# Threat Grid Appliance Administrator's Guide

**Versions: 2.5**

**Updated:** 9/14/2018

Cisco Systems, Inc. www.cisco.com

# CONTENTS



# LIST OF FIGURES

# INTRODUCTION

A Cisco Threat Grid Appliance ("TGA") is a stand-alone device based on the UCS server platform (UCS C220-M3 or UCS C220 M4), or server cluster, that is sold with the Threat Grid malware analysis platform pre-installed.

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 a 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.

### What's New for 2.5

The main changes to this guide for this release include the following:

| Section Heading | Page | Updates |
|---|---|---|
| Installing Updates | 16 | Adds more update details |
| Updates and Clusters | 21 | New section |
| Wipe and Clusters | 57 | New section |
| Joining Appliances to a Cluster | 81 | Adds a note about the need to configure NFS and clustering during the initial setup when joining an appliance |
| Sample Deletion | 88 | New section |

## What's New in 2.4.3 - 2.4.3.3

The main changes to this guide for this release include the following:

| Section Heading | Page | Updates |
|---|---|---|
| Clustering | 64 | Updates the description of a "Tiebreaker" node. |
| Clustering Prerequisites Status | 68 | New section |
| Starting a Cluster with an Existing Standalone Appliance | 70 | Adds a note about standalone appliances with databases backed up to NFS |
| Network Exit Configuration | 89 | New section. Remote exit support is available, replacing `tg-tunnel`. |
| OpAdmin Configuration Menu | 91 | Added **Network Exit** |

## 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 *Threat Grid Appliance product documentation page*.

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

## Browsers

Threat Grid recommends using the following browsers:

- Chrome
- Firefox
- Safari

**Note:** Microsoft Internet Explorer is NOT recommended and is not supported.

## 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

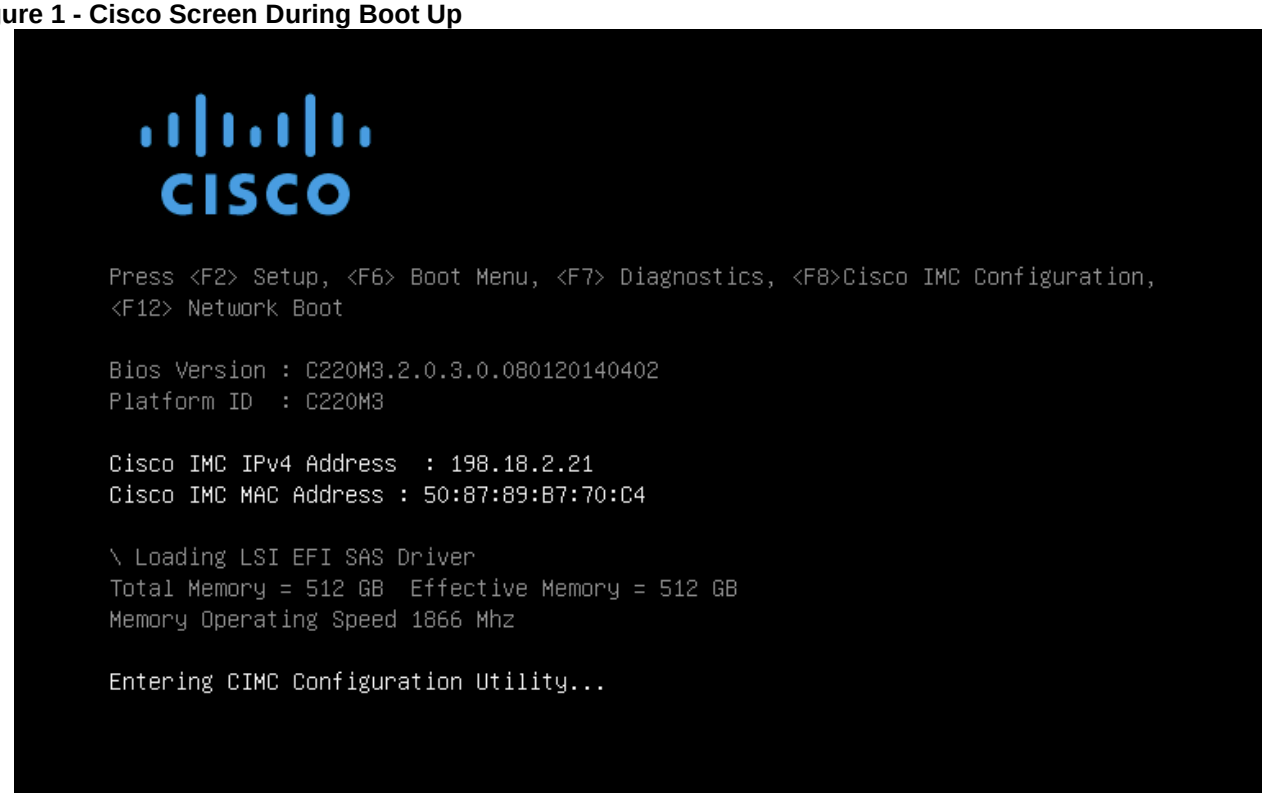
This guide assumes that the initial setup and configuration steps have been completed as described in the *Threat Grid Appliance Setup and Configuration Guide,* and that an initial test malware sample has been successfully submitted and analyzed.

# 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**

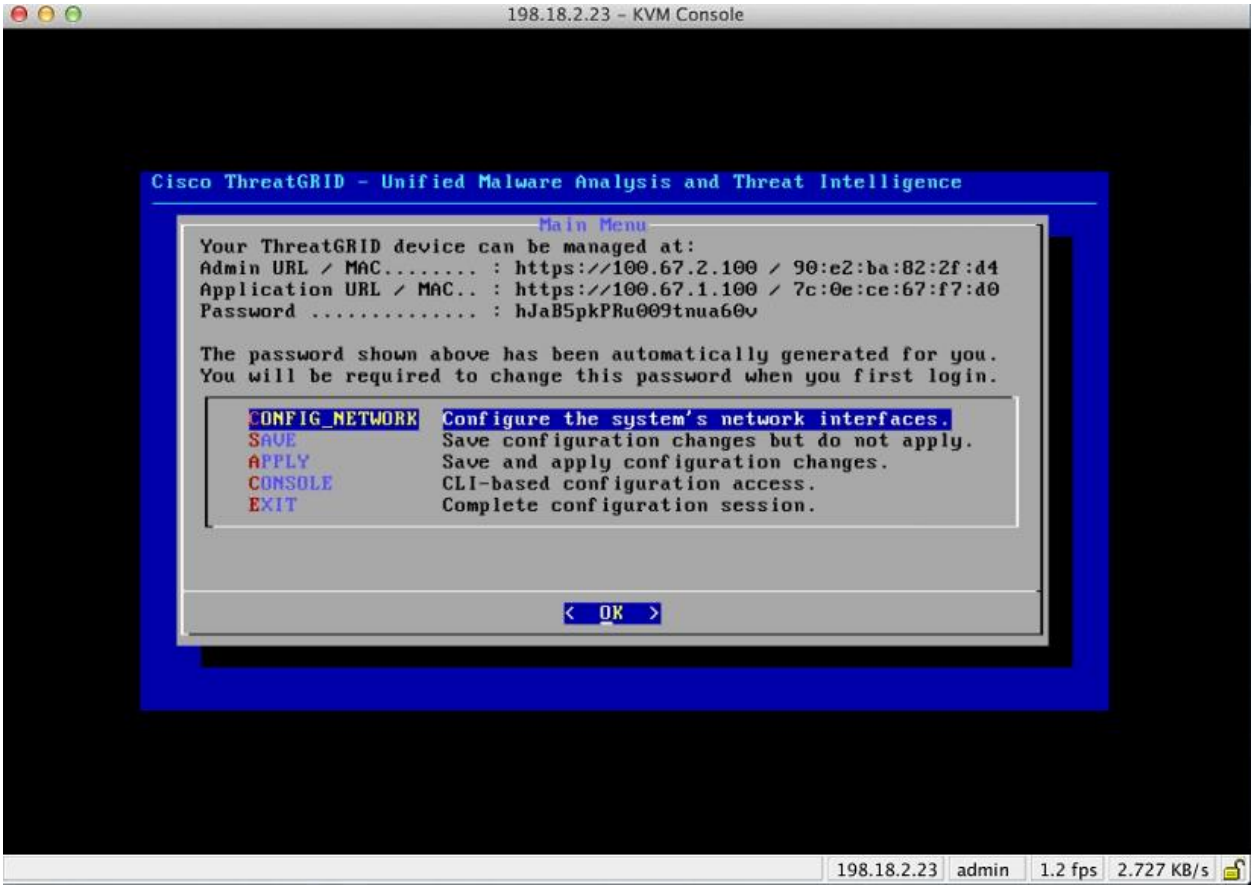



**Note:** If you want to configure the CIMC interface, press **F8** after the memory check is completed.

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 an Administrator's Password

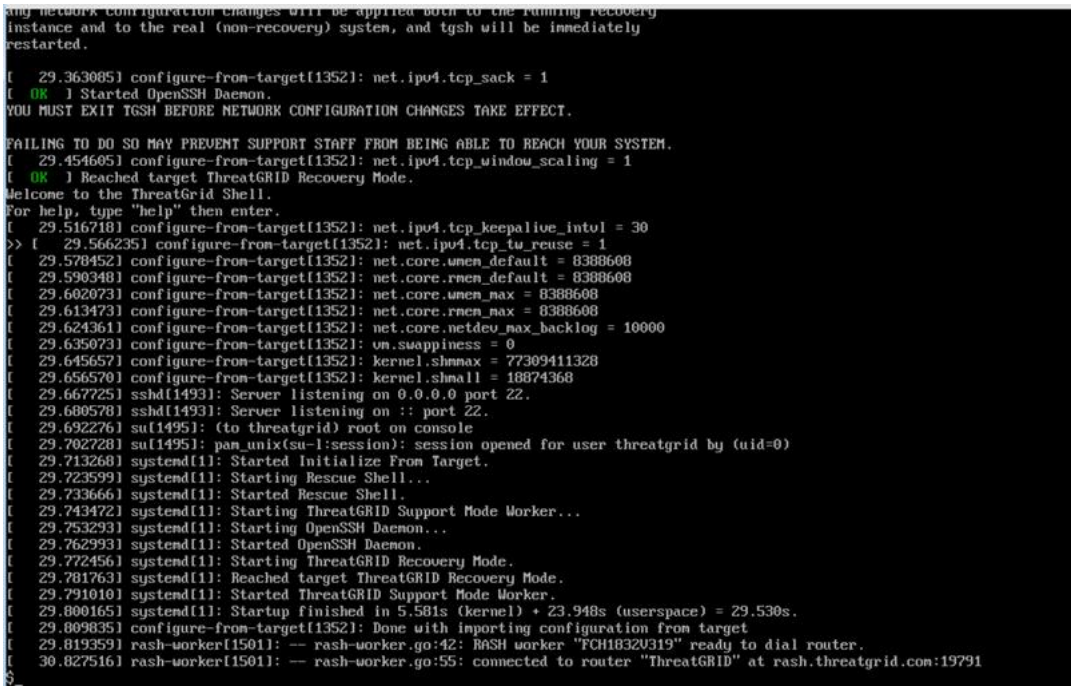
1. Reboot your Appliance.

