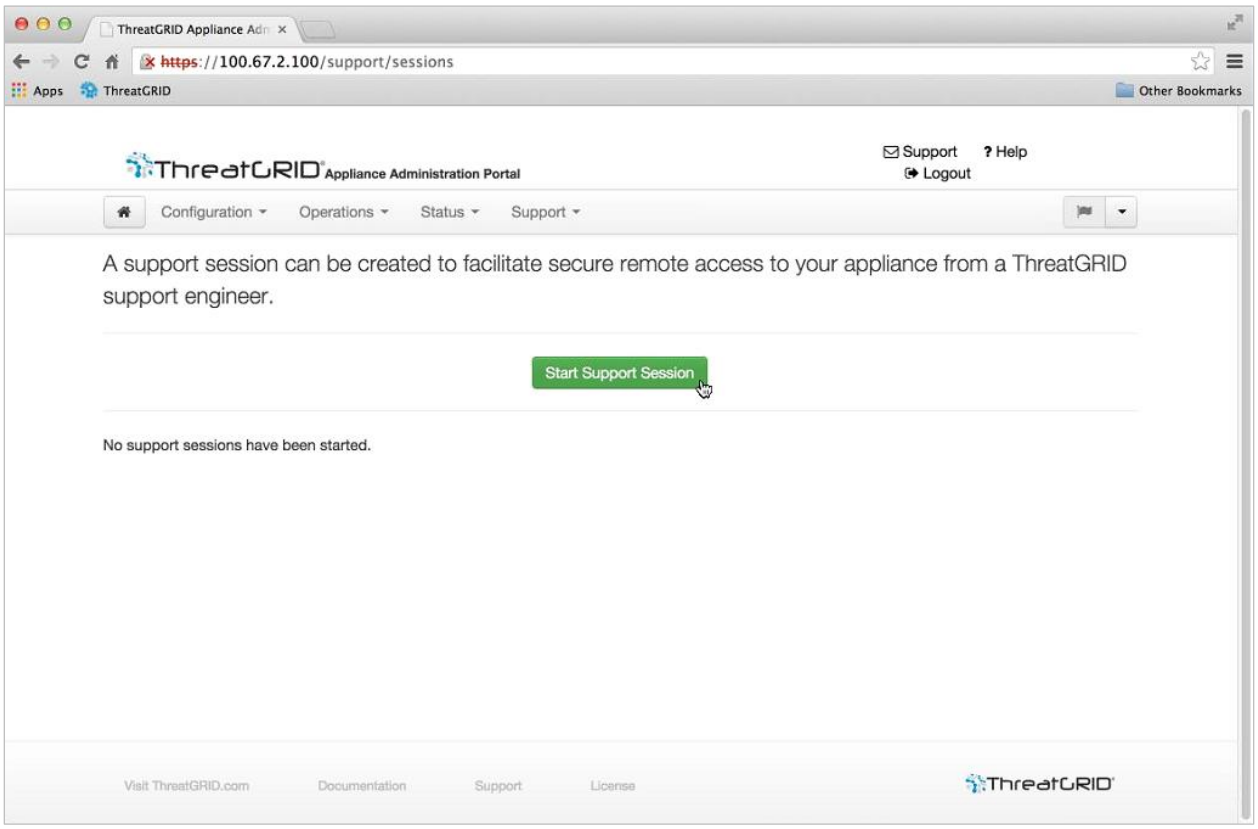
Support Mode

If you require support from a Threat Grid engineer, they may ask you to enable "support mode", which is a live support session that gives Threat Grid support engineers remote access to the appliance. Normal operations of the appliance will not be affected. This can be done via the **OpAdmin Portal Support** menu. (You can also enable SUPPORT MODE from the TGSH Dialog, from the legacy Face Portal UI, and when booting up into Recovery Mode.)

To start a live support session with Threat Grid tech support:

In OpAdmin, select **Support > Live Support Session** and click **Start Support Session**.

Figure 7 - OpAdmin Start a Live Support Session



Support Servers

Establishing a support session requires that the TG appliance reach the following servers:

- support-snapshots.threatgrid.com
- rash.threatgrid.com

Both servers should be allowed by the firewall during an active support session.

Support Snapshots

A support snapshot is basically a snapshot of the running system, which contains logs, ps output, etc., to help Support staff troubleshoot any issues.

1. From the **Support** menu, select **Support Snapshots**.
2. Take the snapshot.
3. Once you take the snapshot you can either download it yourself as .tar .gz, or you can press **Submit**, which will automatically upload the snapshot to the Threat Grid snapshot server.

CONFIGURATION MANAGEMENT

The initial Threat Grid Appliance configuration was performed during the appliance setup, as documented in the *Threat Grid Appliance Setup and Configuration Guide.*

Threat Grid Appliance configuration is managed in the **TGSH Dialog** and the **OpAdmin Portal** interfaces.

Threat Grid Organizations and User accounts are managed via the Threat Grid Portal UI (from the navigation bar upper-right **Welcome** menu).

The TGSH Dialog and OpAdmin configuration tasks are described in detail in the following sections.

Network Interface Configuration Management – TGSH Dialog

The TGSH Dialog interface is used primarily to manage the following:

- Network Interface Configuration
- View the OpAdmin Administrator's Password
- Install Updates
- Enable Support Mode
- Create and Submit Support Snapshots

Note: If you are using DHCP to obtain your IPs, then skip to the *Networking* section below: *Using DHCP*.

To Configure the TGSH Dialog Interface

1. Login to TGSH Dialog.

   Note: 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.

2. In the **TGSH Dialog** interface, select **CONFIG_NETWORK**.

   The Network Configuration console opens, displaying the current network settings.

3. Make your changes as needed.

   Note: You need to BACKSPACE over the old character before you can enter the new one.

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

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. If this is the case, then fix the errors and re-Validate.

   After validation, the Network Configuration Confirmation displays the values you've entered.

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

The console will become a blank grey box, and then it will list detailed information about the configuration changes that have been made.

7. Select **OK**.

   The Network Configuration Console refreshes again and displays the IP addresses you entered. Network configuration is now complete.

Reconnecting to the TGSH Dialog

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

One way to reconnect to the TGSH Dialog is to SSH into the Admin IP address as the user **'threatgrid'**. The required password will either be 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.

Password Updates

Lost password? See *Lost Password Recovery* in the *Getting Started* section, above.

Setting Up Networking in Recovery Mode

1. Initiate a reboot, and wait for the boot menu, which is only present for a short period of time- so be ready (see Figure 3 - Boot Menu - Support Mode, above).
2. Select Recovery Mode. Wait a couple of minutes for the system to start up.
3. Once the system is up, press Enter several times to get a clean command prompt.
4. Enter **netctl clean** and answer the questions as follows:

   Configuration type: static

   IP Address: <Clean IP Address>/<Netmask>

   Gateway Address: <Clean network gateway>

   Routes: <leave blank>

   Answer y to the final question.
5. Enter **Exit** to apply the configuration.

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

Main Configuration Management – OpAdmin Portal

The initial setup and configuration wizard is described in the *Threat Grid Appliance Setup and Configuration Guide*. New appliances may require the administrator to completed 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 TGA's **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
- 3rd 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.

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 have 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.

Reminder: OpAdmin uses HTTPS. Pointing a browser at the Admin IP is not sufficient; you must point to:

https://adminIP/

OR

https://adminHostname/

SSH Keys

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

It does NOT provide root access or a command shell. Multiple keys may be added.

Configuration > SSH

Syslog

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

1. In OpAdmin, under **Configuration** > **Syslog**
2. Enter the server DNS in the field provided, and then select a protocol from the dropdown list; TCP is the default, the other is UDP.
3. Check the **Verification** box to perform a DNS lookup when you click **Save**. 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 box, the appliance will accept any name, whether valid in DNS or not.
4. Click **Save**.

To Edit or Delete: If you need to update the Syslog DNS, simply edit or delete it and click **Save**.

Configuring LDAP Authentication for OpAdmin and TGSH Dialog

The 2.1.6 release includes LDAP authentication and authorization for OpAdmin and TGSH Dialog login was added to the Threat Grid Appliance. Previously, the OpAdmin and TGSH Dialog interfaces had just one password; if you had more than one appliance administrator they had to share the password between them. Not only is it a bad idea, but avoiding that scenario is a requirement for many of our customers. We have implemented LDAP Authentication as a remedy.

It is now possible to authenticate multiple appliance administrators with different credentials that are managed on the domain controller or the LDAP server. LDAP configuration is not trivial, and we recommend taking some care with this step, with a thorough understanding of the details prior to setting it up.

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.

Be aware of the following:

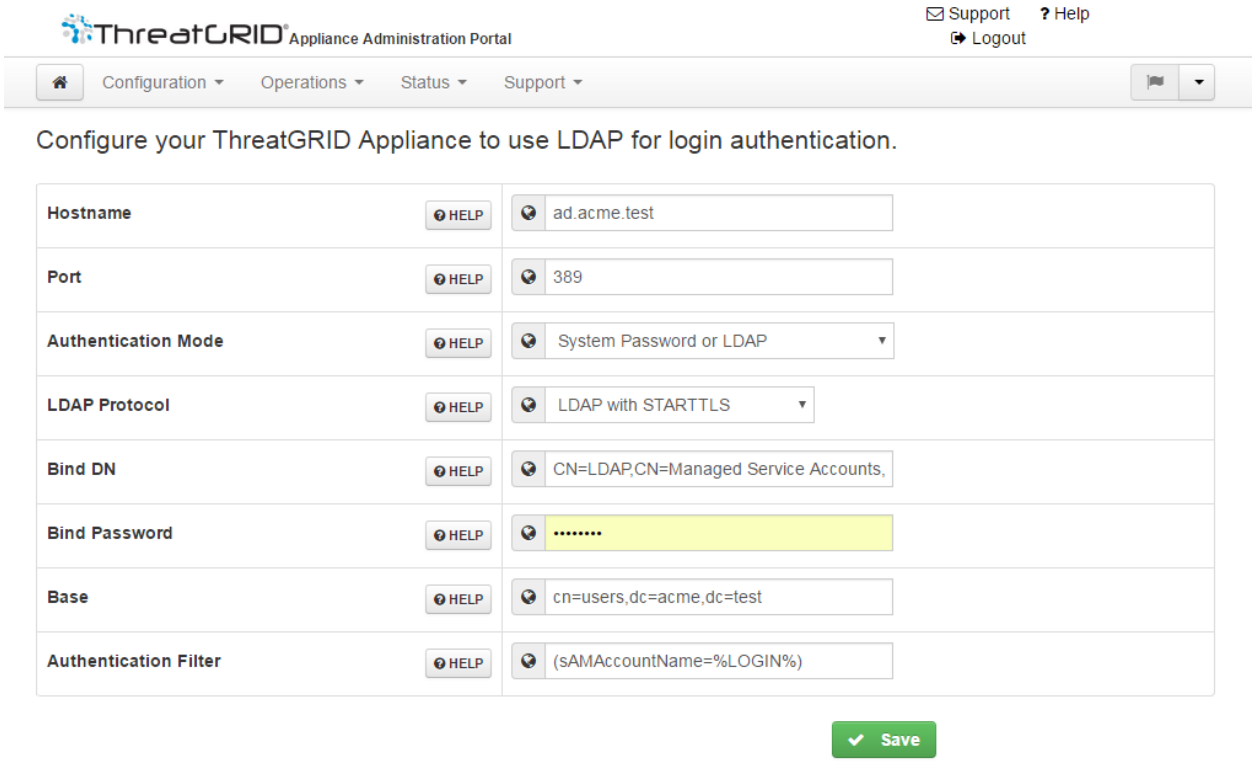
- The “dual” authentication mode (**System Password or LDAP**) is required in order to avoid accidentally locking yourself out of the appliance when setting up LDAP. Selecting **LDAP Only** is not allowed initially; you must go through dual mode to make sure it works first. You will need to log out of 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.

To Configure LDAP Authentication

1. In OpAdmin, select **Configuration** > **LDAP**. The LDAP configuration page opens:

Figure 8 - LDAP Authentication Configuration



2. Complete the fields.

   Click the **?Help** buttons next to each field for a detailed description and more information.

   Again, note that the first time you configure LDAP authentication, you must select System Password or LDAP, log out of OpAdmin, and then log back in using LDAP credentials in order to change the setting in order to implement **LDAP Only**.