   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**

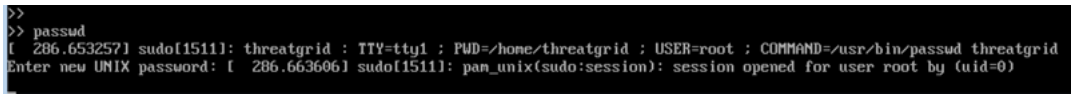

The Threat Grid Shell opens:

**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.

If the update server sends an update, the client will move all the way forward to that version. It's not always possible to skip interim releases; when it's not, the update server will require the appliance to install the release before it can download the next update round.

If the server allows you to download a version, you are eligible to move to that version directly; that is, with no intervening reboots beyond those needed for a single upgrade.

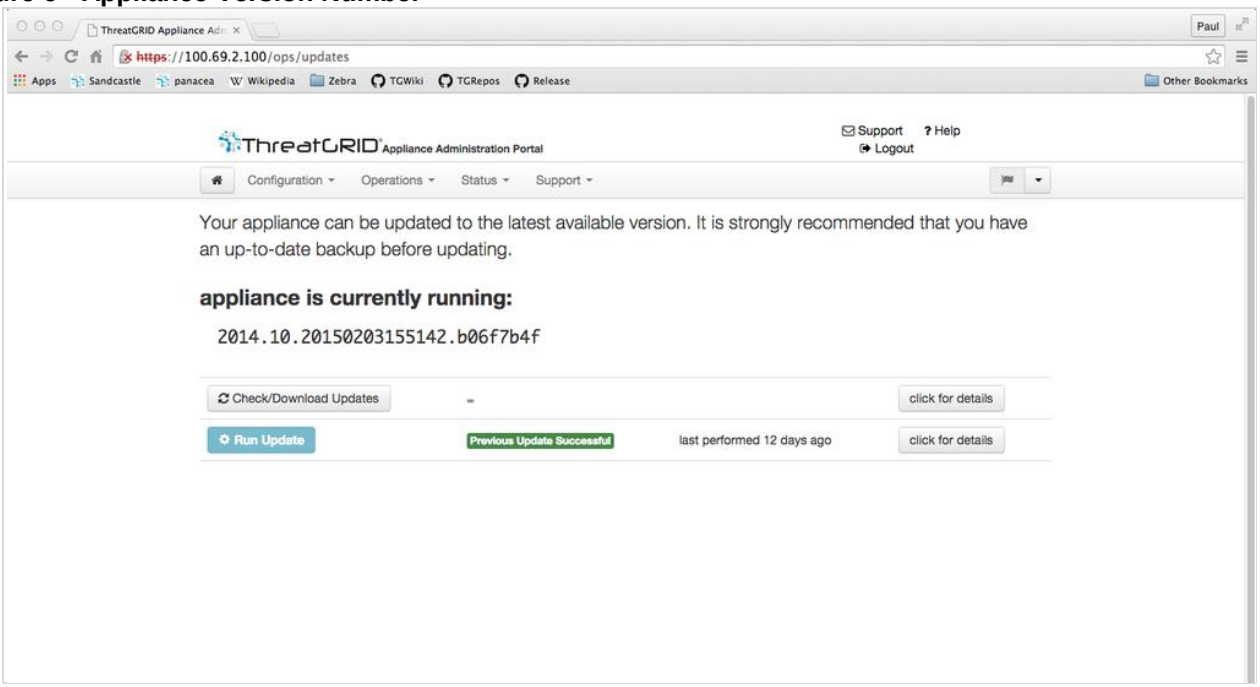
Updates are one-directional: you cannot revert to a previous version after you upgrade to a more recent version.

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.

## 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 |
|---|---|---|---|
| 2018.08.20180914205342.474e26a8.rel | 2.5 | 9/14/2018 | Win10, sample deletion, Refresh to 3.5.11 |
| 2017.12.20180601200650.e0c052b0.rel | 2.4.3.3 | 6/1/2018 | Fix cluster initialization, prune ancient ES/PG migration support |

| Build Number | Release Version | Release Date | Notes |
|---|---|---|---|
| 2017.12.20180519011227.ed8a11e9.rel | 2.4.3.2 | 5/19/2018 | ClamAV update for CVE-2018-1000085. Bug fixes. |
| 2017.12.20180501005218.4e3746f4.rel | 2.4.3.1 | 5/1/2018 | PG schema reporting for DDL error detection at update check |
| 2017.12.20180427231427.e616a2f2.rel | 2.4.3 | 4/27/2018 | Remote Virtual Exit Localization; direct standalone-to-cluster migration |
| 2017.12.20180302174440.097e2883.rel | 2.4.2 | 3/2/2018 | Clustering |
| 2017.12.20180219033153.bb5e549b.rel | 2.4.1 | 2/19/2018 | Clustering support in OpAdmin. Refreshes the portal software to 3.4.59. |
| 2017.12.20180130110951.rel | 2.4.0.1 | 1/30/2018 | Security update to ClamAV only |
| 2017.12.20171214191003.4b7fea16.rel | 2.4 | 12/14/2017 | Clustering EFT.<br>jp/kr contsubs. Refresh portal to 3.4.57. |
| 2016.05.201711300223355.1c7bd023.rel | 2.3.3 | 11/30/2017 | Starting point for 2.4 upgrade |
| 2016.05.20171007215506.0700e1db.rel | 2.3.2 | 10/7/2017 | Elasticsearch shard count reduction. |
| 2016.05.20170828200941.e5eab0a6.rel | 2.3.1 | 8/28/2017 | Bug fixes. |
| 2016.05.20170810212922.28c79852.rel | 2.3 | 8/11/2017 | Automates license download. Refreshes the portal software to 3.4.47. |
| 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. |

| Build Number | Release Version | Release Date | Notes |
|---|---|---|---|
| 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. |
| 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 | |

| Build Number | Release Version | Release Date | Notes |
|---|---|---|---|
| 2015.08.20160131061029.8b6bc1d6 | 2.0 | 2/11/2016 | Force update to 2.0.1 from here |
| 2014.10.20160115122111.1f09cb5f | 1.4.6<br>**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 | | |
| 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.

## Updates and Clusters

Historically, on standalone appliances, database migrations associated with updates would occur while the system was offline in single-user mode, *except* in a cluster, where the updates would occur after the first upgraded node came back online. (The exception to this was for unusually long updates that could be run in the background, which we handled on a case-by-case basis.)

Beginning with release 2.5.0, database schema updates are going to behave the same way that clusterd ones have worked in the recent past, and take place after the system finishes reboot. This may potentially cause that boot take slightly longer. (Very long ones will continue to be handled case-by-case.)

In prior releases, non-clustered systems with backup support enabled would make a best-effort attempt to operate correctly when their NFS server was down. Due to changes in ElasticSearch functionality, we can no longer guarantee this behavior.

# 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

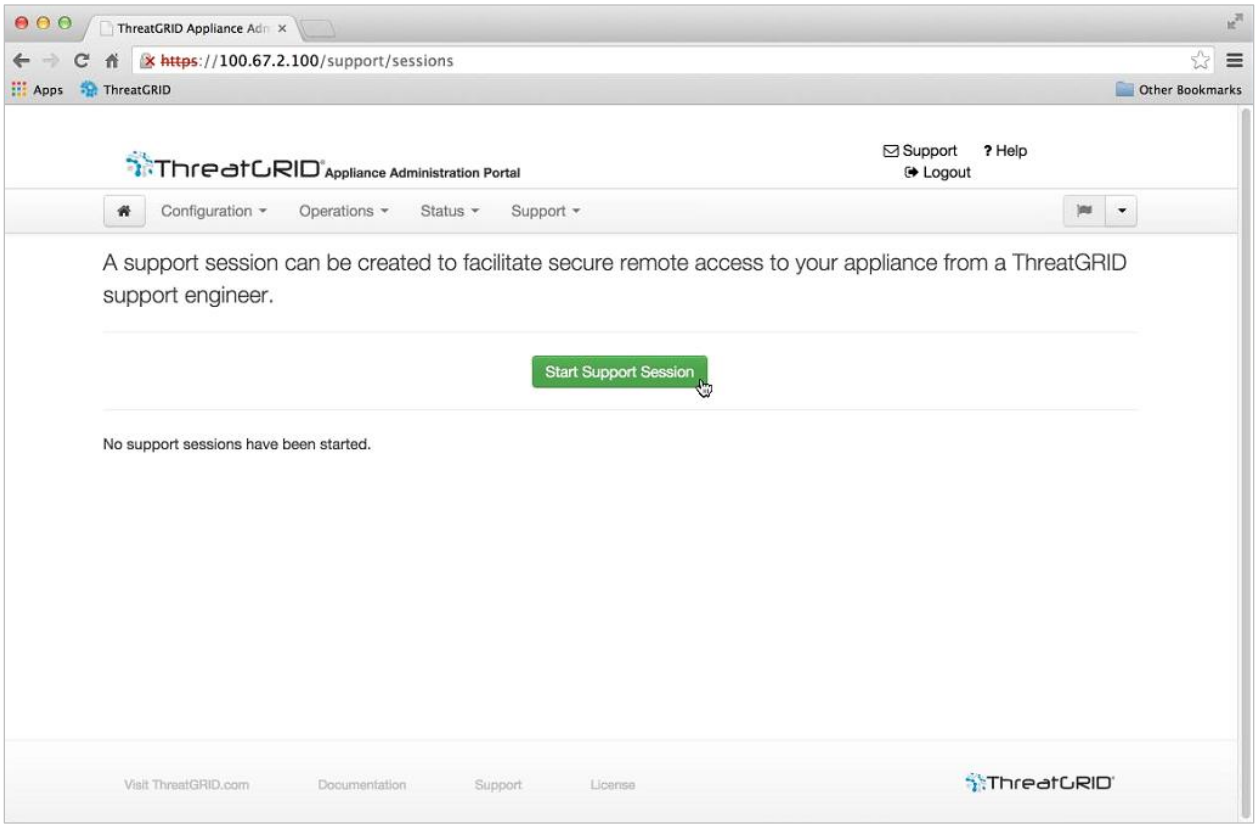
## Support Mode

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 dropdown arrow next to your login name in the navigation bar).

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.

### 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.

### Adding Multiple Appliance Administrators

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:

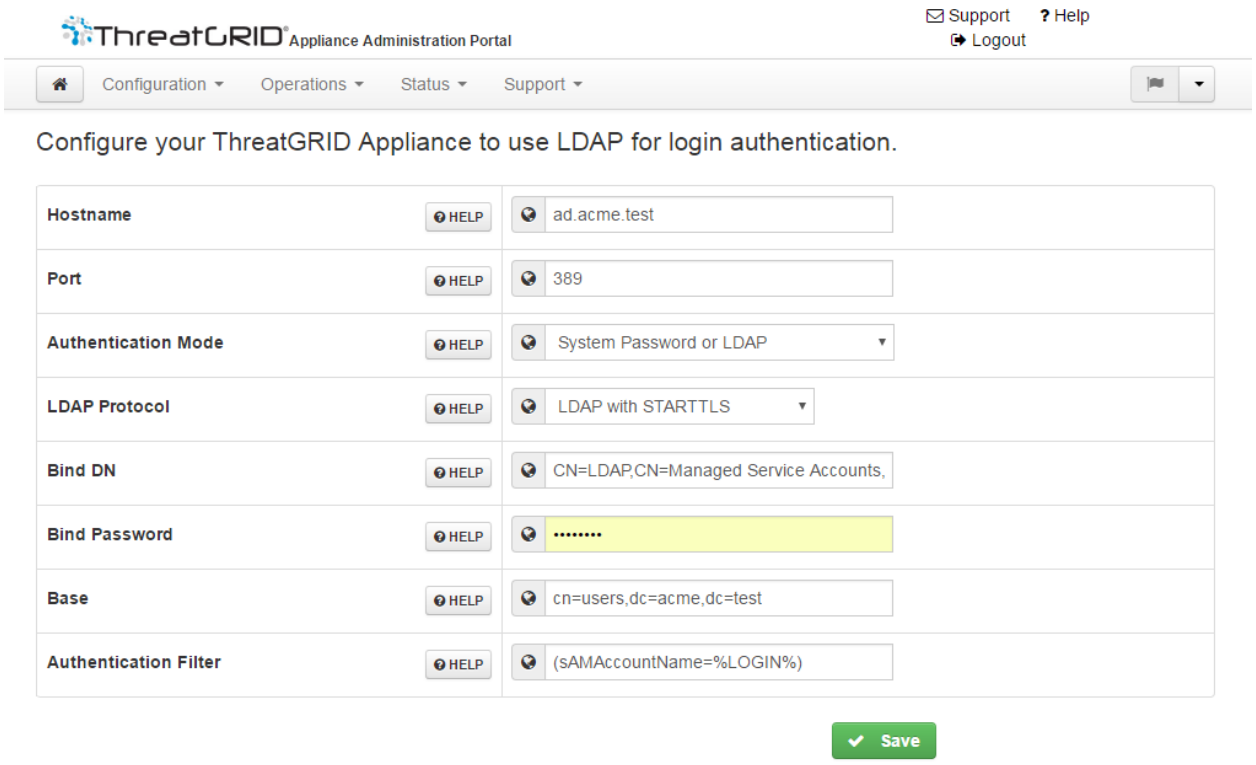
- The “dual” authentication mode (**System Password or LDAP**) is required in order to avoid accidentally locking yourself out of the appliance when setting up LDAP. Selecting **LDAP Only** is not allowed initially; you must go through dual mode to make sure it works first. You will need to log out of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

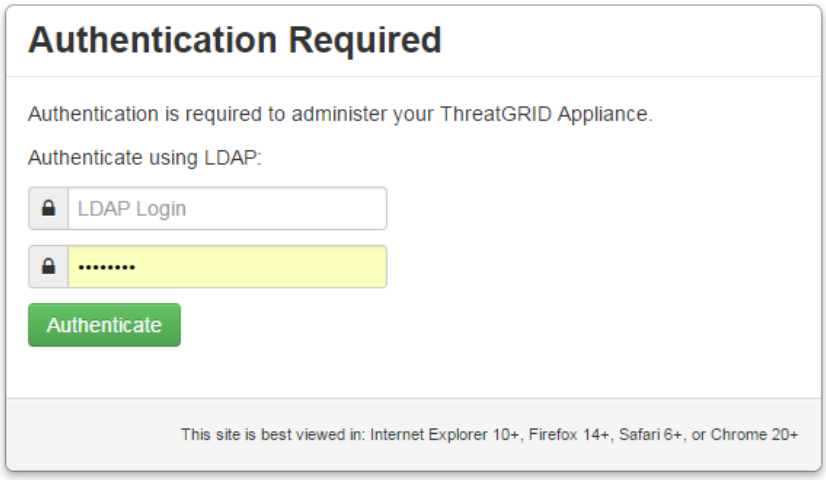
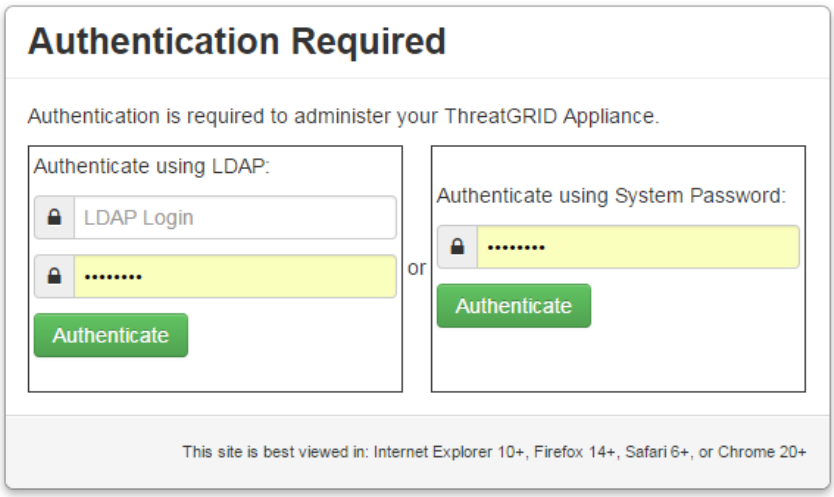



**Figure 10 - System Password or LDAP**



# Configuring Third Party Detection and Enrichment Services

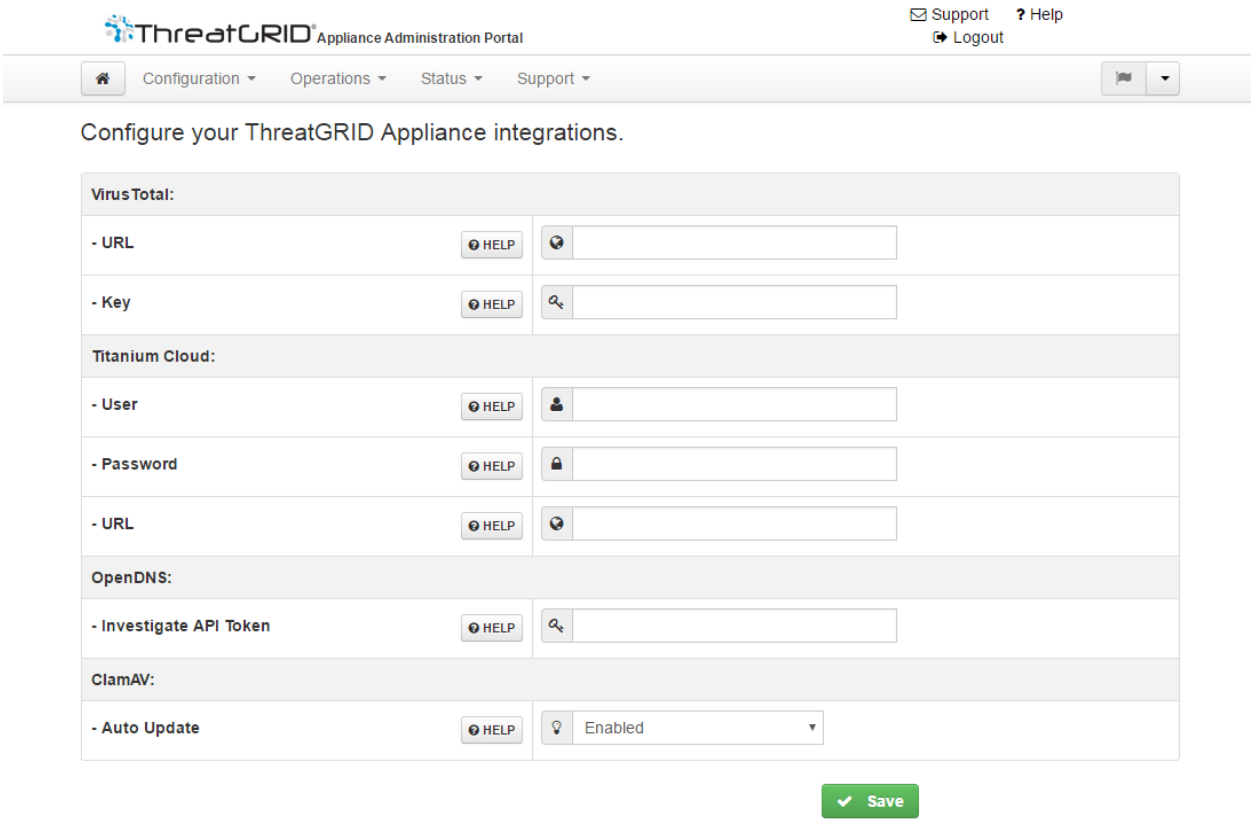
With version 2.2, integrations with several third party detection and enrichment services, including OpenDNS, TitaniumCloud, and VirusTotal, can be configured on the appliance using the new Integration Configuration page.

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

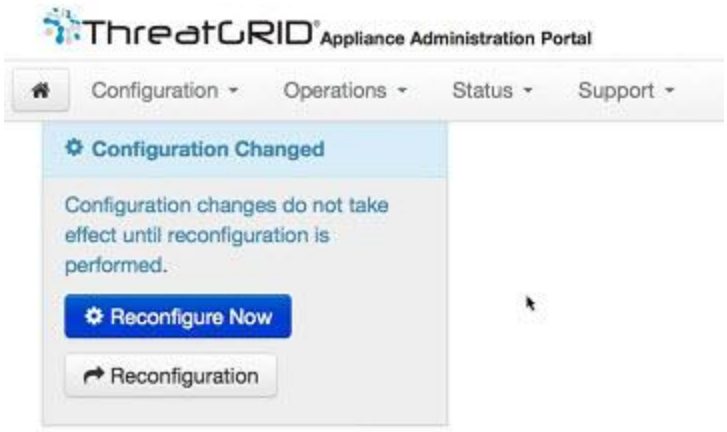
With the 2.2 update, ClamAV signatures can be automatically updated on a daily basis. This is enabled by default, and can be disabled from the new Integrations Configuration page (above).

# 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.

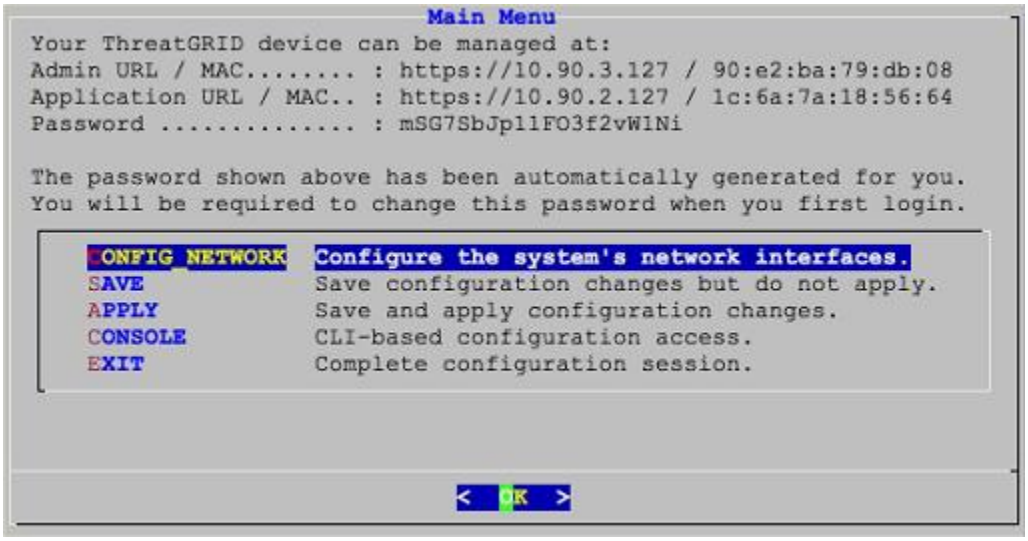
TGSH Dialog displays the information you will need to in order to access and configure the OpAdmin Portal interface.