3. Click **Save**.

Now, when users login to OpAdmin or TGSH Dialog they will see the following:

Figure 9 - LDAP Only

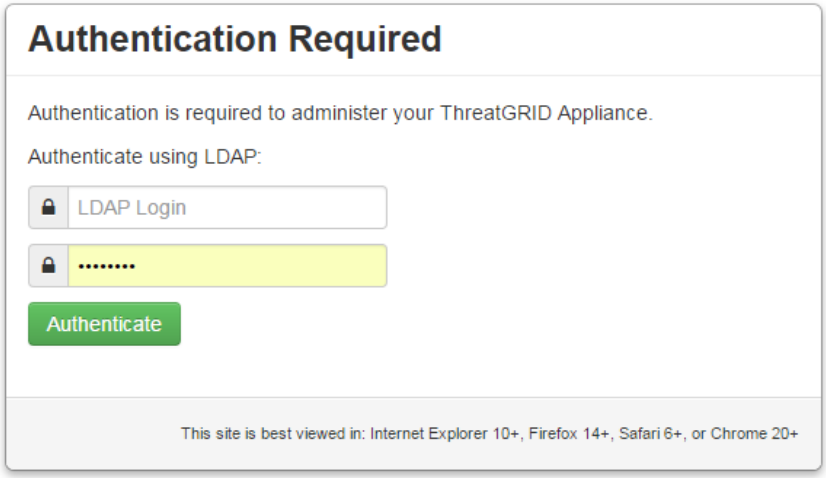
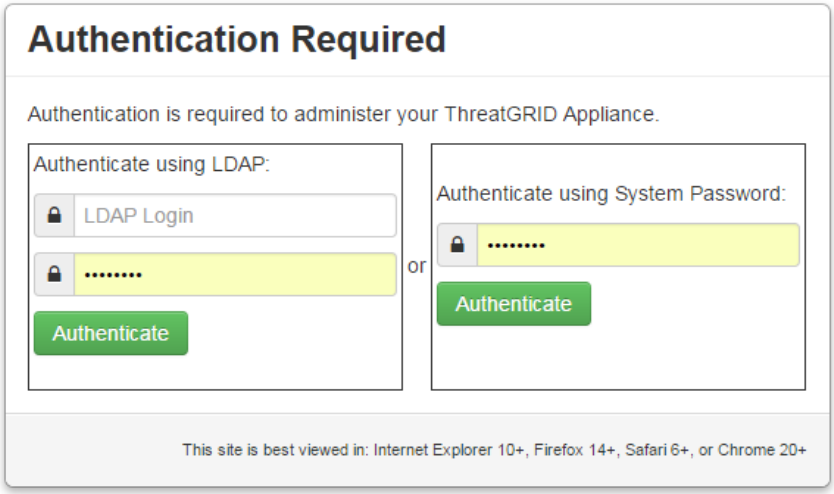


Figure 10 - System Password or LDAP



Configuring 3rd Party Detection and Enrichment Services

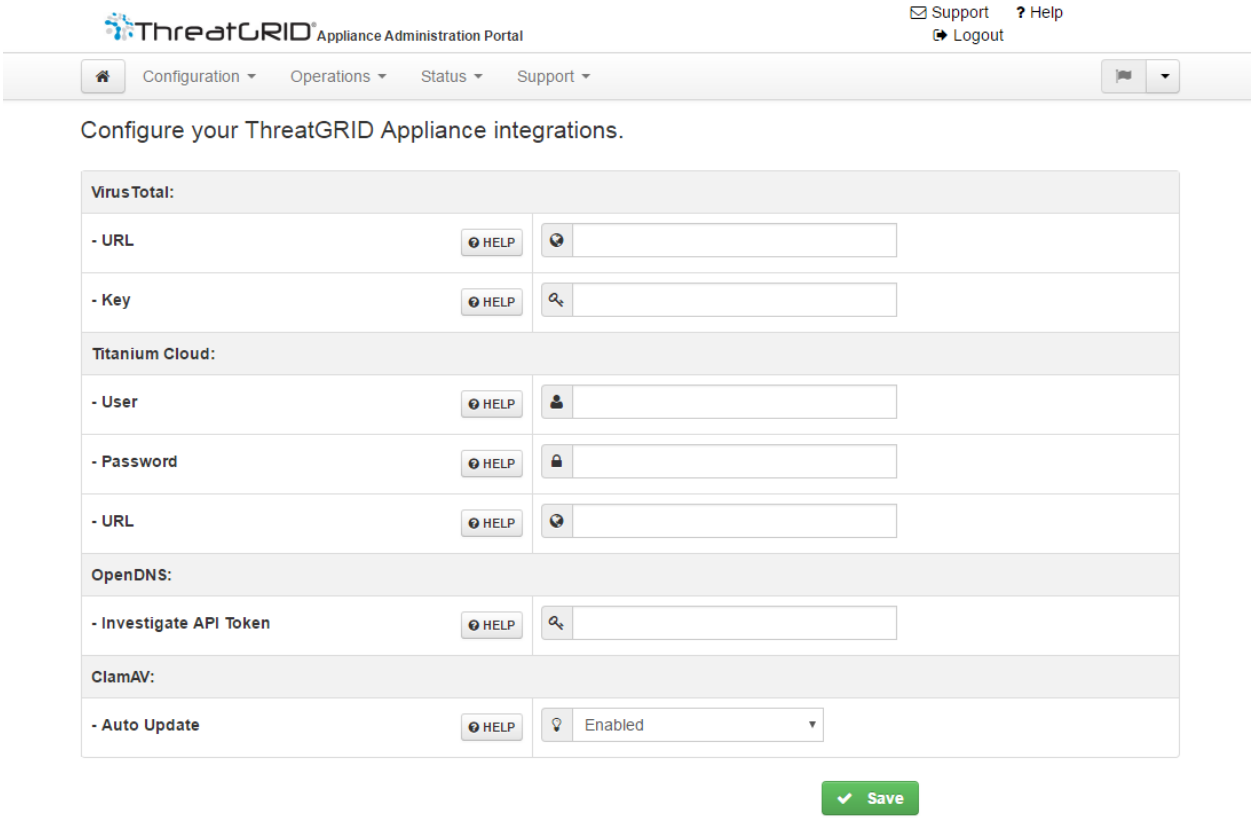
With version 2.2, integrations with several third party detection and enrichment services, including OpenDNS, TitaniumCloud, and VirusTotal, can be configured on the appliance using the new integration configuration page.

In **OpAdmin**, select **Configuration > Integrations** to open the integrations configuration page:

Enter the authentication or other values required, and click **Save**.

OpenDNS: Note that 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.

Figure 11 – Integrations Configuration



ClamAV Signatures Automatically Updated Daily by Default

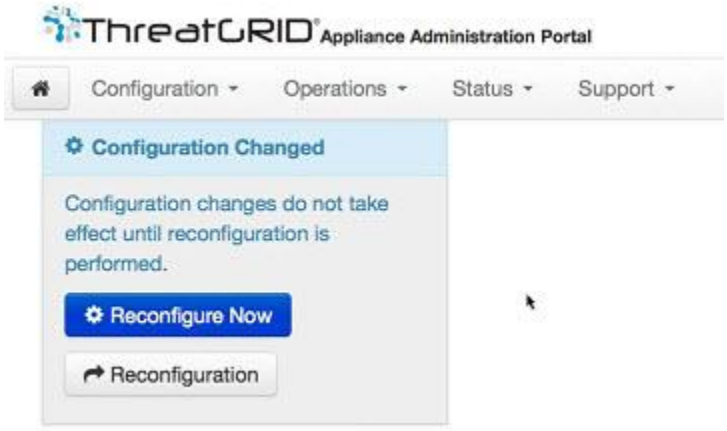
With the 2.2 update, ClamAV signatures can be automatically updated on a daily basis. This is enabled by default, and can be disabled from the new Integrations Configuration page (above).

Reconfiguration

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

1. Click **Configuration Changed**. The **Reconfiguration** dialog opens:

Figure 12 - Reconfigure Now



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

Using DHCP

Most 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* below.

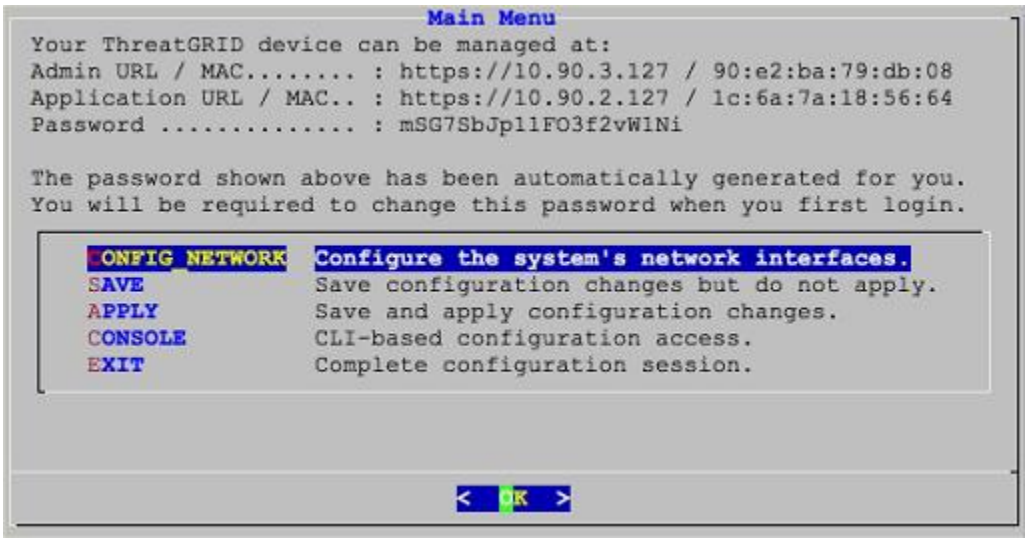
TGSH Dialog displays the information you will need to in order to access and configure the OpAdmin Portal interface.

The IP addresses for DHCP may not be displayed immediately after your Appliance boots. Please be patient!

Explicit DNS for DHCP

As of v1.3, systems using DHCP need to explicitly specify DNS. Previously, they did not. An upgrade of a system without a DNS server explicitly specified to 1.3 will fail.

Figure 13 - 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.

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** is 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 on using 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, follow the steps below:

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 have 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.

1. In the left column, click on **Network**. (Although **Configuration > Network** is checked in the License window, the DHCP network configuration has NOT yet been done.)

   The *Network Configuration* page opens.

Clean

2. **IP Assignment.** Choose **Static** from the dropdown.
3. **IP Address.** Enter a static IP Address for the **Clean** network interface.
4. Complete the **Subnet** mask and **Gateway** as appropriate.
5. Check the box next to **Validate DNS Name**, to verify that the DNS resolves to the IP Address you entered.

Dirty

6. **IP Assignment.** Choose Static from the dropdown.
7. **IP Address.** Enter a static IP Address for the **Dirty** network interface.
8. Complete the **Subnet mask** and **Gateway** as appropriate.

Administration

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

DNS

9. Complete the **Primary** and **Secondary DNS** server fields.

Save Your Settings

10. When done, click **Next (Applies Configuration)** to save your network configuration settings.

SMTP/Email

Email configuration is managed from the *Email* page.

Time

NTP servers are managed on the *Date and Time* page.

Apply the DHCP Configuration

To apply your DHCP configuration settings, click **Configuration Changed**, then **Reconfigure Now**.

SSL CERTIFICATES AND THREAT GRID APPLIANCES

All network traffic passing to and from the Threat Grid Appliance is encrypted using SSL. A full description of how to administer SSL certificates is beyond the scope of this Guide. However, the following information is provided to assist you through the steps for setting up SSL certificates to support Threat Grid Appliance connections with ESA/WSA appliances, AMP for Endpoints Private Cloud, and other integrations.

Interfaces That Use SSL

There are two interfaces on the Threat Grid Appliance that use SSL:

- **Clean** interface for the Threat Grid Portal UI and API, as well as integrations (ESA/WSA appliances, AMP for Endpoints Private Cloud Disposition Update Service, etc.)
- **Admin** interface for the **OpAdmin Portal**.

SSL/TLS Versions Supported

- TLSv1.0
- TLSv1.1
- TLSv1.2

Customer-Provided CA Certificates Are Supported

With the 2.0.3 release we now support customer-provided CA certificates, allowing customers to import their own trusted certificates or CA certificates.

SSL Certificates - Self-Signed Default

The Threat Grid Appliance is shipped with a set of self-signed SSL certificates and keys already installed. One set is for the **Clean** interface and the other is for the **Admin** interface. The appliance SSL certificates can be replaced by an administrator.