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.

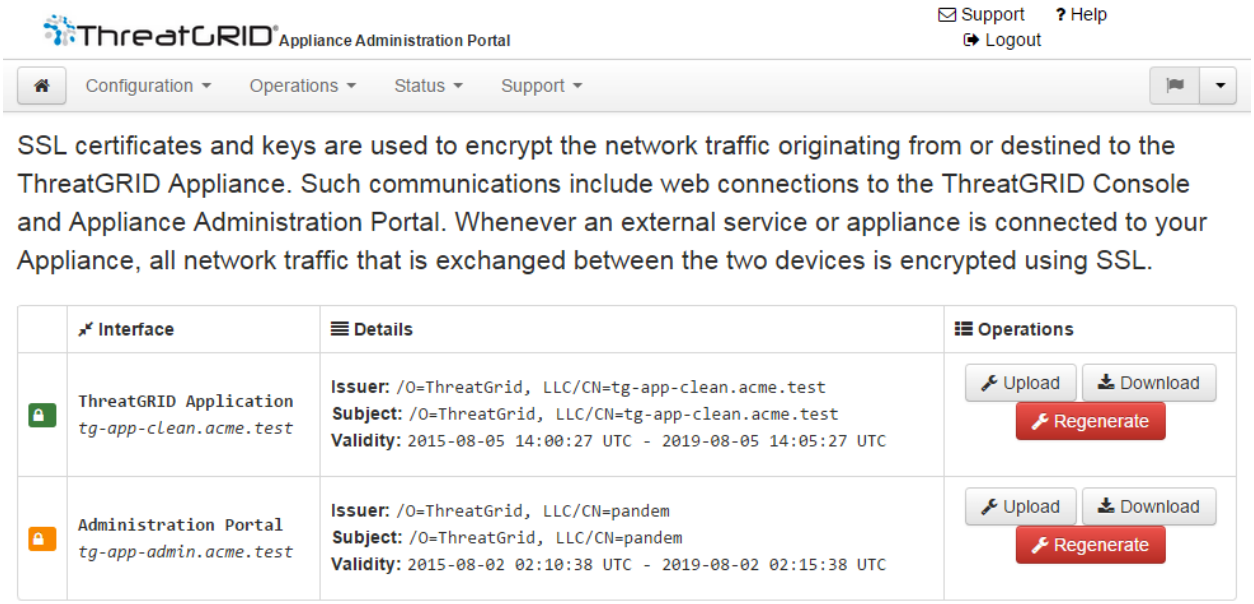
## Configuring SSL Certificates for Inbound Connections

: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, AMP for Endpoints Private Cloud (formerly known as 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 dropdown on the navigation bar next to your login name, select **Manage FireAMP Integration**. The Disposition Update Service page opens (See Figure 15 - Disposition Update Syndication Service page below.)
2. Enter the **AMP for Endpoints Private Cloud URL**, the **admin user name** and **password** provided by the AMP for endpoints 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 AMP for Endpoints Private Cloud 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:
https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

The WSA user guides are located here:
https://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 as normal (i.e., no integration yet).<br><br>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**<br><br>If you will deploy a self-signed SSL certificate:<br><br>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.)<br><br>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.<br><br>Use the hostname, not the IP address. | |
| **4** | | **Verify Connectivity**<br><br>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:**<br><br>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<br><br>1. Select **Security Services** > **File Reputation and Analysis**.<br><br>2. Click **Enable**.<br><br>3. Click **Edit Global Settings**.<br><br>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.<br><br>4. In the **File Analysis** section, select the file types to send to the Cloud for analysis.<br><br>5. Configure the **Advanced Settings for File Analysis** as needed, according to the ESA or WSA guides:<br><br>**File Analysis Server URL:**<br><br>Select **Private Cloud**.<br><br>**Server:**<br><br>**URL** of the on-premises Cisco Threat Grid appliance.<br><br>Use the hostname, not the IP address, for this value and for the certificate.<br><br>**SSL Certificate:**<br><br>Upload a self-signed certificate that you have generated from your on-premises Cisco Threat Grid appliance.<br><br>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.<br><br>6. Submit and commit your changes.<br><br>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**<br><br>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**<br><br>1. Log into the Threat Grid Portal UI as Admin.<br><br>2. From the navigation bar dropdown menu next to your login name, select **Manage Users**. The **Threat Grid Users** page opens.<br><br>3. Open the **User Details** page for the device user account (you may need to use Search to find it).<br>The user status is currently "de-activated".<br><br>4. Click Re**-Activate User**. A dialog opens asking you to confirm.<br><br>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 as normal (i.e., no integration yet).<br><br>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:**<br><br>Select **Integrations > Threat Grid** and go to the **Connection to Threat Grid** section.<br><br>To complete the connection with the Threat Grid appliance, you have to trust it. You need its DNS hostname, SSL certificate, and API key.<br><br>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: –**<br><br>In the Threat Grid appliance OpAdmin interface, select **Configuration > SSL**<br><br>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.)<br><br>**Hostname**<br><br>Select **Configuration > Hostname**<br><br>**API Key**:<br><br>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:<br><br>1. Go to the **Threat Grid Portal UI**.<br><br>2. From the navigation bar dropdown menu next to your login name, select **Manage Users**.<br><br>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:<br><br>1. Enter the TGA Hostname<br>2. Enter the Threat Grid API Key for the account that is to be used for integrations.<br>3. Choose the TGA SSL Certificate file.<br>4. Click Save Configuration.<br>5. Click Test Connection.<br>6. Once the connection test passes, you will need to run the Reconfiguration on the AMP for Endpoints Private Cloud to apply the changes.<br><br>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.<br><br>(For more information, please refer to the user documentation for the AMP for Endpoints Private Cloud.) |
| **4** | **Set up the Disposition Update Service**<br><br>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):**<br><br>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.<br><br>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:**<br><br>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:<br><br>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.<br><br>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**.<br><br>3. The certificate is retrieved.<br><br>4. Click **Import**.<br><br>(OR click **Import from Clipboard.** Paste the PEM from the clipboard, and click **Add Certificate**.) | |

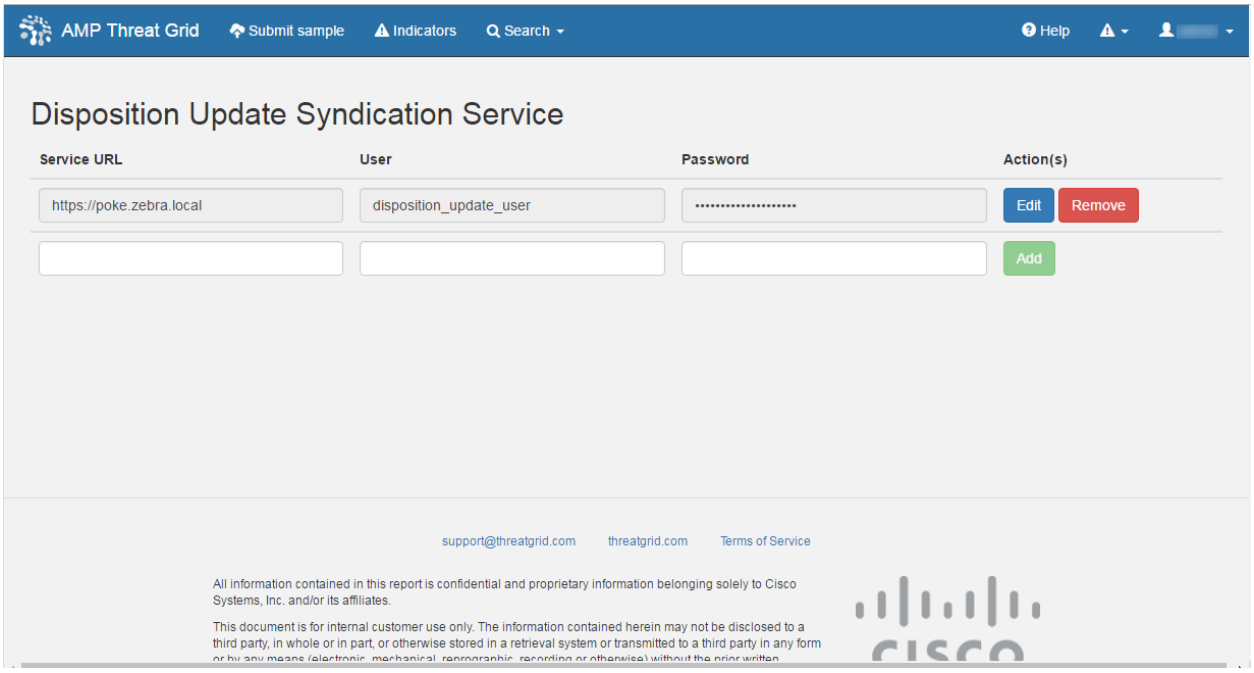
| STEPS | Threat Grid Appliance ("TGA") | AMP for Endpoints Private Cloud |
|---|---|---|
| **4.3** | **FireAMP Integration Management:**<br><br>In the Threat Grid Face Portal UI, from the upper-right menu select **Manage FireAMP Integration**. The Disposition Update Syndication Service window opens (see below).<br><br>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**).<br><br>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 Administrator's menu, and select **Manage Organization**.

   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 creating and managing user accounts - including how to add users - see the Threat Grid Portal UI online help: From the navigation bar select **Help > Using Threat Grid Online Help > Managing Threat Grid Users**.

**NOTE:** Users can only be removed a) via the API, b) if they have submitted no samples.

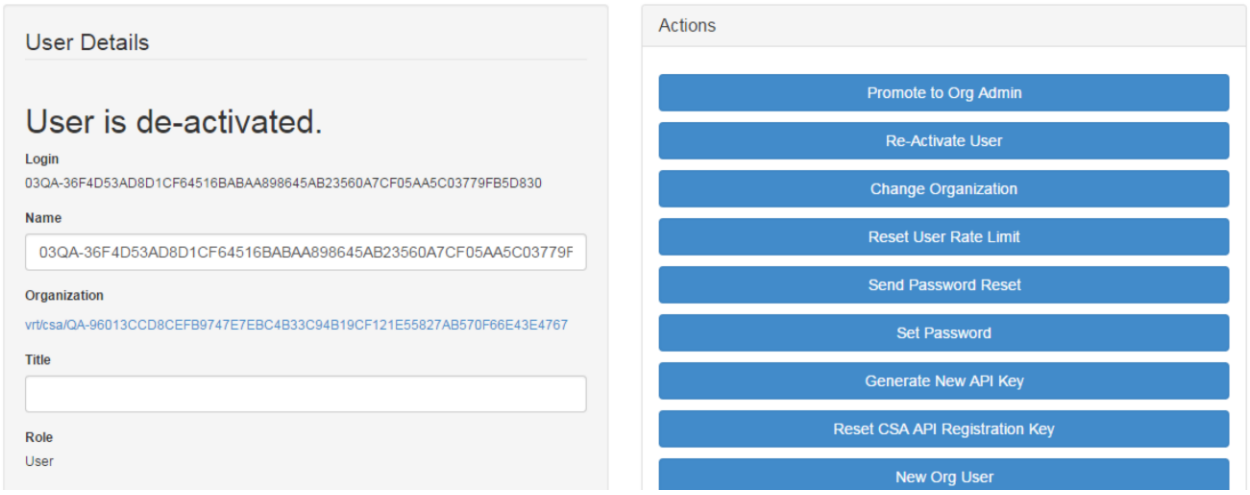
Managing device user accounts for integrating Cisco ESA/WSA appliances and other devices is described in the next section.