The default Threat Grid Appliance SSL certificate hostname (Common Name) is "*pandem*", which is valid for 10 years. If a different hostname was assigned to the Threat Grid Appliance during configuration, then the hostname and the CN in the certificate will no longer match. The hostname in the certificate must also match the hostname expected by a connecting ESA or WSA appliance, or other integrating Cisco device or service, as many client applications require SSL certificates where the CN used in the certificate matches the hostname of the appliance.

Configuring SSL Certificates for Inbound Connections

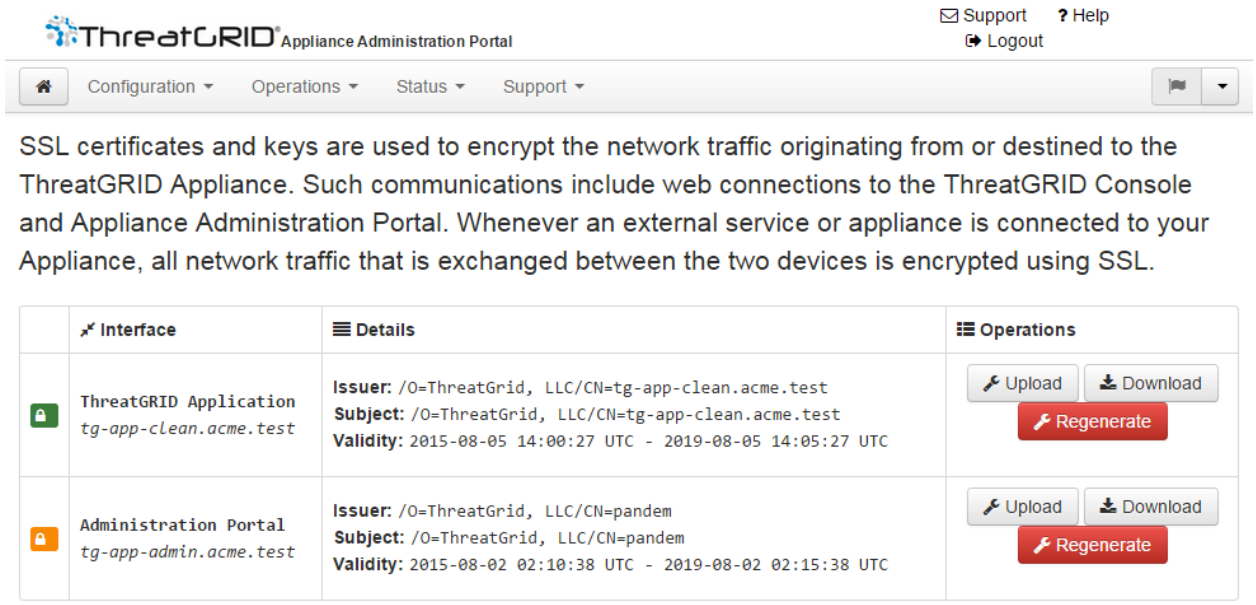
Other Cisco products, such as such as ESA and WSA appliances and AMP for Endpoints Private Clouds, can integrate with a Threat Grid Appliance and submit samples to it. These integrations are *Inbound* connections from the perspective of the Threat Grid Appliance. The integrating appliance or other device must be able to trust the Threat Grid Appliance's SSL certificate, so you will need to export it from the TGA (first making sure that it

uses the correct hostname in the CN field and regenerating or replacing it if necessary), and then import it into the integrating appliance or service.

The certificates on the Threat Grid Appliance that are used for inbound SSL connections are configured in the **SSL Certificate Configuration** page. The SSL certificates for the **Clean** and **Admin** interfaces can be configured independently.

Select **OpAdmin > Configuration > SSL**. The SSL Certificate configuration page opens:

Figure 14 - SSL Certificate Configuration Page



There are two SSL certificates in the illustration above: "ThreatGRID Application" is the **Clean** interface, and "Administration Portal" is the **Admin** interface.

CN Validation

In the SSL Certificate Configuration page, a colored padlock icon indicates the status of the SSL certificates on the TG Appliance. The hostname must match the CN (“Common Name”) used in the SSL certificate. If they do not match, you will need to replace the certificate with one that uses the current hostname. See Replacing an SSL Certificate below.

- The green padlock icon indicates that the Clean interface hostname matches the CN ("Common Name") used in the SSL certificate.
- The yellow padlock icon is a warning that the Admin interface hostname does NOT match the CN in that SSL certificate. You will need to replace the certificate with one that uses the current hostname.

Replacing an SSL Certificate

SSL certificates usually need to be replaced at some time, for a variety of reasons. For example, they expire, or the hostname changes. An SSL certificate may also need to be added or replaced in order to support integrations between the Threat Grid Appliance and other Cisco devices and services.

ESA/WSA appliances and other CSA Cisco integrating devices may require an SSL certificate in which the Common Name matches the Threat Grid Appliance hostname. In this case, you will need to replace the default SSL certificate and generate a new one using the same hostname from which you'll be accessing the Threat Grid Appliance.

In the case where you are integrating a Threat Grid Appliance with a AMP for Endpoints Private Cloud to use its Disposition Update Service, you will need to install the AMP for Endpoints Private Cloud SSL Certificate so the Threat Grid Appliance can trust the connection.

There are several ways to replace an SSL certificate on a Threat Grid Appliance:

- Regenerating a new SSL Certificate, which will use the current hostname for the CN.
- Downloading an SSL Certificate
- Uploading a new SSL Certificate. This can be a commercial or enterprise SSL, or one you make yourself using OpenSSL.
- Generating Your Own SSL Certificate – an Example Using OpenSSL

These are described in the following sections.

Regenerating an SSL Certificate

This replaces the need in pre-v1.3 Threat Grid Appliances to generate a new SSL certificate manually using OpenSSL or other SSL tool. However, that method is still valid, as described in the section Generating Your Own SSL Certificate – an Example Using OpenSSL, below.

NOTE: The Threat Grid Appliance should be upgraded to 1.4.2 or higher before performing this task.

In the **OpAdmin SSL Certificate Configuration** page, click **Regenerate**. A new, self-signed SSL certificate is generated on the Threat Grid Appliance that uses the current hostname of the appliance in the CN field of the certificate. The CN validation padlock icon is green. The regenerated certificate (.cert file) can be downloaded as described in the next section, and installed on the integrating appliance.

Downloading an SSL Certificate

The Threat Grid SSL certificate, but not the key, can be downloaded, and installed on your integrating device so it can trust connections from the TG Appliance. You will only need the .cert file for this step.

1. In the OpAdmin SSL Certificate Configuration page, click **Download** next to the certificate you wish to obtain**.** The SSL Certificate is downloaded.
2. Next, install the downloaded SSL certificate on the ESA/WSA appliance, FireAMP Public Cloud, or other integrating Cisco products just as you would install any other SSL certificate.

Uploading an SSL Certificate

If you already have a commercial or corporate SSL certificate in place within your organization, you can use that to generate a new SSL certificate for the TGA, and use the CA cert on the ESA/WSA or other integrating device.

Generating Your Own SSL Certificate – an Example Using OpenSSL

Another alternative is to generate your own SSL certificate manually, such as when there is no SSL certificate infrastructure already in place on your premises, and you are unable to obtain one by other means. This can then be uploaded as described above.

This example illustrates the command for generating a new self-signed SSL certificate for the "Acme Company". The example uses OpenSSL, which is a standard open source SSL tool for creating and managing OpenSSL certificates, keys, and other files.

NOTE: OpenSSL is not a Cisco product, and Cisco provides no technical support for it. Search the Web for additional information on using OpenSSL. Cisco offers an SSL library, *Cisco SSL*, for generating SSL certificates.

```
openssl req -x509 -days 3650 -newkey rsa:4096 -keyout
tgapp.key -nodes -out tgapp.cert -subj "/C=US/ST=New
York/L=Brooklyn/O=Acme Co/CN=tgapp.acmeco.com"
```

- **openssl**: OpenSSL.
- **req**: Specifies that we want to use X.509 certificate signing request (CSR) management. "X.509" is a public key infrastructure standard that SSL and TLS use for key and certificate management. We want to create a new X.509 cert, so we are using this subcommand.
- **-x509**: This modifies the previous subcommand by telling the utility that we want to make a self-signed certificate instead of generating a certificate signing request, as would normally happen.
- **-days 3650**: This option sets the length of time for which the certificate will be considered valid. Here we set it for 10 years.
- **-newkey rsa:4096**: This specifies that we want to generate a new certificate and a new key at the same time. We did not create the key that is required to sign the certificate in a previous step, so we need to create it along with the certificate. The rsa:4096 portion tells it to make an RSA key that is 4096 bits long.
- **-keyout**: This line tells OpenSSL where to place the generated private key file that we are creating.
- **-nodes**: This tells OpenSSL to skip the option to secure our certificate with a passphrase. The appliance needs to be able to read the file without user intervention, when the server starts up. A passphrase would prevent this from happening because we would have to enter it after every restart.
- **-out**: This tells OpenSSL where to place the certificate that we are creating.
- **-subj:** Example:

  C=US: Country.

  ST=New York: State.

  L=Brooklyn: Location.

  O=Acme Co: Owner's name.

CN=tgapp.acmeco.com: Please enter the Threat Grid Appliance FQDN ("Fully Qualified Domain Name"). This includes the HOSTNAME of the Threat Grid Appliance ("tgapp" in our example), together with the associated domain name ("acmeco.com") appended to the end.

IMPORTANT: You will need to change at the very least the Common Name to match the FQDN of the Threat Grid Appliance Clean interface.

Once the new SSL certificate is generated, use the SSL page **Upload** button to upload it to the Threat Grid Appliance, and also upload it to the ESA/WSA appliance (.cert only).

Configuring SSL Certificates for Outbound Connections

The Threat Grid Appliance release 2.0.3 includes features to support integrations with AMP for Endpoints Private Cloud for the Disposition Update Service.

Configure DNS

By default, DNS uses the Dirty interface. If the hostname of an integrating appliance or service such as a AMP for Endpoints Private Cloud cannot be resolved over the Dirty interface, because the Clean interface is used for the integration, then a separate DNS server that uses the Clean interface can be configured in OpAdmin.

In **OpAdmin**, select **Configuration > Network**, and complete the DNS fields for the Dirty and Clean networks, and click **Save**.

CA Certificate Management

One of the features added with release 2.0.3 is a new page for the CA Certificate Management truststore for the *Outbound* SSL connections, so the TGA can trust the AMP for Endpoints Private Cloud to notify it about analyzed samples that are considered to be malicious.

In **OpAdmin**, select **Configuration > CA Certificates**. Select:

1. **Import from Host.** Retrieve the certificate from the server. The Retrieve certificates from server dialog opens.
2. Enter the **Host** and **Port** for the AMP for Endpoints Private Cloud and click **Retrieve**. The certificate is retrieved.

OR

Import from Clipboard. Paste the PEM from the clipboard, and click **Add Certificate**.

3. Click **Import**.

Disposition Update Service Management

This task is performed from within the Threat Grid Portal UI.

1. From the **My Account** dropdown, select **Manage FireAMP Integration**. The Disposition Update Service page opens.
2. Enter the **AMP for Endpoints Private Cloud URL**, the **admin user name** and **password** provided by the FireAMP configuration portal, and click **Config**.

For more information on AMP for Endpoints Private Cloud appliance integrations, see Connecting a Threat Grid Appliance to a Cisco , below.

Connecting ESA/WSA Appliances to a Threat Grid Appliance

Other Cisco products such as ESA/WSA and other appliances, devices, services, etc. may integrate with Threat Grid Appliances via connections encrypted with SSL, in order to submit possible malware samples to it for analysis.

"CSA Integrations": Integrations between ESA/WSA appliances and Threat Grid appliances are enabled by the Cisco Sandbox API ("CSA API"), and are often referred to as "CSA Integrations".

An integrating ESA/WSA appliance must be registered with the Threat Grid Appliance before it can submit samples for analysis. Before the integrating ESA/WSA appliance can be registered with the Threat Grid Appliance, the ESA/WSA administrator must first set up the SSL certificate connection as appropriate for their appliance and their network environment.

This section describes the steps necessary for setting up integrating ESA/WSA appliances and other Cisco products to communicate with Threat Grid appliances.

Links to ESA/WSA Documentation

See the instructions for *"Enabling and Configuring File Reputation and Analysis Services"* in the online help or user guide for your ESA/WSA. (The Threat Grid Appliance is often referred to as an "analysis service", or "private cloud file analysis server" in these guides.)

- The ESA user guides are located here: http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
- The WSA user guides are located here: http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html

Integration Process Overview

Before you begin: This section provides an overview of the steps in setting up a connection between an ESA/WSA appliance or other CSA integration (inbound) with a Threat Grid Appliance.

A table containing more detailed descriptions of each step follows this section.

Threat Grid Appliance SSL Certificate SAN or CN Must Match its Current Hostname and ESA/WSA Expectations:

The Threat Grid appliance SSL certificate SAN ("Subject Alternative Name" – if defined), or the CN ("Common Name") needs to match the hostname, and also the ESA/WSA expectations: for a successful connection with an integrating ESA/WSA appliance, this must be the same hostname by which the integrating ESA/WSA appliance identifies the Threat Grid Appliance.

Depending on your requirements, you may need to regenerate the self-signed SSL certificate on the Threat Grid Appliance so it uses the current hostname in the SAN/CN field, then download it to your working environment and upload and install it onto the integrating ESA/WSA appliance.

Alternatively, you may need to replace the current TGA SSL certificate by uploading an enterprise or commercial SSL certificate (or a certificate generated manually).

For detailed instructions, see the section above: Configuring SSL Certificates for Inbound Connections.

Verify Connectivity:

Once the SSL certificate setup is complete, the next step is to verify that the ESA/WSA appliances can communicate with the Threat Grid Appliance.

Cisco ESA/WSA appliances must be able to connect to the **Clean** interface of the Threat Grid Appliance over your network.

Follow the instructions in the appropriate guide for your product to verify that the TGA and ESA/WSA Appliances can communicate with each other. (See links above.)

Complete the ESA/WSA File Analysis Configuration:

Enable the File Analysis security service, and configure the advanced settings.

Register the Cisco ESA/WSA/other device with the Threat Grid Appliance:

An ESA/WSA appliance that is configured according to the documentation for those products registers itself automatically with the Threat Grid appliance.

Upon registration of the connecting device, a new Threat Grid user is created automatically with the Device ID as the login ID, and a new organization is created with a name based on the same ID. An administrator, as described in the next section, must activate the new Device user account.

Activate the New ESA/WSA Account on the Threat Grid Appliance:

When the ESA/WSA appliance or other integration connects and registers itself with the Threat Grid Appliance, a new Threat Grid user account is created automatically. The initial status of this user account is "de-activated". Just like any other Threat Grid user, a Threat Grid Appliance administrator must manually activate the device user account before it can be used for submitting malware samples for analysis.

ESA/WSA Integration Process Steps

This connection is *incoming* from the perspective of the Threat Grid Appliance.

This integration uses the CSA API.

Please refer to the ESA and WSA User Guides for more detailed information on the tasks that must be performed on that side.

STEPS	Threat Grid Appliance (“TGA”)	ESA/WSA/Other CSA API Integrations
1	Set up and configure the Threat Grid Appliance (“TGA”) as normal (i.e., no integration yet). Check for updates and install if found.	
2		Set up and configure the ESA/WSA appliance as normal (i.e., no integration yet).

STEPS	Threat Grid Appliance ("TGA")	ESA/WSA/Other CSA API Integrations
3	**The TGA SSL Certificate SAN or CN Must Match its Current Hostname and ESA/WSA Expectations** If you will deploy a self-signed SSL certificate: Generate a new SSL Certificate (on the "Threat Grid Application" – the Clean interface), to replace the default if needed, and download it to install in the ESA/WSA appliance device. (TGA SSL Certificates are documented in the section above, SSL CERTIFICATES AND THREAT GRID APPLIANCES.) Be sure to generate a certificate that has the hostname of your Threat Grid appliance as the SAN or CN. The default certificate from the Threat Grid appliance does NOT work. Use the hostname, not the IP address.	
4		**Verify Connectivity** Cisco ESA/WSA appliances must be able to connect to the **Clean** interface of the Threat Grid Appliance over your network.

STEPS	Threat Grid Appliance ("TGA")	ESA/WSA/Other CSA API Integrations
5		**Configure the ESA/WSA appliance for the TG Appliance Integration:** Please refer to the ESA/WSA guides for complete instructions. The following steps are specific to the ESA, as this is currently the most common type of integration 1. Select **Security Services** > **File Reputation and Analysis**. 2. Click **Enable**. 3. Click **Edit Global Settings**. File Analysis is enabled by default. If you do not uncheck **Enable File Analysis**, the File Analysis feature key will be activated after the next commit. 4. In the **File Analysis** section, select the file types to send to the Cloud for analysis. 5. Configure the **Advanced Settings for File Analysis** as needed, according to the ESA or WSA guides: **File Analysis Server URL:** Select **Private Cloud**. **Server:** **URL** of the on-premises Cisco Threat Grid Appliance. Use the hostname, not the IP address, for this value and for the certificate. **SSL Certificate:** Upload a self-signed certificate that you have generated from your on-premises Cisco Threat Grid Appliance. The most recently uploaded self-signed certificate is used. It is not possible to access a certificate uploaded prior to the most recent certificate; if needed, upload the desired certificate again. 6. Submit and commit your changes. Note the **File Analysis Client ID** that appears at the bottom of the page. This identifies the "user" that you will need to activate in step 7.

STEPS	Threat Grid Appliance ("TGA")	ESA/WSA/Other CSA API Integrations
		Registration with the Threat Grid Appliance is Automatic Registration of your Email Security appliance or Web Security appliance with your Threat Grid appliance occurs automatically when you submit the configuration for File Analysis. However, you must activate the registration as described in step 7, below.
7	**Activate the New Device User Account on the Threat Grid Appliance** 1. Log into the Threat Grid Portal UI as Admin. 2. From the navigation bar **Welcome** menu, select **Manage Users**. The **Threat Grid Users** page opens. 3. Open the **User Details** page for the device user account (you may need to use Search to find it). The user status is currently "de-activated". 4. Click Re-**Activate User**. A dialog opens asking you to confirm. 5. Click **Re-Activate** in the dialog to confirm.	

The ESA/WSA or other integrating appliance or device can now initiate connections with the Threat Grid Appliance.

Connecting a Threat Grid Appliance to a Cisco AMP for Endpoints Private Cloud

The Threat Grid Appliance Disposition Update Service and AMP for Endpoints Private Cloud integration setup tasks must be performed on the devices in the following order, particularly if you are setting up new appliances. If you are integrating appliances that are already set up and configured, the order is not as critical.

This connection is outgoing from the perspective of the Threat Grid Appliance. This integration does not use the CSA API ("Cisco Sandbox API").

Please refer to the AMP for Endpoints Private Cloud documentation for more detailed information on the tasks which must be performed on that side.

STEPS	Threat Grid Appliance ("TGA")	AMP for Endpoints Private Cloud
1	Set up and configure the Threat Grid Appliance ("TGA") as normal (i.e., no integration yet). Check for updates and install if found.	
2		Set up and configure the AMP for Endpoints Private Cloud as normal (i.e., no integration yet).
3		**Configure the AMP for Endpoints Private Cloud for the TGA Integration:** Select **Integrations > Threat Grid** and go to the **Connection to Threat Grid** section. To complete the connection with the Threat Grid Appliance, you have to trust it. You need its DNS hostname, SSL certificate, and API key. Go to step 3.1 in the TGA column to find this information.

STEPS	Threat Grid Appliance ("TGA")	AMP for Endpoints Private Cloud
3.1	**SSL Certificate: –** In the Threat Grid Appliance OpAdmin interface, select **Configuration > SSL** Regenerate a new SSL Certificate (on the "Threat Grid Application" – the Clean interface), to replace the default if needed, and download it to install in the AMP for Endpoints Private Cloud device. (TGA SSL Certificates are documented in SSL CERTIFICATES AND THREAT GRID APPLIANCES.) **Hostname** Select **Configuration > Hostname** **API Key**: The API Key may be found in the Threat Grid Face Portal UI, in the **User Details** page for the account that is going to be used for integrations: 1. Go to the **Threat Grid Portal UI**. 2. From the upper-right Welcome menu (located in the upper-right corner of the navigation bar), select **Manage Users**. 3. Navigate (use Search if necessary) to the **User Details** page for the integration's user account, and copy the **API Key**. Note that this does not need to be the "admin" user, but can be another user that was specifically created for this purpose on the Threat Grid Appliance.	

STEPS	Threat Grid Appliance ("TGA")	AMP for Endpoints Private Cloud
3.2		Complete the **Connection to Threat Grid** fields: 1. Enter the TGA Hostname 2. Enter the Threat Grid API Key for the account that is to be used for integrations. 3. Choose the TGA SSL Certificate file. 4. Click Save Configuration. 5. Click Test Connection. 6. Once the connection test passes, you will need to run the Reconfiguration on the AMP for Endpoints Private Cloud to apply the changes. Technically, this will allow AMP to talk to the Threat Grid Appliance, and you can now submit samples to TG at this point. However, you must complete the remaining steps to set up the Disposition Update Service, in order to communicate disposition results to the TGA. (For more information, please refer to the user documentation for the AMP for Endpoints Private Cloud.)
4	**Set up the Disposition Update Service** The following steps describe how to set up the Disposition Update Service	

STEPS	Threat Grid Appliance ("TGA")	AMP for Endpoints Private Cloud
4.1	**Configure DNS (if needed):** The Clean interface is used for the FireAMP integration. But by default, DNS uses the Dirty interface. If the AMP for Endpoints Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in OpAdmin. In OpAdmin, select **Configuration > Network**, and complete the fields for DNS on the **Dirty** and **Clean** networks, and click **Save**.	
4.2	**CA Certificate Management:** The next step is to download or copy/paste the AMP for Endpoints Private Cloud SSL certificate to the Threat Grid Appliance so it can trust the integrating device: 1. In OpAdmin, select **Configuration > CA Certificates**. You can select an SSL certificate to import from the AMP for Endpoints Private Cloud Host, or import from the clipboard. 2. Select the certificate to import and click **Import from Host**. The **Retrieve certificates from server** dialog opens. Enter the **Host** and **Port** for the FireAMP Appliance Disposition Service, and click **Retrieve**. 3. The certificate is retrieved. 4. Click **Import**. (OR click **Import from Clipboard.** Paste the PEM from the clipboard, and click **Add Certificate**.)	

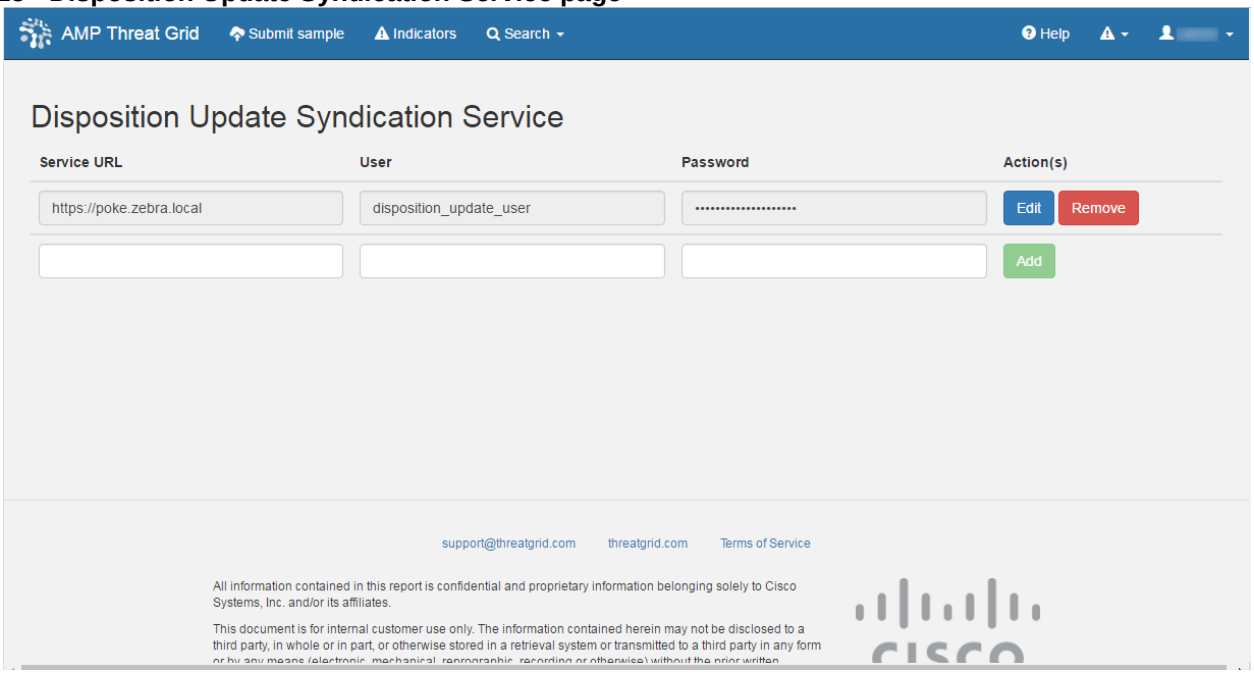
STEPS	Threat Grid Appliance ("TGA")	AMP for Endpoints Private Cloud
4.3	**FireAMP Integration Management:** In the Threat Grid Face Portal UI, from the upper-right menu select **Manage FireAMP Integration**. The Disposition Update Syndication Service window opens (see below). Enter the AMP Disposition Update Service URL (you can find this on the FireAMP appliance: select **Integrations > Threat Grid > AMP for Endpoints Private Cloud Details**). Enter your **admin user name** and **password**, and click **Config**.	