# 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.
2. From the navigation bar dropdown menu next to your login name, select **Manage Users**. The **Threat Grid User Detailss** 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":

**Figure 16 - User Details Page > Re-Activate User**




4. Click **Re-Activate User**. A dialog opens asking you to confirm.
5. Click **Re-Activate User** 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.

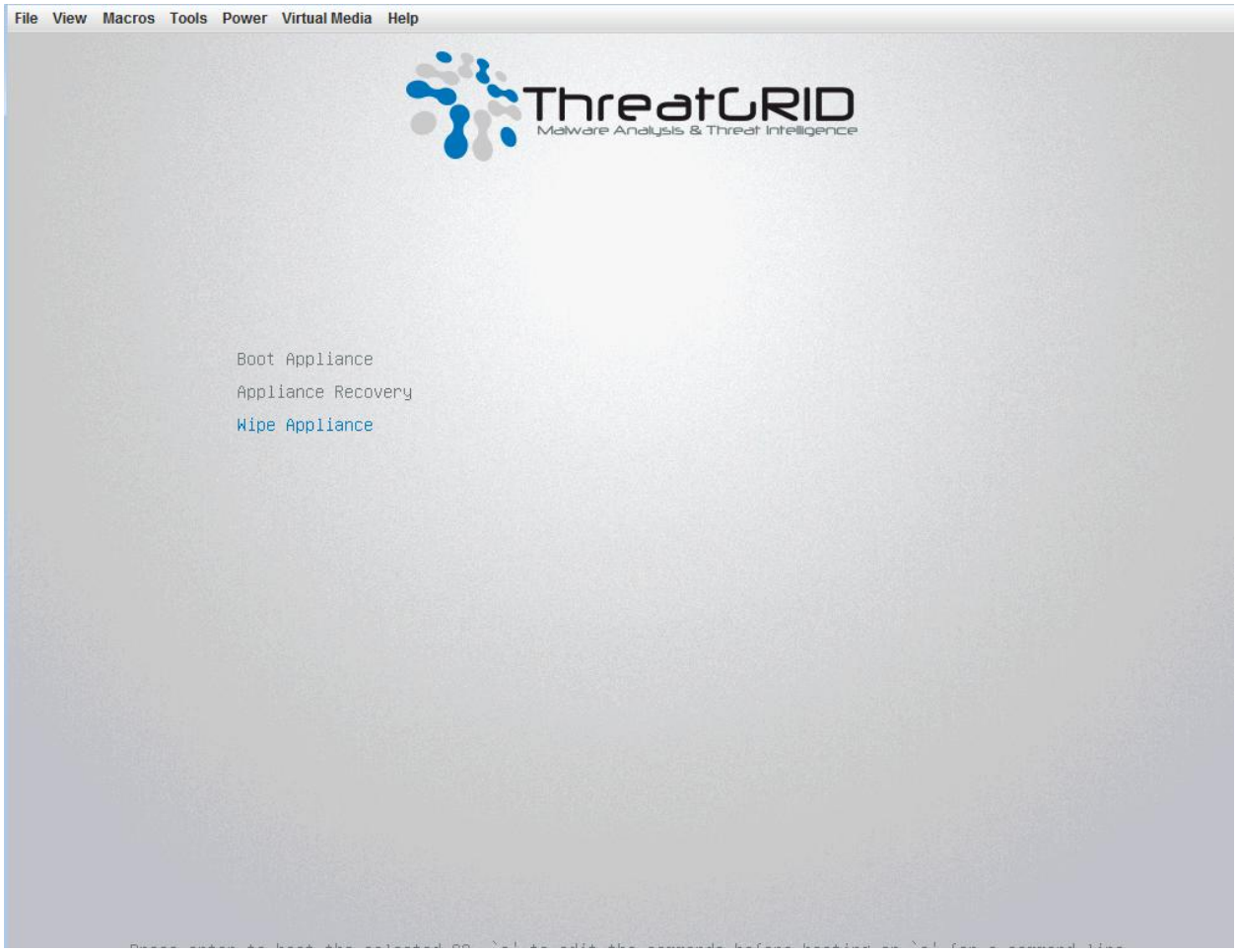
Use the Wipe Appliance option to remove all data from the appliance prior to decommissioning or returning it to the Cisco Demo Loan Program. Several variants of this process are available, some of which perform additional passes to provide safety against attempts at data retrieval using advanced techniques. (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**



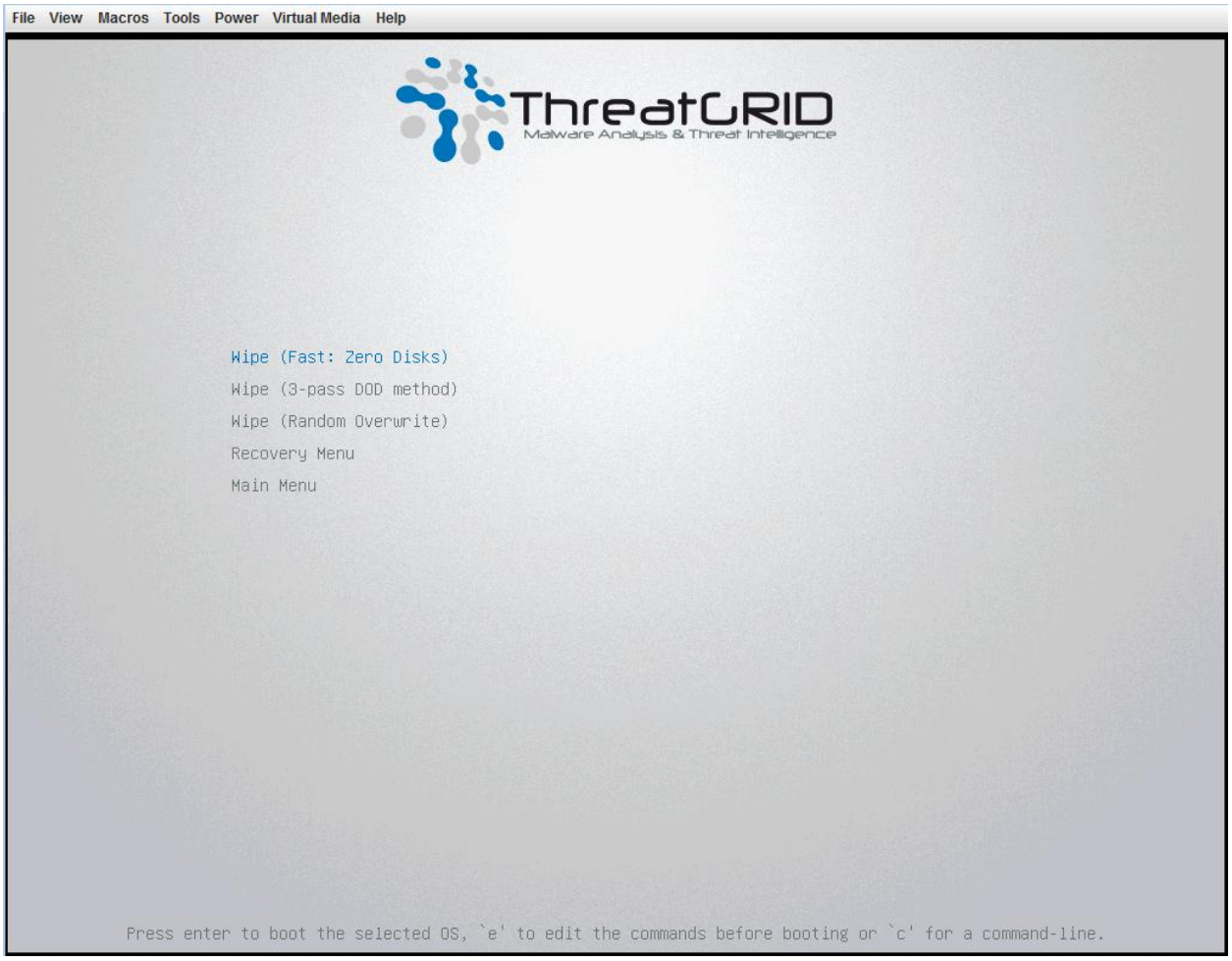

2. This option requires the following username and password:

username: "wipe"

password: "I ACCEPT ALL RESPONSIBILITY FOR THIS ACTION"

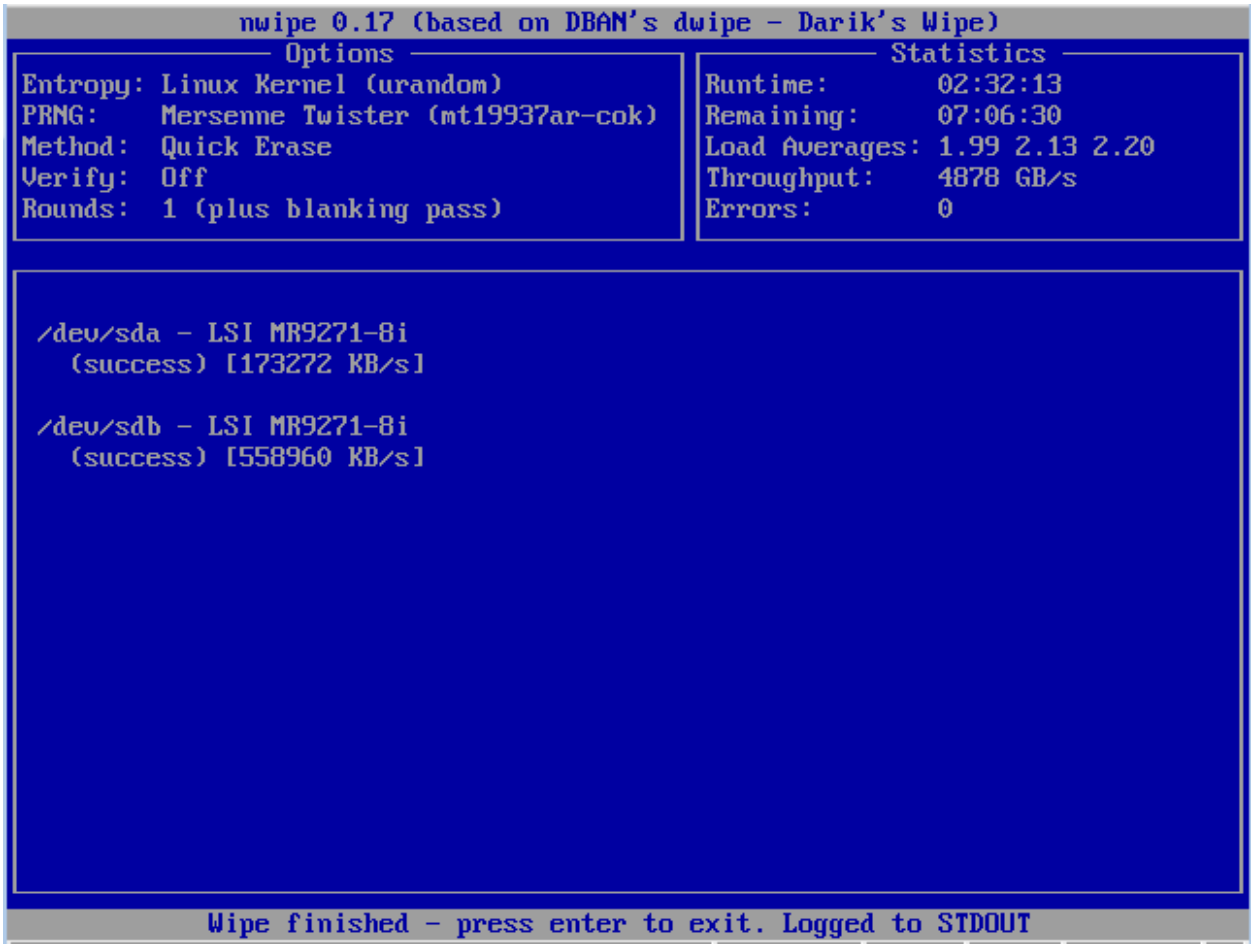
3. Next, select a Wipe option. See Wipe Options for the approximate run times of each option.