Managing the Disposition Update Syndication Service

With the 2.2 release, support was added for configuring more than one URL for Disposition Update notifications (sometimes referred to as "multi-POKE").

URLs can be Added, Edited, and Deleted from the new Disposition Update Syndication Service page:

Figure 15 - Disposition Update Syndication Service page



MANAGING THREAT GRID ORGANIZATIONS AND USERS

Threat Grid is installed on the appliance with a default organization and Admin user. Once the appliance is set up and the network configuration is completed, you may create additional organization and user accounts, so people can login and begin submitting malware samples for analysis.

Adding organizations, users, and administrators may require planning and coordination among multiple users and teams, depending on your organization.

Creating a New Organization

Users are always affiliated with an organization; before you can add users, you must first create the Organization to add them to.

IMPORTANT: You cannot delete an organization from this interface once it has been created, so plan this task carefully.

1. Log into the Threat Grid portal as Admin.
2. Click the **Welcome** dropdown link located in the upper-left corner, and select **Manage Orgs**. The Organizations page opens, listing all of the Organizations on the appliance.
3. Click the **Add Organization** button, located in the upper-right corner of the screen. The Properties dialog opens.
4. All fields are required.

   Name. Add a name for the organization (there is currently no size limit to the name).

   Industry. Select the type of business from the Industry dropdown. If none of the industries on the list are applicable, then leave it set to Unknown, and contact Threat Grid support (support@threatgrid.com) to request that an option be added.

   Complete the other Options.

   Rate Limit:

   The API rate limit is global for the appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions. The rate limit in the license applies to the Organization.

   Set the default user submission rate limit. You can also set sample submission rates on individual users - as documented in Using Threat Grid, the Threat Grid Portal online Help (From the navigation bar select Help > Using Threat Grid Online Help).

   Rate limits are based on a 24-hour window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error, plus a message about how long to wait before retrying.

   The Priority field is going away; for now just enter “50”.
5. Click **Create**. The new organization is created and is now visible in the list of Organizations.

Managing Users

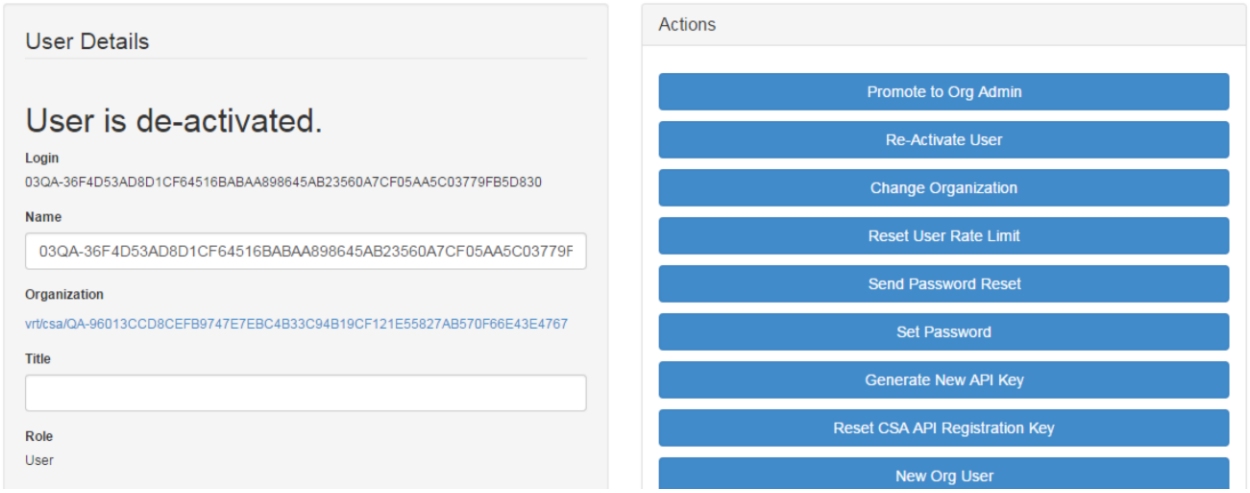
For instructions and documentation on managing user accounts - including accounts for integrating Cisco ESA/WSA appliances and other devices - see the Threat Grid Portal UI online help. From the navigation bar select **Help > Using Threat Grid Online Help > Managing Users**.

Activating a New Device User Account on the Threat Grid Appliance

When the ESA/WSA appliance or other CSA ("Cisco Sandbox API") integration connects and registers itself with a Threat Grid Appliance, a new Threat Grid user account is created automatically. The initial status of this user account is "de-activated". Just like any other Threat Grid user, the device user account must be manually activated by a Threat Grid Appliance administrator before it can be used for submitting malware samples for analysis.

1. Log into the Threat Grid Portal UI as Admin.
1. From the navigation bar **Welcome** menu, select **Manage Users**. The **Threat Grid Users** page opens.
2. Open the **User Details** page for the device user account (you may need to use Search to find it). The user status is currently "de-activated":

Figure 16 - User Details Page > Re-Activate User



3. Click Re**-Activate User**. A dialog opens asking you to confirm.
4. Click **Re-Activate** in the dialog to confirm.

The ESA/WSA or other integrating appliance or device can now communicate with the Threat Grid Appliance.

PRIVACY AND SAMPLE VISIBILITY

When submitting samples to a Threat Grid appliance for analysis, an important consideration is the privacy of their contents. Privacy is a particularly important consideration if sensitive documents or archive types are submitted for analysis, because locating sensitive material could be relatively easy for those with access to the Threat Grid appliance, especially with the search API.

The privacy and sample visibility model for sample submissions to Threat Grid is relatively simple: Unless samples are designated as Private, they will be visible to users who are outside the submitter's Organization. *Private* samples may only be seen by Threat Grid users within the same Organization as the user who submitted the sample.

Privacy and Visibility for Integrations

The privacy and sample visibility model is modified on Threat Grid Appliances for samples that are submitted by " Integrations." Integrations are Cisco products such as ESA/WSA appliances and other devices or third party services., (You may see the term "CSA Integrations", which refers to ESA/WSA and other Cisco appliances, devices, and other services that are integrated i.e., registered, with Threat Grid appliances via the Cisco Sandbox API.)

All sample submissions on Threat Grid appliances are Public by default, and can be viewed by any other appliance user, including Integrations, regardless of which Organization they belong to.

All appliance users can see all details of samples submitted by all other users.

Threat Grid users may also submit Private samples to the Threat Grid appliance, which are only visible to other Threat Grid appliance users, including integrations, from the same organization as the sample submitter..

Privacy and sample visibility model on Threat Grid Appliances illustrated in the table below:

Figure 17 - Privacy and Visibility on a Threat Grid Appliance

	Public Submissions (Default)	Private Submissions	Integration Submissions (Public by Default)
Users from Same Org	✔	✔	✔
Users from Different Org	✔	✖	✔
Integrations from Same Org	✔	✔	✔
Integrations from Different Org	✔	✖	✔

The green checkmark means that users have full access to the sample and the analysis results.

The red "X"s mean that users have no access to the sample or the analysis results.

The same basic privacy rules apply to Threat Grid Appliance integrations with AMP for Endpoints Private Cloud.

WIPE APPLIANCE

A new boot menu option is available with V1.4.4 that will allow you to wipe the disks on a Threat Grid Appliance.

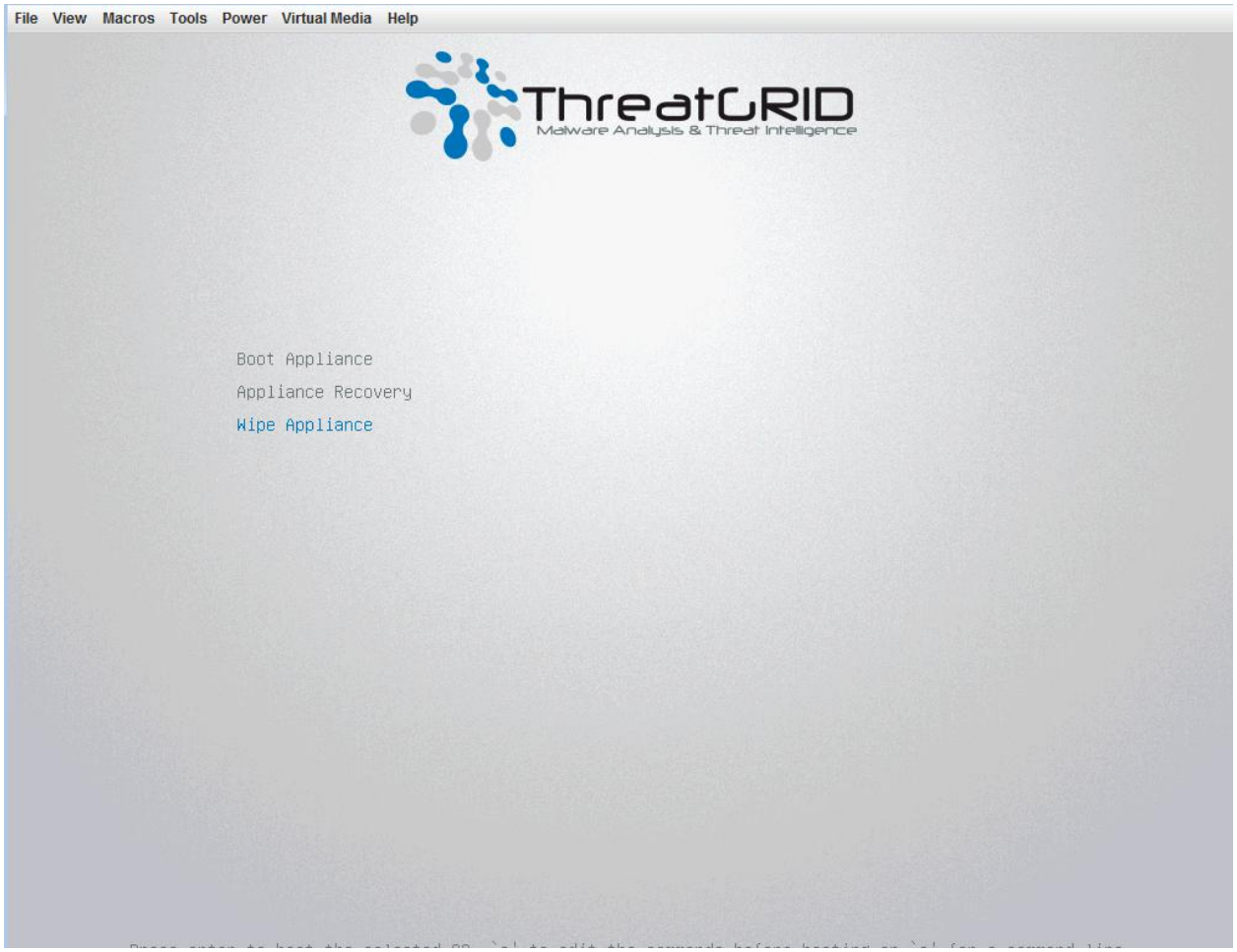
Use the Wipe Appliance option to remove all data from the appliance prior to decommissioning or returning it to the Cisco Demo Loan Program. Several variants of this process are available, some of which perform additional passes to provide safety against attempts at data retrieval using advanced techniques. (Note these techniques are believed to be ineffectual against modern hard drive encodings, so even the fastest single-pass Wipe option is considered safe and sufficient.)

IMPORTANT: Note that after performing this operation, the appliance will no longer operate without being returned to Cisco for reimaging.

1. Reboot your Appliance.

   During the boot, there will be a 4-second window in which you can select Wipe Appliance:

Figure 18 - Wipe Appliance



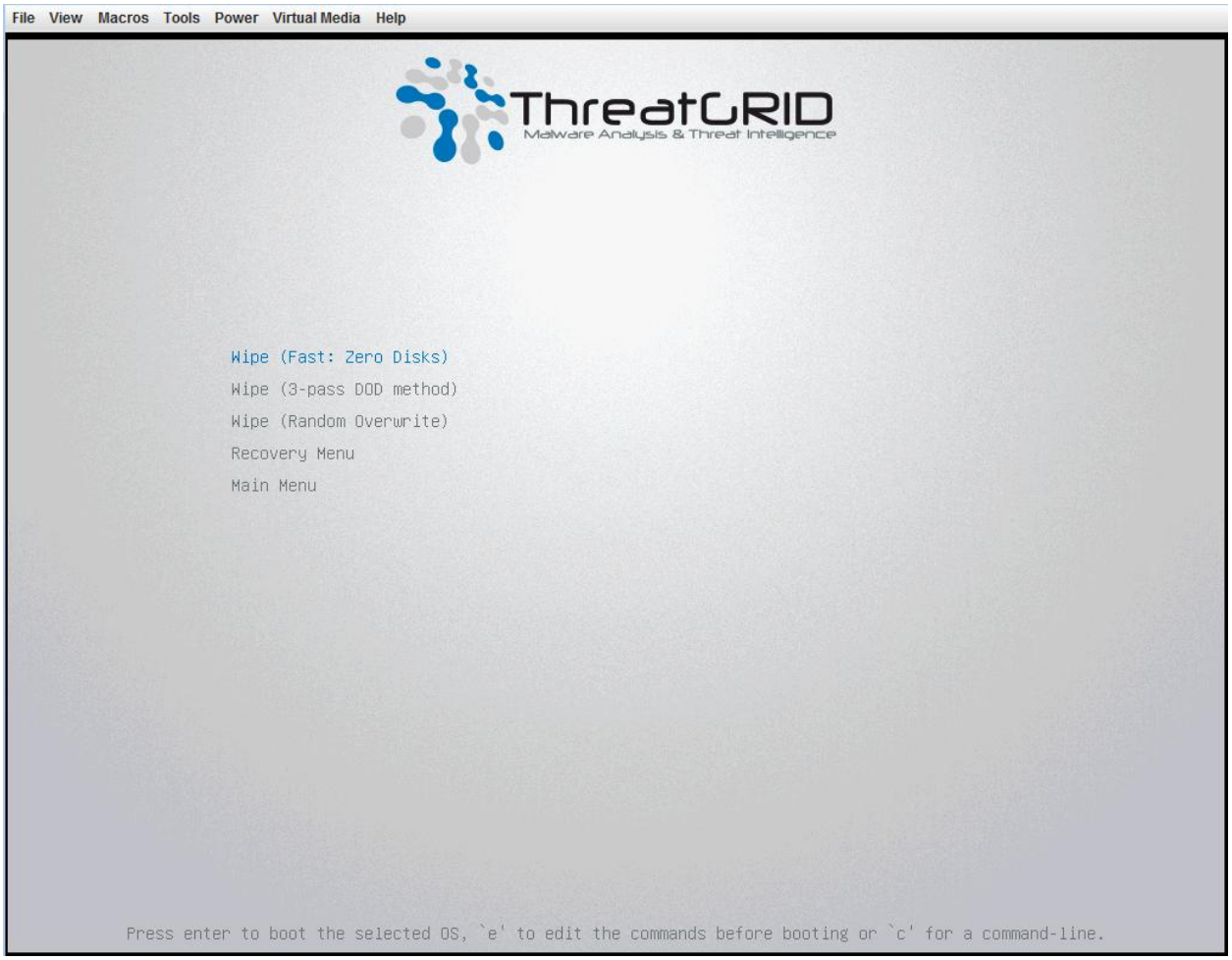
2. This option requires the following username and password:

   username: "wipe"

   password: "I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION"

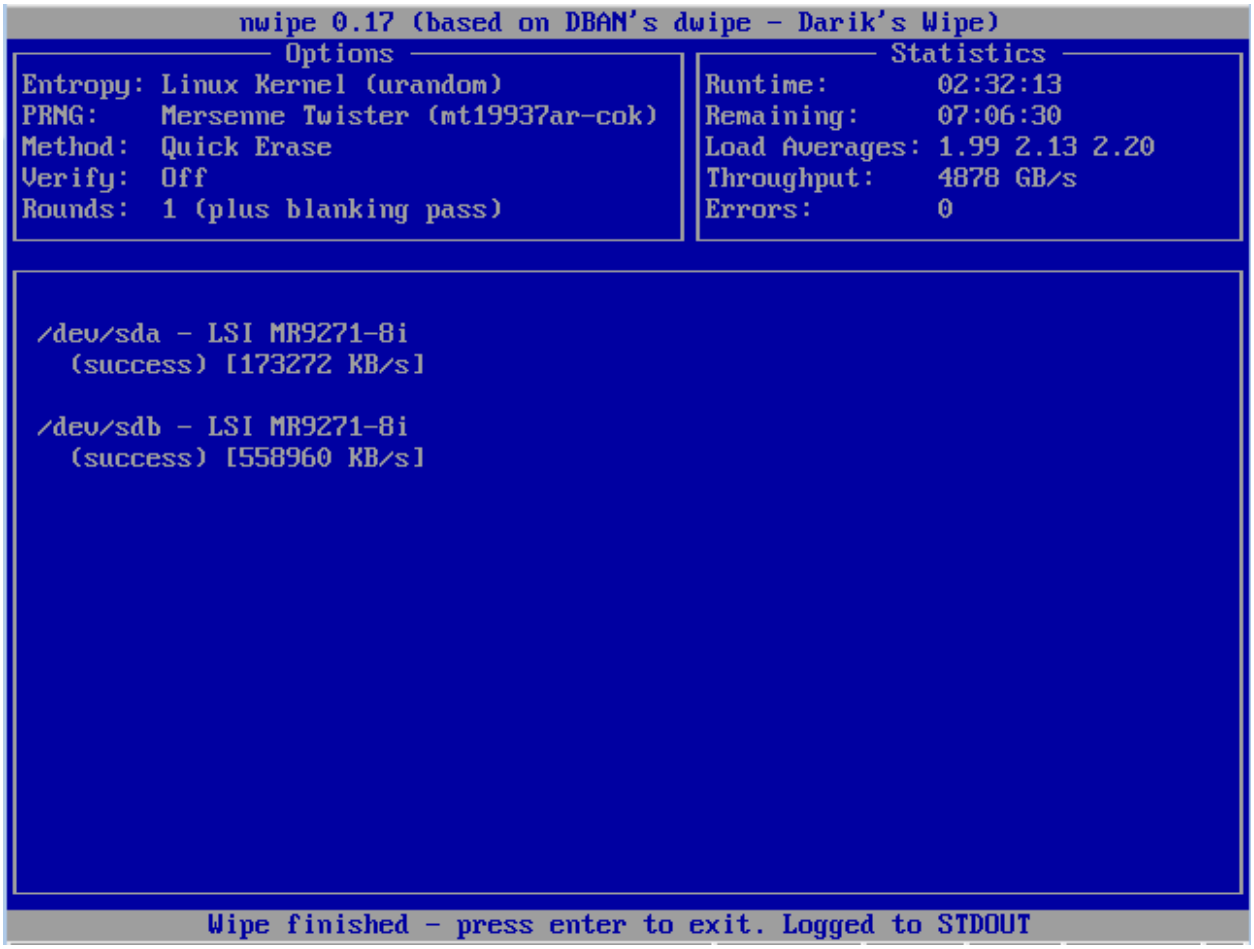
3. Next, select a Wipe option. See Wipe Options for the approximate run times of each option.

Figure 19 - Wipe Options



4. The **Wipe Finished** screen is displayed when the wipe operation is complete:

Figure 20 - Wipe Finished



5. Press **Enter** to exit.

Wipe Options

Wipe Option	Approximate Run Time
Wipe (Fast: Zero Disks)	2.5 hours
Wipe (3-pass DOD method)	16 hours
Wipe (Random Overwrite)	12 hours

BACKUPS

The 2.2.4 release introduces a backup feature. Threat Grid appliances now support encrypted backups to NFS-backed storage; initialization of data from such storage; and reset to an empty-database state into which such a backup can be loaded.

Note that reset is different from the WIPE APPLIANCE process used to allow an appliance to be shipped off customer premises without information leakage. The wipe process appropriate for that purpose already exists in the recovery bootloader, but is NOT suitable for preparing a system to restore a backup; reset is for backup preparation.

Content is encrypted with gocryptfs, a 3rd-party open-source product.

Note that filename encryption is disabled for performance reasons. As samples and other content in Threat Grid are not stored with their original names under any circumstances, this does not leak customer-owned data.

We *strongly* encourage consulting the documentation prior to use. Extended documentation regarding the backup functionality is available, and we strongly encourage consulting it prior to use. For additional technical information and instructions see the *Backup Notes and FAQ*, and the *Threat Grid Appliance Setup and Configuration Guide*, which are both available on the **Threat Grid Appliance Install and Upgrade page** on the Cisco.com website.

NFS Requirements

- Must be running the NFSv4 protocol over TCP, accessible from the appliance's admin interface.
- Configured directory, must be writable by nfsnobody (UID 65534).
- The NFSv4 server must be accessible via the Admin 10Gb interface.
- Sufficient storage. See Backup Storage Requirements below for details.

The following mount parameters are unconditionally used: `rw,sync,nfsvers=4,nofail`

Invalid NFS configuration (or configuration pointing the service at an incorrectly-configured NFS server) will generally cause the process of applying configuration to fail. Correcting this configuration in OpAdmin and reapplying should result in success.

Exposing files for write by `nfsnobody` is secure. The only processes on the Threat Grid appliance running as `nfsnobody` or with write to `nfsnobody`, are those responsible for encryption of data. Plaintext data is exposed under distinct user accounts for different subtrees according to principal of least privilege; the PostgreSQL service on the appliance cannot access ElasticSearch data or the freezer; the ElasticSearch service cannot access PostgreSQL or freezer data; etc.

Using the `nfsnobody` account simplifies configuration, preventing the need to build an `idmap.conf` for each customer's site mapping local and remote account names together.

Backup Storage Requirements

A backup store consists of the following components:

The Object Store. In practice this will generally be the bulk of the storage in use. Data retention for the bulk component of a backup store follows the same policies and limits documented for the appliance release in use – for 2.2.x-series appliances, the document at

http://www.cisco.com/c/dam/en/us/td/docs/security/amp_threatgrid/amp-threat-grid-appliance-data-retention-v2–2.pdf is applicable, and places maximum storage use for this component as 4.1TB.

The PostgreSQL database store. This contains two full backups of the PostgreSQL store, and a chain of WAL logs sufficient to allow replay from the oldest of the retained full backups. This should be less than 500GB in total.

The ElasticSearch snapshot store. This should be less than 1TB in total.

Total Storage. Thus, given the above, a backup store should not require more than **5.6TB.**

Expectations

Included in the Backup - The initial release of the Threat Grid appliance backup process includes the following customer-owned bulk data:

- Samples
- Analysis results, artifacts, flagging
- Application-layer (not OpAdmin) organization and user account data.
- Databases (including users and organizations)
- Configuration done within the Face or Mask portal UI

Not Included -

- System logs
- Previously downloaded and installed updates
- This release DOES NOT include configuration done inside the appliance OpAdmin interface, including SSL keys and CA certificates

PostgreSQL - PostgreSQL base backup takes place on a 24-hour cycle. Database backup cannot be restored, and a warning will be displayed, until this has successfully completed at least once.

ElasticSearch - ElasticSearch backup takes place incrementally, once every 5 minutes.

Freezer - Freezer backup takes place on an ongoing basis, with a job following behind every 24 hours to handle any objects which were missed from the ongoing backup.

New Key Generation - Generating a new key creates a new, independent backup store. Like the original, this new store is not valid until a base backup has taken place on a 24-hour cycle.

Backup Data Retention

PostgreSQL -For PostgreSQL, the last two successful backups and all WAL segments since those backups are retained.

ElasticSearch - For ElasticSearch, the last two 5-minute snapshots are retained.

Bulk Storage - For bulk storage, the same retention policy followed and documented for a single appliance is used for the shared store.

Backup Process Overview

The backup process on Threat Grid appliances consists of the following steps.

Step 1 Create the backup target directory according to the NFS Requirements above.

Step 2 Complete the NFS Configuration page of the setup wizard in OpAdmin. (See *Configuring a* Threat Grid Appliance to Use NFS for instructions.)

Step 3 Download the encryption key that is generated once you complete the NFS configuration.

IMPORTANT NOTE: the customer is responsible for backing up the encryption key and storing it securely!