**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 |

## Wipe and Clusters

After performing a wipe operation, an appliance will no longer operate without being returned to Cisco for reimaging. Wipe should only ever be used on a cluster node after that node has been flagged in OpAdmin as permanently removed. Do not remove a node from a cluster, wipe it, and re-add it. Otherwise, if that node ever becomes master after being re-added, undesirable outcomes may result.

Use the **Remove** button in OpAdmin to inform the system that the node is not just inactive but removed.

# 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`
  Note: These parameters do not need to be entered manually, and manually entering any parameters that conflict with them is explicitly unsupported and may result in undefined behavior.
- 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.

**Elastisearch** - 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.

For customers who wish to retain historical data for longer periods, making use of a NFS server with filesystem- or block-layer snapshot support is strongly recommended.

# 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 (**Configuration > NFS**), as described in the Threat Grid Appliance Setup and Configuration Guide.

**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.

## 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 that is 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. However, 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.

**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:

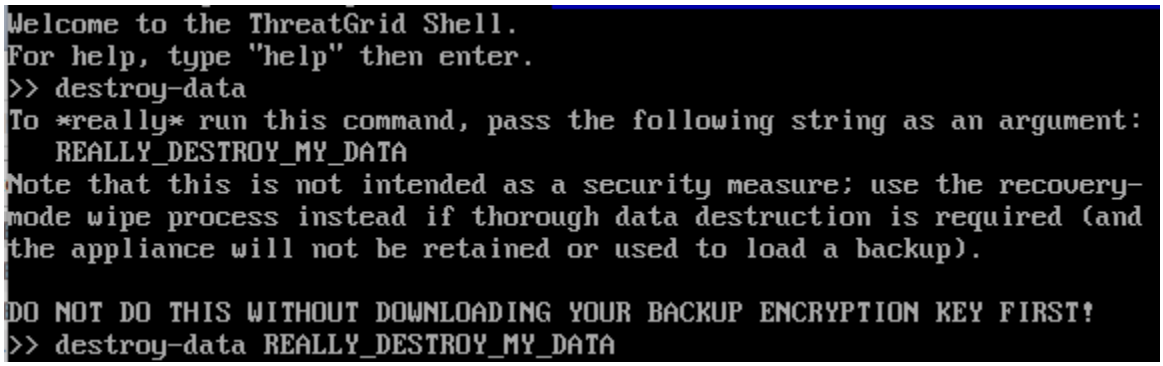
a) Access the `tgsh-dialog` configuration interface, either via the appliance's TTY or via SSH.

b) Select the `CONSOLE` option to enter tgsh. (Note that entering tgsh via recovery mode is not suitable for this use case.)

c) 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:

**Figure 21 - The destroy-data REALLY_DESTROY_MY_DATA command and argument**




The following data is destroyed:

- 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
- NFS configuration and credentials.
- The local copy of the encryption key used for NFS.

**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.

# CLUSTERING

The ability to cluster multiple Threat Grid appliances was introduced in v2.4.0 for early field trials, and became a generally available feature with v2.4.2.

Each appliance in a cluster saves data in the shared file system, and will therefore have the same data as the other nodes in the cluster.

## Goal

The main goal of clustering is to increase the capacity of a single system by joining several appliances together into a cluster consisting of 2 - 7 nodes).

The other goal is to support recovery from failure of one or more machines in the cluster, depending on cluster size.

> **Questions? Contact Customer Support:** If you have any questions, we ask that you please contact customer support for active involvement when installing or reconfiguring clusters to avoid ***mistakes that could destroy your data***.

## Features

- **Shared Data:** Every appliance in a cluster can be used as if they were standalone; each is accessing and presenting the same data.
- **Sample Submissions Processing:** Submitted samples are processed on any one of the cluster members, with any other member able to see the analysis results.
- **Rate Limits:** The submission rate limits of each member are added up to become the cluster's limit.
- **Cluster Size:** The preferred cluster sizes are 3, 5, or 7 members; 2-, 4- and 6-node clusters are supported, but with availability characteristics similar to a degraded cluster (that is, a cluster in which one or more nodes are not operational) of the next size up.
- **Tiebreaker:** When a cluster is configured to contain an even number of nodes, the one designated as the tiebreaker gets a "second vote" in the event of an election to decide which node has the primary database.

  Each node in a cluster contains a database, but only the database on the primary node is actually used: the others just have to be able to take over if and when the primary node goes down. Having a tiebreaker can prevent the cluster from being down when exactly half the nodes have failed, but only when the tiebreaker is not among the failed nodes.

  Odd-numbered clusters won't have a tied vote. In an odd-numbered cluster, the tiebreaker role will only become relevant if a node (not the tiebreaker) is dropped from the cluster, which would then become even-numbered.

  Note: This feature is fully tested only for 2-node clusters.

## Limitations

- When building a cluster of existing standalone appliances, only the 1st node (the initial node) can retain its data. The other nodes will have to be manually reset because merging existing data into a cluster is not allowed. Remove existing data with the previously documented `destroy-data` command. (Do NOT use Wipe Appliance, which will make the appliance inoperable until it's returned to Cisco for reimaging.)

- Adding or removing nodes can result in brief outages, depending on cluster size and the role of the member nodes.
- Clustering on the M3 server is not supported. Please contact support@threatgrid.com if you have any questions.

## Requirements

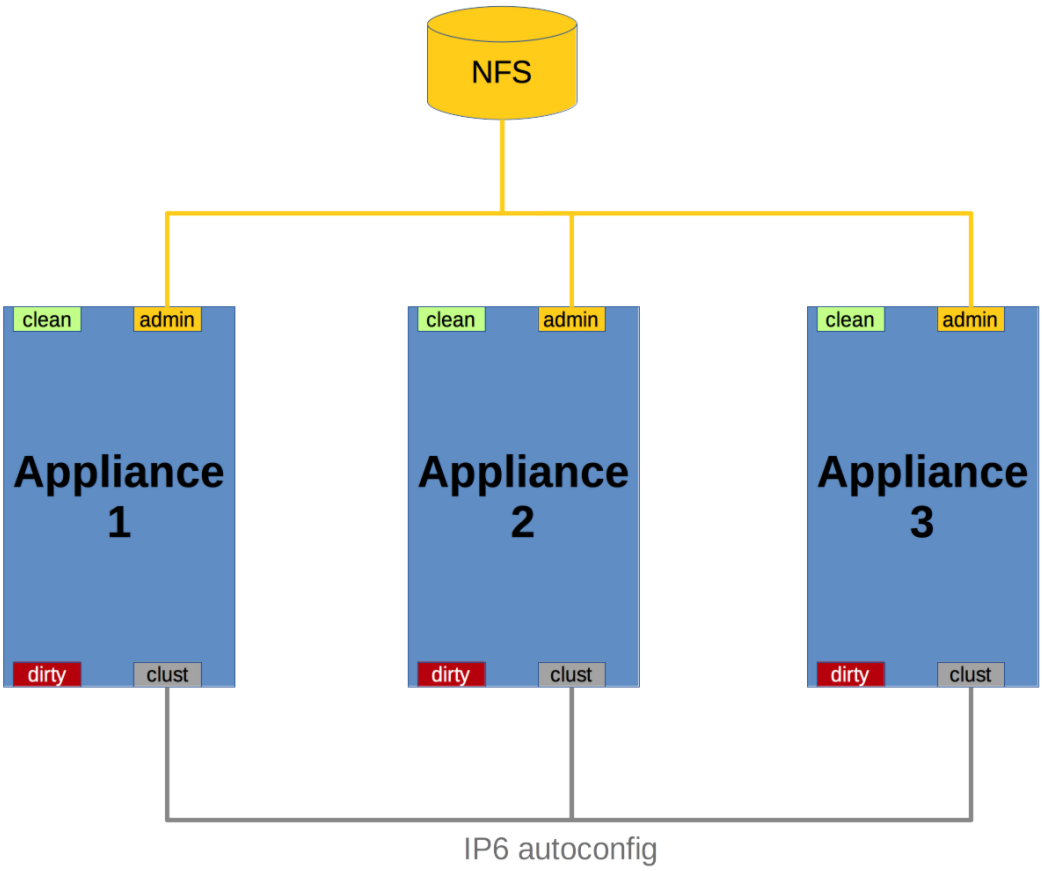
- **Version:** All appliances must be running the same version to set up a cluster in a supported configuration, and it should always be the latest version available.
- **Clust Interface:** Each Threat Grid appliance requires a direct interconnect to the other appliances in that cluster, with a SFP+ (not included with the standalone appliance) installed into the Clust interface slot on each one. "Direct" in this context means that all appliances must be on the same layer-2 network segment, with no routing required to reach other nodes, and without significant latency or jitter. Network topologies where the nodes are not on a single physical network segment are not supported.
- **Airgapped Deployments Discouraged:** Due to the increased complexity of debugging, appliance clustering is strongly discouraged in airgapped deployments or other scenarios where a customer is unable or unwilling to provide L3 support access to debug.
- **Data:** An appliance may only be joined to a cluster when it contains no data. (Only the initial node may contain data.) Moving an existing appliance into a data-free state requires the use of the database reset process that was added in appliance 2.2.4.

  DO NOT USE the destructive Wipe Appliance process that was added in 1.4.3. (Wipe Appliance will not only remove all data, it will make the appliance inoperable until it's returned to Cisco for reimaging.)
- **SSL Certificates:** If the customer is installing SSL certificates signed by a custom CA on one cluster member, then all other nodes' certificates should be signed by the same CA.

## Networking and NFS Storage

- Threat Grid appliance clusters require a NFS store to be enabled and configured: it must be available via the Admin interface, and must be accessible from all cluster nodes.
- Each cluster must be backed by a single NFS store with a single key. While that NFS store may be initialized with data from a preexisting appliance, it MUST NOT be accessed by any system which is not a member of the cluster while the cluster is in operation.
- The NFS store is a single point of failure, and the use of redundant, highly reliable equipment for that role is therefore absolutely essential.

**Figure 22 - Clustering Network Diagram**




## Building a Cluster Overview

Building a cluster in a supported manner requires that all members be on the same version, which should always be the latest available. This may mean that all of the members have to be built standalone first to get fully updated. If the appliance has been in use as standalone machines prior, only the data of the first member can be preserved. The others need to be reset as part of the build.

Start a new cluster with an initial node, and then join other appliances to it.