Threat Grid does NOT retain a copy.

Backup is useless without this key!

Step 4 Reset the backup restore target. (See *Resetting a Threat Grid Appliance as a Backup Restore Target* for instructions.)

Step 5 Restore backed-up data. (You will need the encryption key from Step 3. See *Restoring Backed-Up Contents* for instructions.)

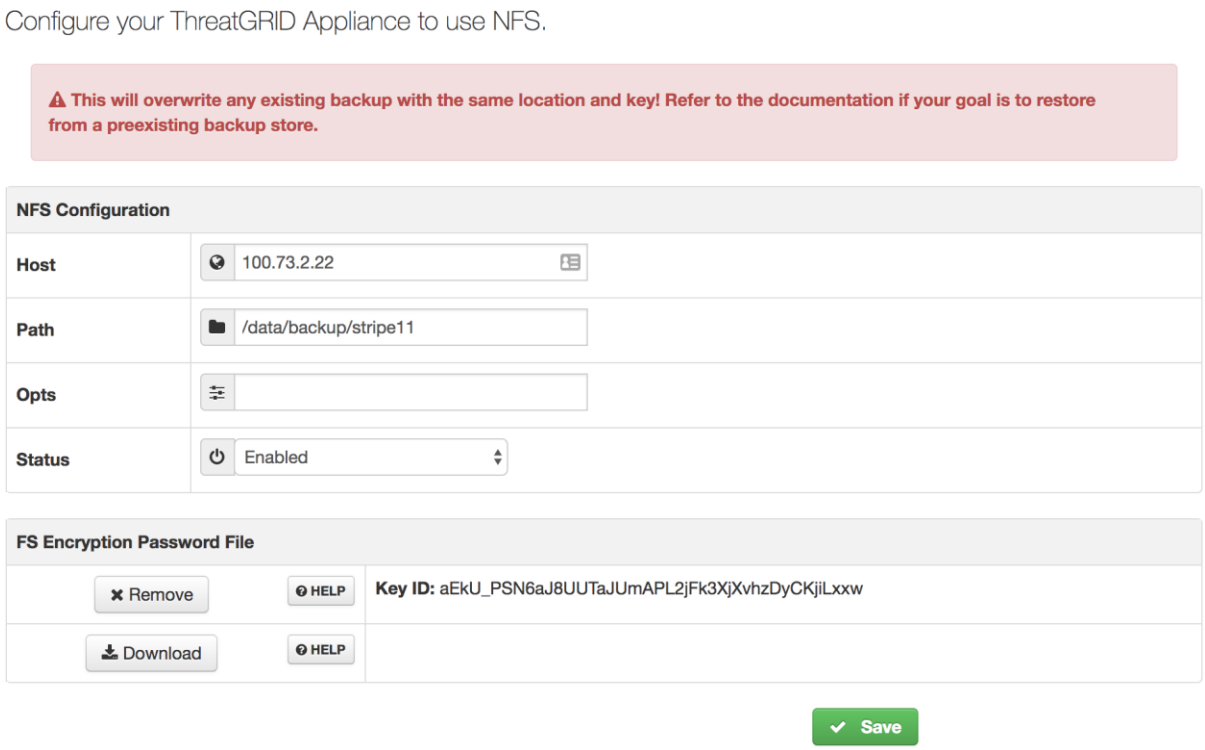
See the following sections for detailed instructions.

Configuring a Threat Grid Appliance to Use NFS

NFSv4 (NOT v3) is required for the Threat Grid appliance backup. (See NFS Requirements for more information.) NFS configuration is completed in the OpAdmin interface via a new step added to the setup wizard. A new menu entry is added for later access to NFS configuration.

1. Open the NFS Configuration page of the setup wizard in OpAdmin (**Configuration > NFS**).

Figure 21 - NFS Configuration



2. Configure the page as follows:

   Host - The address of the NFSv4 server for storing the appliance's backup data

   Path - The path to the Host server backup directory

   Opts - NFS mount options

   Status - Select Enabled from the dropdown (Pending Key).

3. Click **Save**. The page will refresh, with a FS Encryption Password Key ID now available.

   The first time you configure this page, options to **Remove** or to **Download** the encryption key become visible. **Upload** is available if you have NFS enabled but no key created. Once you create a key, **Upload** is changed to a **Download** button. (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. As already noted, backups cannot be restored without the encryption key.

4. Finish the remainder of the setup wizard as usual.

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

Backup Frequency

For bulk storage of samples, artifacts and reports, content is backed up continuously. Additionally, a pass is performed to look for and transfer missing content on a 24-hour cycle.

For the PostgreSQL database, a base backup is created on a 24-hour cycle, and incremental content is continually added thereafter - either as soon as a 16MB threshold of newly-written database content is reached, or not less than once every 5 minutes.

For the ElasticSearch database, content is incrementally added to the backup store on a 5-minute cycle.

Backup frequency cannot be controlled or tuned. As tuning these values would make estimates regarding storage usage, restore-process time, and performance overhead invalid, they are not presently tunable.

Resetting a Threat Grid Appliance as a Backup Restore Target

CAUTION! Leveraging this process will destroy customer-owned data! Be very careful, and very certain! Read through all of the documentation before working any tasks.

Before an appliance can be used as a restore target, it must be in a preconfigured state. Appliances ship in this state. However, getting one back to the preconfigured state once it has been configured requires explicit administrative action. (See *Resetting a Threat Grid Appliance as a Backup Restore Target* for more information.)

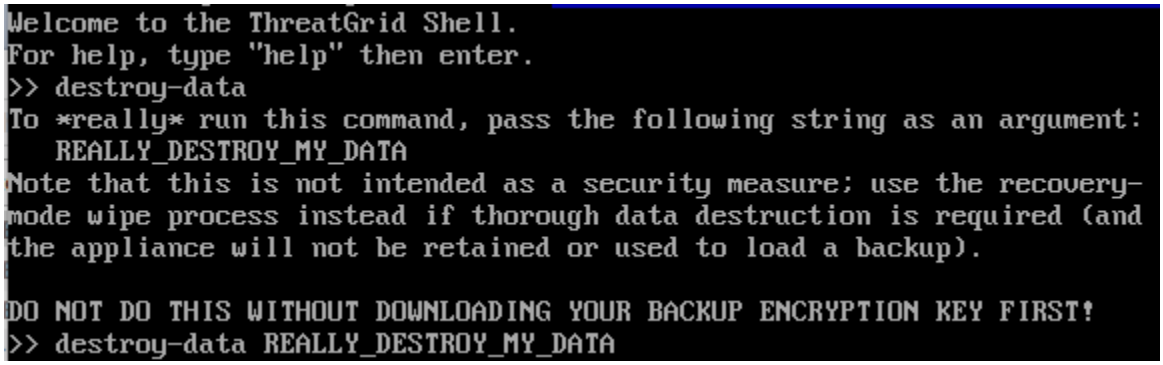
NOTE: Reset is not the same as the secure wipe available in recovery mode; only the recovery-mode secure wipe is appropriate to completely remove customer-owned data from a machine before shipping it to a DLP reimaging center. The secure wipe in recovery mode is NOT a replacement for this reset: secure wipe renders an appliance unusable until reimaged, while this reset prepares an appliance to restore a backup.

1. **If not restoring to a system fresh from manufacturing:**

   The restore target appliance must be returned to the preconfigured state by clearing pre-existing data and NFS-related configuration from the system:

   - Access the `tgsh-dialog` configuration interface, either via the appliance's TTY or via SSH.
   - Select the `CONSOLE` option to enter tgsh. (Note that entering tgsh via recovery mode is not suitable for this use case.)
   - At the `tgsh` prompt, enter the command `destroy-data`. Carefully read and follow the instructions provided with the prompt.
   - CAUTION! There is NO *Undo* from this command:

Fig. 2 - The `destroy-data REALLY_DESTROY_MY_DATA` command and argument



The following data is destroyed:

- All data listed above under ***Error! Reference source not found.***
- NFS configuration and credentials.
- The local copy of the encryption key used for NFS.

2. **If another system is actively writing to the backup being restored:**

   (For example, if this is a test restore of content being written by a second, master appliance actively used in production.)

   Generate a consistent, writable copy of the datastore, and point your appliance doing the test restore at this writable copy rather than at the store which is being continuously written.

Once the appliance is in a preconfigured state, it can function as the target for the backup store as described in the next section,

Restoring Backed-Up Contents

IMPORTANT NOTE: The system is unavailable for sample submission during the restore process.

Required: the encryption key.

Upload the Backup Encryption Key:

In the NFS Configuration page of the setup wizard in OpAdmin (**Configuration > NFS**), click **Upload** to retrieve the backup key previously generated when configuring the server on which the backup was created.

- 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.

- The install wizard checks for a directory matching the backup key, and if it finds one, will begin restoring the data into that location.
- Time Required: The amount of time required to restore data depends on the size of the backup and other factors. In testing, a 1.2GB restore simply fly by, while a 1.2TB restore required 16+ hours.
- NOTE: There is no progress bar, so on lengthy restores it may appear that the install has hung; be patient. OpAdmin will report that the restore succeeded, and the appliance will start up.
- The restored data looks just like the original data.

Notes on Backup Restore

Sample submission is unavailable during the restore process.

Backups can only be restored from the setup wizard.

Set up the same NFS store as used previously, and the same encryption key as used previously, with a process identical to the original.

The act of setting up an appliance with a prior NFS store and encryption key will trigger a restore.

IMPORTANT NOTE: Only one server can be running with data from a given backup store active at a time!

To test the restore process on a different Threat Grid appliance while your primary appliance is still operational, make a copy of a consistent snapshot of the backup store, and point a new appliance (with the encryption key uploaded) at that copy.

Backup-Related Service Notices

Network storage not mounted. Check that the network filesystem being used as a backend is fully operational, and try reapplying configuration through opadmin or rebooting your appliance.

Network storage not working. Check that the network filesystem being used as a backend is fully operational; if the system does not recover within 15 minutes of correcting any problems with the NFS server, try rebooting your appliance.

Backup filesystem access failure. Contact customer support.

No PostgreSQL backup found - This is a normal condition between the point in time when a backup store has been configured and the point in time when the first base backup (run automatically on a 24-hour cycle) takes place. Note that until this is complete, a backup is not considered complete and cannot be restored. *If and only if* this message persists for more than 48 hours, contact customer support.

Newest PostgreSQL base backup more than two days old - This indicates that the system has not been successful in generating a new base backup for PostgreSQL. If unremediated, this can result in unbounded usage on the backup store (to retain a full chain of writes necessary to restore from an increasingly-old backup point), and unacceptably long processing time needed for a restore to take place. Contact customer support.

Backup Creation Messages: - These reflect errors detected when starting or triggering a backup.

ES Backup (Creation) Inactive - Indicates that when ElasticSearch was started, the backup store was unavailable. This can be remediated by rebooting the appliance, or (if NFS and the encryption service are now functional) by logging into tgsh and running the command `service restart elasticsearch.service`.

Backup Maintenance Messages: - These reflect errors detected when checking status of previously-created backups.

ES Backup (Maintenance) snapshot (…) status FAILED - This indicates that in the most recent attempt to update the backup of the ElasticSearch database, no indices could be successfully written. Check that the NFS server is functional and has free space; if no issue can be identified and the issue persists, contact customer support.

ES Backup (Maintenance) snapshot (…) status INCOMPATIBLE - Should only occur immediately after an appliance upgrade installing a new version of ElasticSearch; will be displayed until the backup store has been upgraded to be compatible with this new release. Restoring from an INCOMPATIBLE backup may require customer service assistance, should a failure occur while in this state.

ES Backup (Maintenance) snapshot (…) status PARTIAL - Contains one of two messages in the body: *No prior successful backups seen, so retaining.* (if we're keeping a partial backup as better than none at all); or *Prior successful backups exist, so removing.* (if we're discarding that partial backup with the intent to retry later).

ES Backup (Maintenance) - Backup required (…)ms - Occurs if a backup requires more than 60 seconds. This is not necessarily an error: ElasticSearch performs periodic maintenance which can cause significant write load even on idle systems. However, if it takes place consistently when under periods of low load, investigate storage performance or contact customer service for assistance.