**There are two distinct paths that are available to starting a new cluster:**

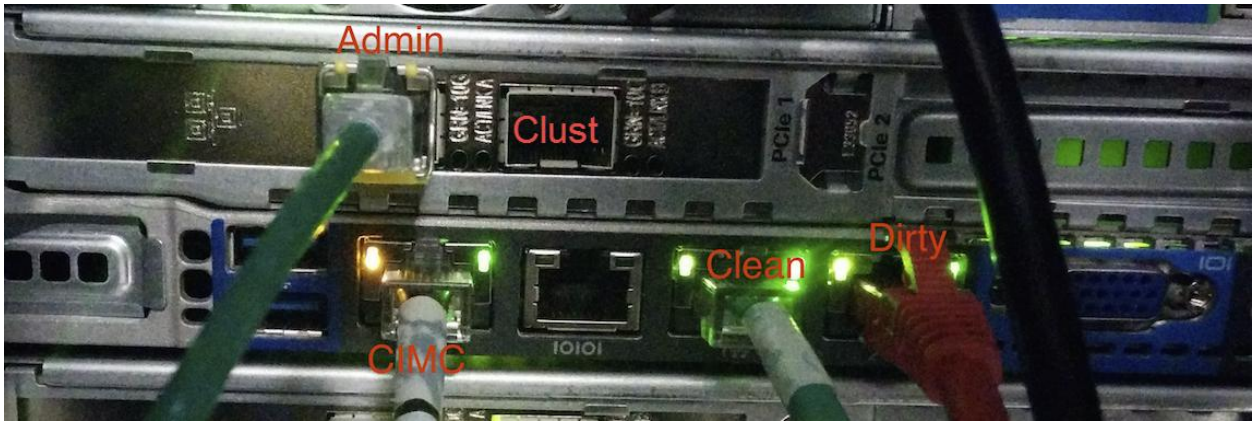
- Start a new cluster using an existing standalone appliance
- Start anew cluster using a new appliance

## Clust Interface Setup

**Required:** Each appliance in the cluster requires an additional SFP+ for the Clust interface.

Install a SFP+ module in the 4th (non-Admin) SFP port that was previously labeled **Reserved**; it is now used for the **Clust** interface, as illustrated in the next two figures:

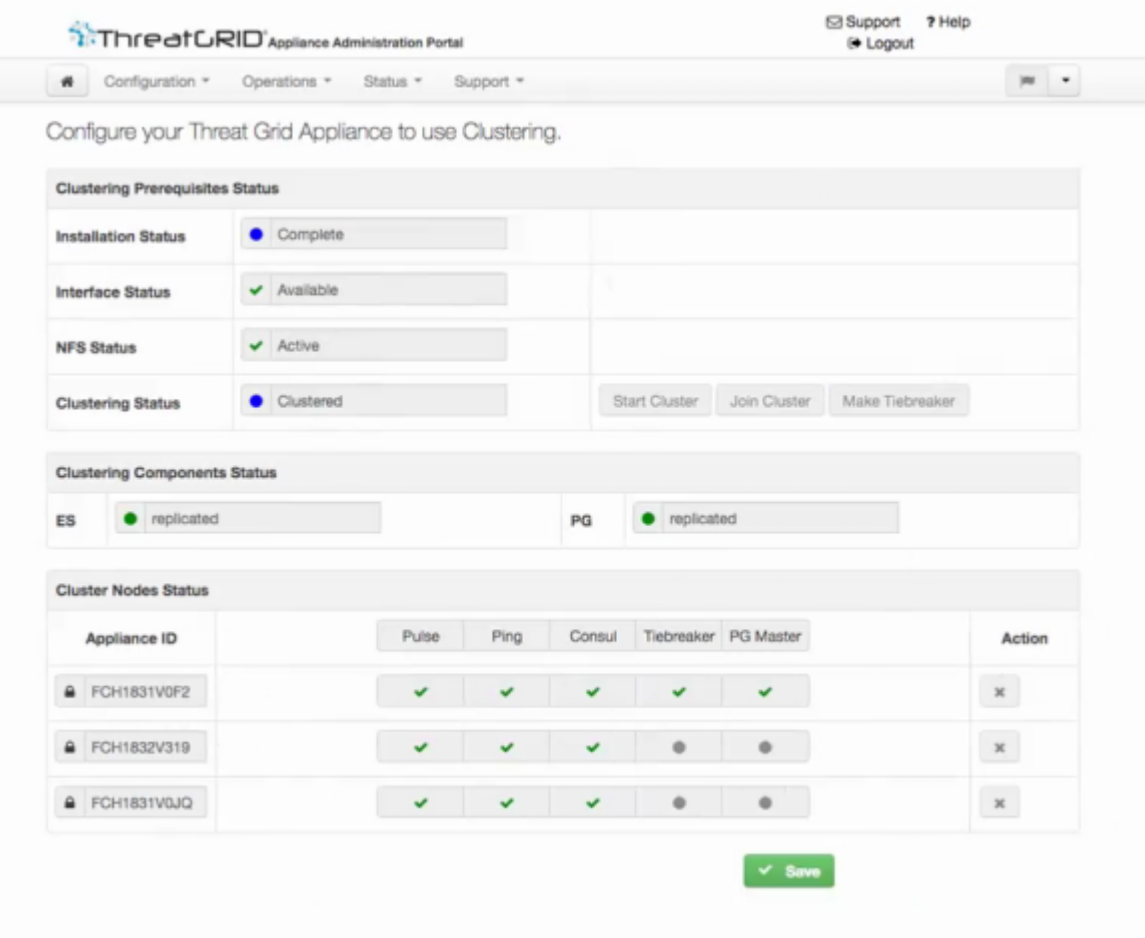
**Figure 23 - Clust Interface Setup for Cisco UCS M4 C220**




## The Clustering Page

Clusters are configured and managed on the OpAdmin *Clustering* configuration page **(Configuration > Clustering)**. The figure below shows a 3-node, active, healthy cluster.

**Figure 24 - The Clustering Page of an Active Cluster**




## Clustering Prerequisites Status

**Installation Status** The installation status of the appliance; must be **Complete.** The appliance must fully set up and configured.

**Interface Status** - The status of the clustering network interface, "Clust".

**NFS Status** - NFS must be available.

**Clustering Status -** Indicates whether the appliance is a cluster node or standalone

- **Standalone (unsaved)** - The appliance is not yet configured as either explicitly part of a cluster or a standalone unit. If in the initial setup wizard and the prerequisites for clustering are met, it's possible to make the selection of whether this system will be clustered or not.
- **Standalone** - Configured as a standalone node. Cannot be configured as part of a cluster without a reset.
- **Clustered** - The appliance is clustered with one or more other appliances.

## Clustering Components Status

**ES** - Elasticsearch, the service used for queries that require search functionality.

**PG** - PostgreSQL, the service used for queries that require up-to-date, definitive data (such as account lookups).

Both services are described with one of the following status values:

- **Replicated** - Everything is working properly. Additionally, everything required to take over on failure is also in place. The appliance is able to tolerate failure and continue working. Being in a "replicated" state does not mean that a failure will have zero downtime. Rather, a failure should entail zero data loss and constrained downtime (less than a minute in normal circumstances, with the exception of any active analysis on the specific cluster node that fails).

  Maintenance operations that bring down nodes should only be performed when the cluster is in the replicated state.

  For a fully replicated cluster, recovery should be automatic and require less than a minute to complete in any normal scenario.

- **Available** - Everything is working properly and the referenced service is available for use (that is, it can service API and user requests), but it is not replicated.

- **Unavailable** - The service is known to be non-functional.

(See the *Clustering FAQ* published on the *Threat Grid Appliance product documentation page*, for more information.)

**Status Colors:**

- **Green** - Replicated
- **Yellow** - Available
- **Red** - Unavailable
- **Grey** - Unknown

## Cluster Nodes Status

**Pulse** - Indicates whether the node is actively connected to and using the NFS store (not during initial setup, but while running services).

**Ping** - Describes whether the cluster node can be seen over the "Clust" interface

**Consul** - Indicates whether the node is participating in the consensus store. This requires both a network connection over "Clust" and a compatible encryption key.

A green checkmark indicates running and healthy.

A red "X" generally means that something is either not running yet or it's not healthy.

**Tiebreaker** - Designates the node as the "tiebreaker", which will cast the deciding vote in an election to decide the cluster's primary node.

**Keep Standalone** - Indicates that the appliance should not be configured as a node in a cluster. Selecting this option allows the user to complete the rest of the OpAdmin configuration Wizard process for a non-clustered appliance.

# Starting a Cluster with an Existing Standalone Appliance

This method of starting a cluster allows you to preserve existing data from one machine and use it to start a new cluster. This requires an existing backup to be present on NFS from which a cluster is started.

**Note**: All other nodes to be joined to the cluster will need to have their data removed before joining, i.e. the data from additional nodes cannot be merged into the cluster.

**Note:** In releases prior to v2.4.3.3, standalone appliances with data backed up to NFS no longer require a database reset and restore-from-backup to become the initial node of a new cluster. We suggest that customers upgrade to v2.4.3.3 or later and then perform a reset operation prior to initializing a new cluster (should they receive an appliance with a prior release).

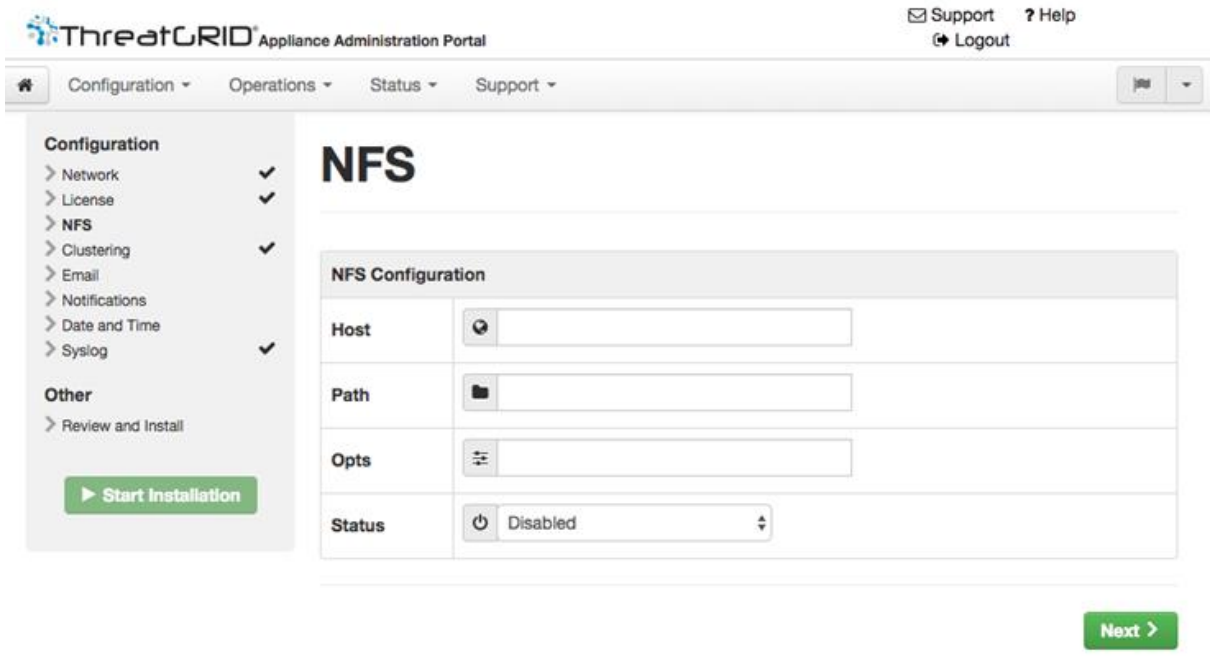
**Detailed steps for the 1st node:**

1. Fully update the appliance to the latest version. Depending on which version is currently running, this may require more than one update cycle to reach the latest.
2. If not already done, set up backup of the machine to NFS as detailed in this step.