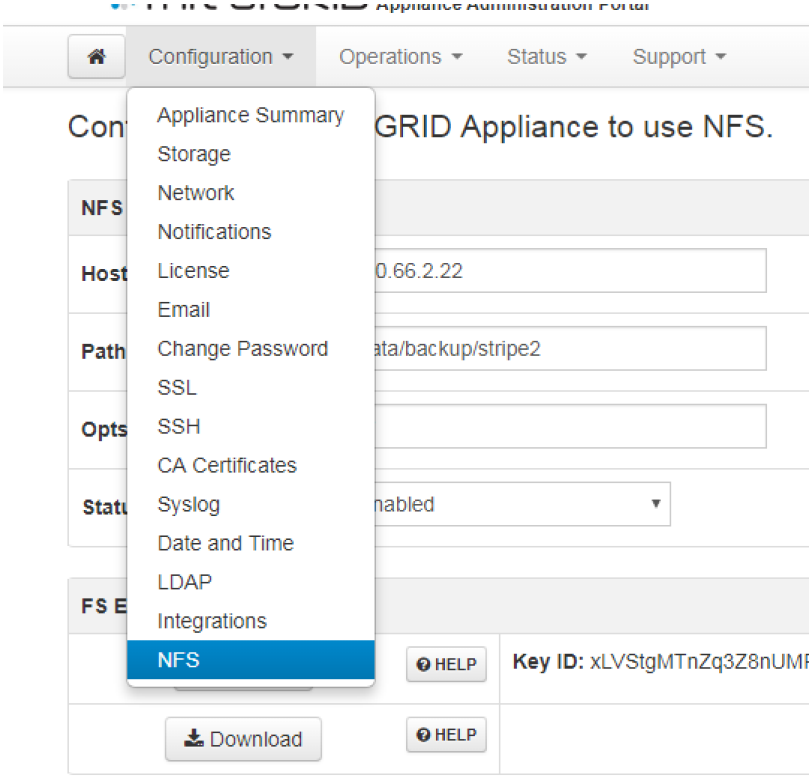
ES Backup (Maintenance) - Unable to query ElasticSearch snapshot status - ElasticSearch could not be contacted; and this failure took place after a backup creation was successfully started. Generally, this will occur in conjunction with other appliance failures, and remediation should focus on those issues. If this error is seen when the appliance is otherwise fully functional and does not go away of its own accord, contact customer support.

APPENDIX - OPADMIN MENUS

We offer the following screenshots to illustrate the various menu options that are available for performing numerous tasks within OpAdmin:

Configuration Menu

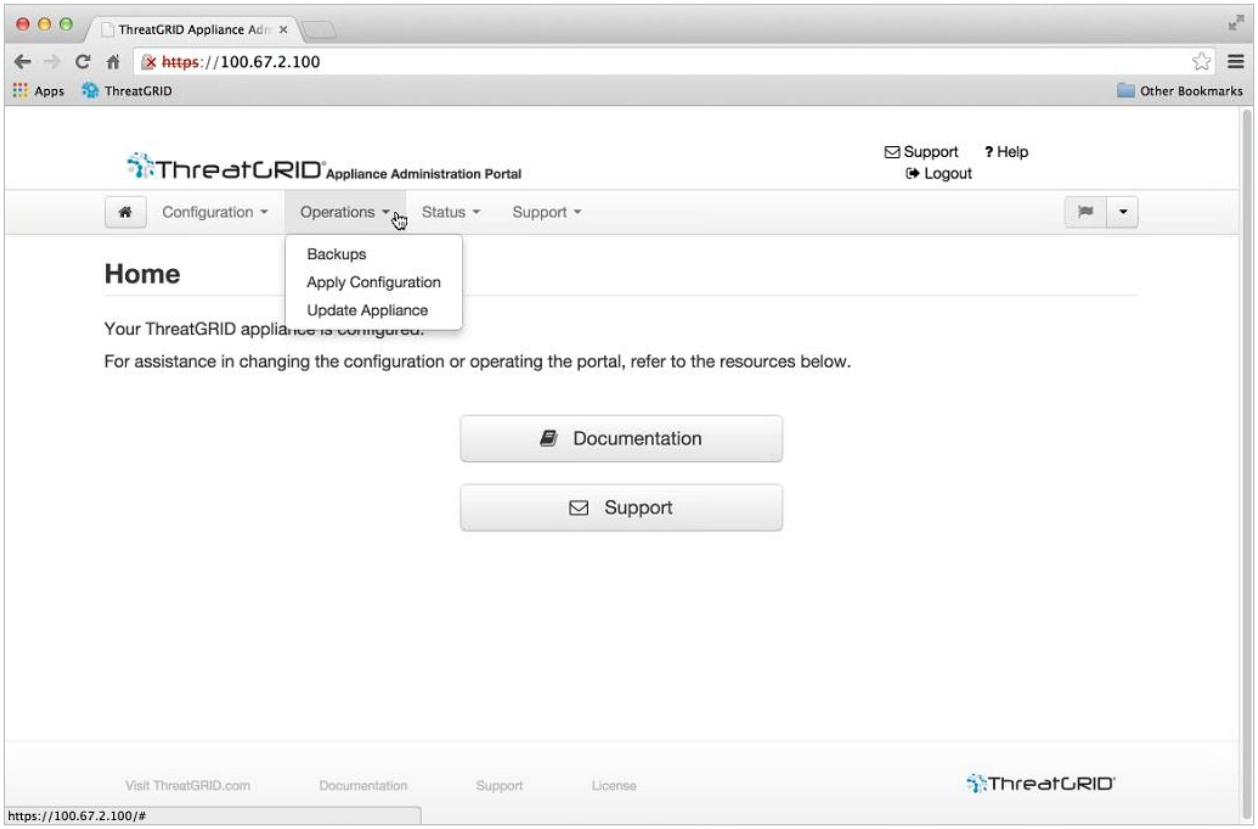
Figure 22 - OpAdmin Configuration Menu



Note: If you need to make changes in the future to your OpAdmin configuration settings, you must access them from the Configuration menu in order to be in edit mode.

Operations Menu

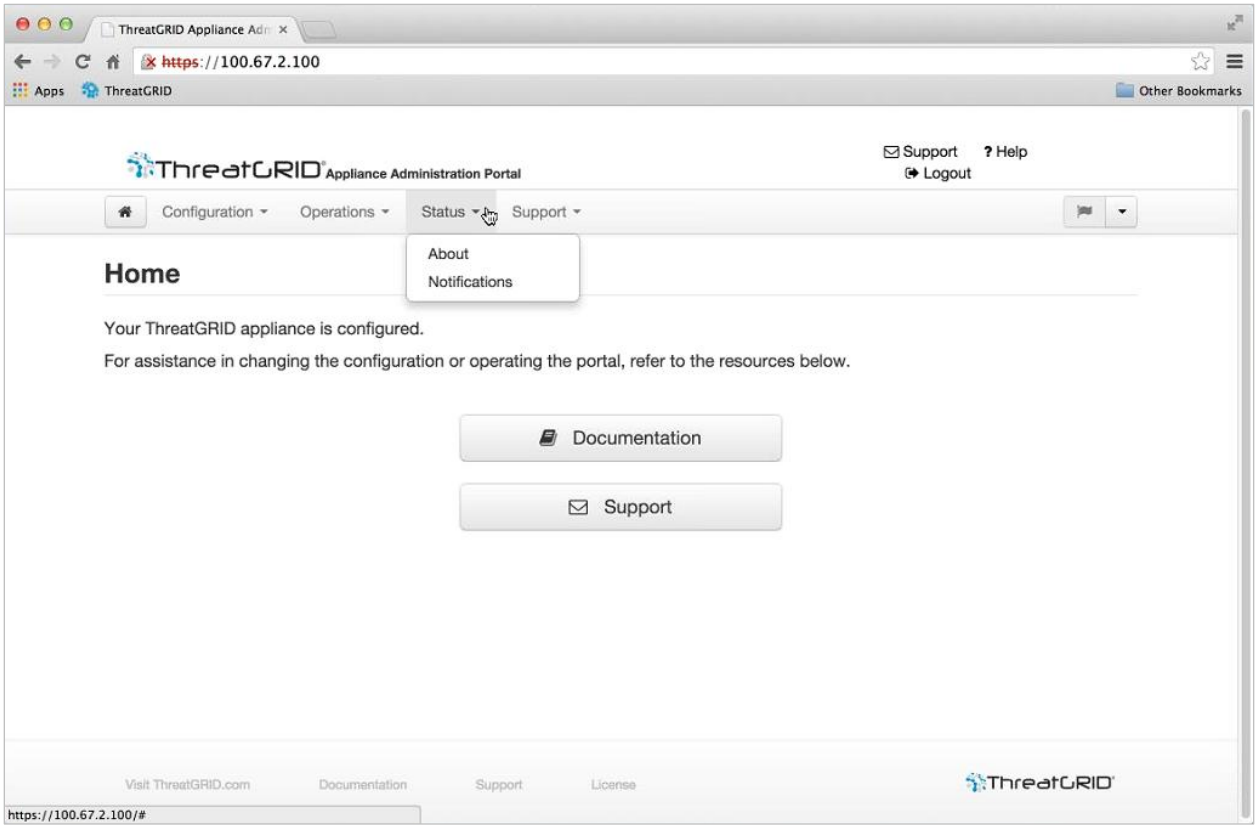
Figure 23 - OpAdmin Operations Menu



Note: Select **Update Appliance** to view the Release Notes.

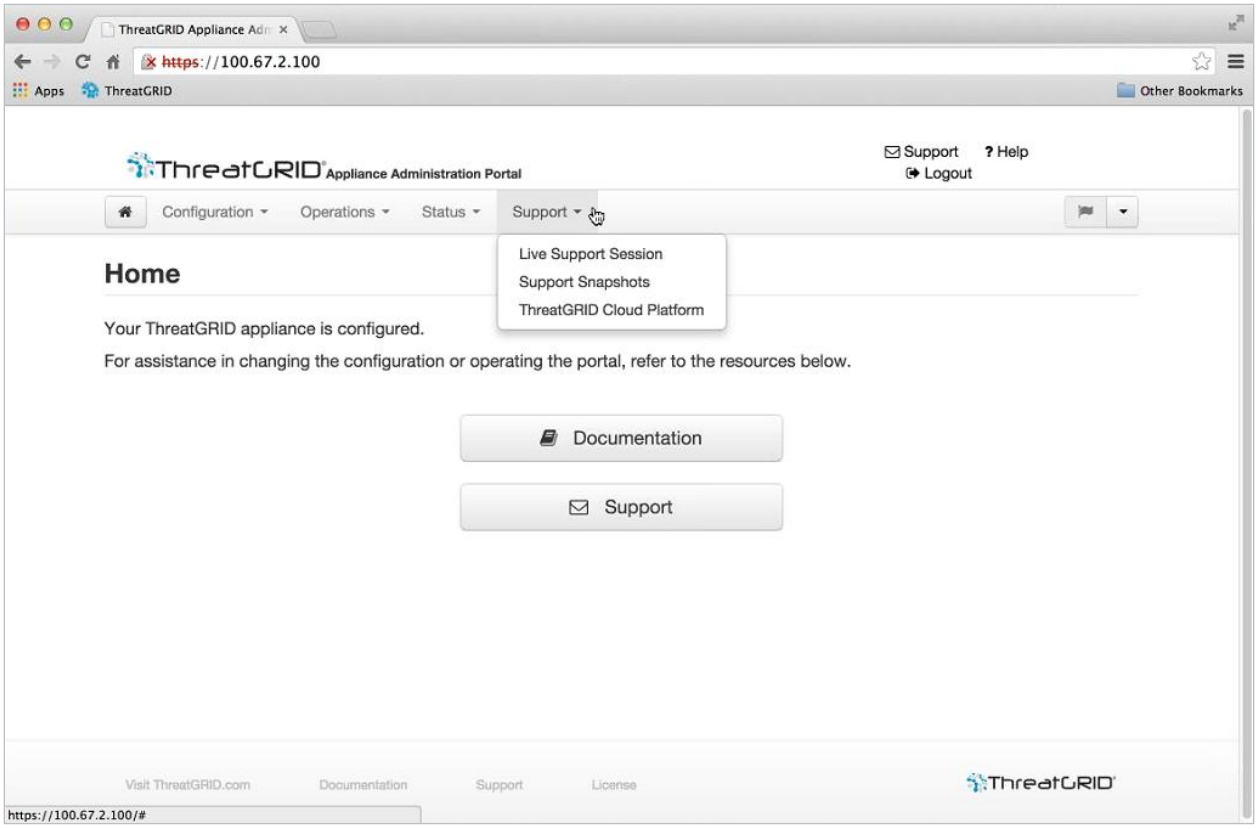
Status Menu

Figure 24 - OpAdmin Status Menu



Support Menu

Figure 25 - OpAdmin Support Menu



You can access a live support session (Support Mode) from this menu; see the Support sections for details.