   **Note:** This section describes the default Linux NFS server implementation, which you may need to adjust depending on your own server setup.

   Complete the *NFS* configuration page of the setup wizard in OpAdmin (**Confi*gur*ation > NFS**):

**Figure 25 - NFS Configuration page**




2.1 Configure the NFS **Host** and **Path**, select **Enabled (Pending Key)** from the Status dropdown.

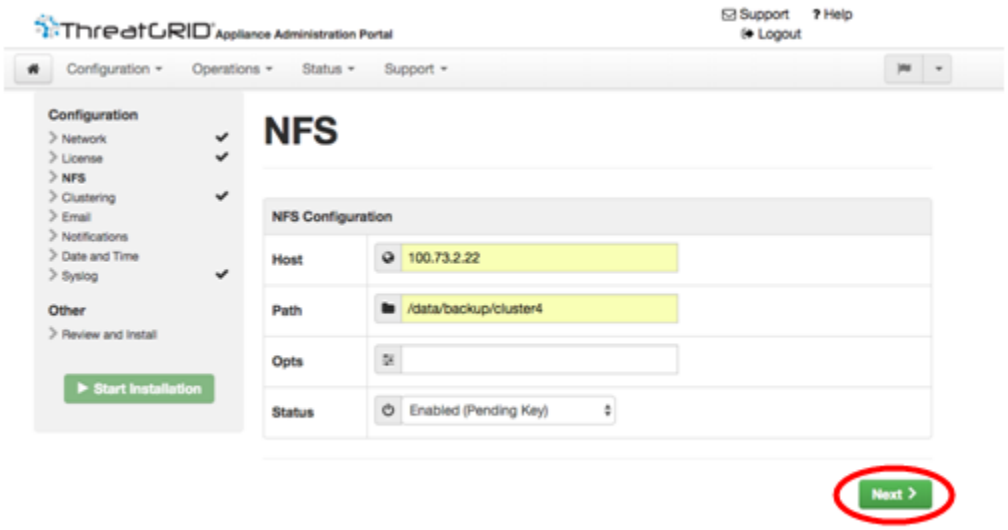
**Host** - The NFSv4 host server . We recommend using the IP address.

**Path** - The absolute path to the location on the NFS host server under which files will be stored. This does not include the Key ID suffix, which will be added automatically.

**Opts** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

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

**Figure 26 - NFS Configuration Enabled (Pending Key)**



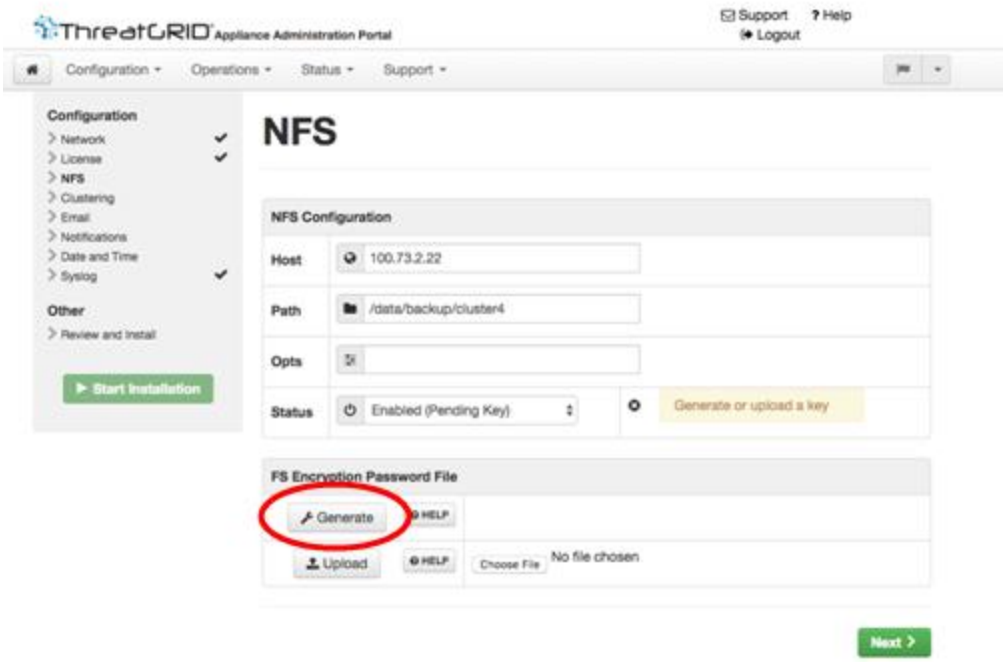

2.2 Click **Next**. The page refreshes. The **Generate** button becomes available:

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** once again.)

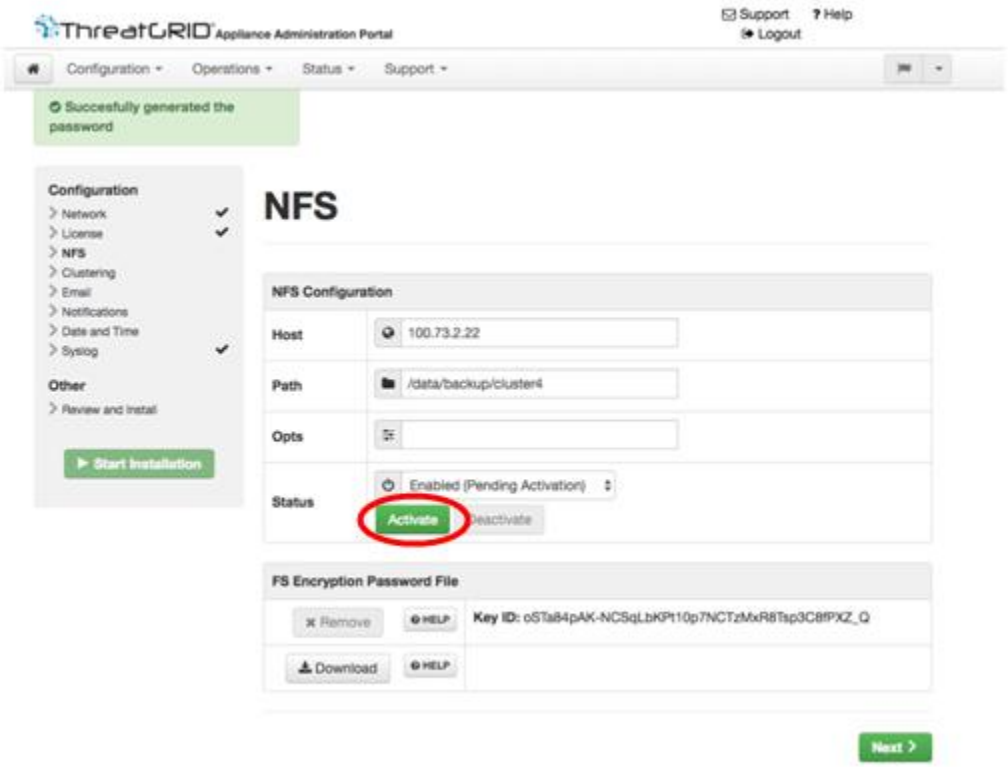
**Note:** If the key correctly matches the one used to create a backup, the Key ID displayed in OpAdmin after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key. The configuration process includes the process of mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

**Figure 27 - Generate a New NFS Encryption Key**



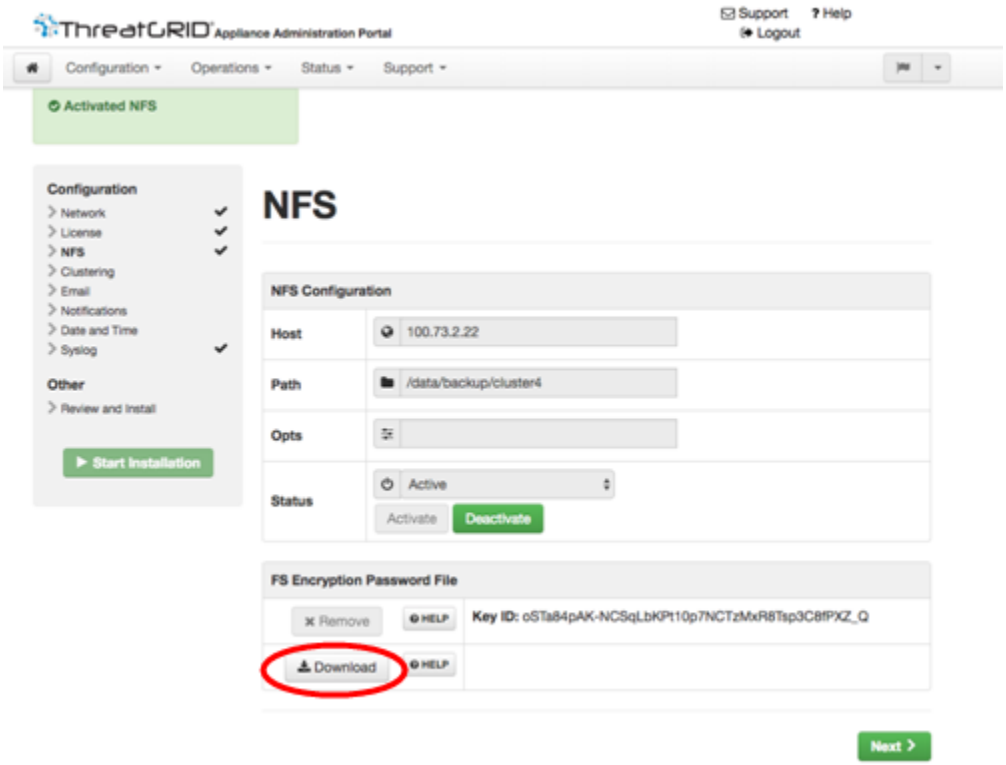

2.3 Click **Generate** to generate a new NFS encryption key. Click **Next.** The page refreshes. The Key ID is displayed, **Activate** and **Download** become available:

**Figure 28 - Activate the NFS Configuration**




2.4 Click **Activate**. This will take a few seconds (the status indicator is located in the lower left corner).The Status becomes **Active**:

**Figure 29 - NFS Active**




2.5 Click **Download** to download the backup encryption key. Save the generated file in a secure location. You will need the key for joining additional nodes to the cluster.

**IMPORTANT: **If this step is missed, all data will be lost in the following steps.****

3. Finish the configuration as needed, and Reboot the appliance to apply the NFS backup configuration.

4. Backup.

   If you do the backup at least 48 hours in advance as recommended, and there are no service notices indicating problems with the backup, then the following manual steps are unnecessary.

   Backup and other service notices are available in the Threat Grid portal UI, from the icon in the upper-right corner. If you see a service notice that "There is no PostgreSQL backup yet", then DO NOT PROCEED.

   If you do the backup immediately after reboot, then you will need to manually initiate a backup of all data to NFS to ensure it's complete. Performing the manual backup commands is only necessary if you are setting up backup immediately before rebuilding the standalone box into a cluster.

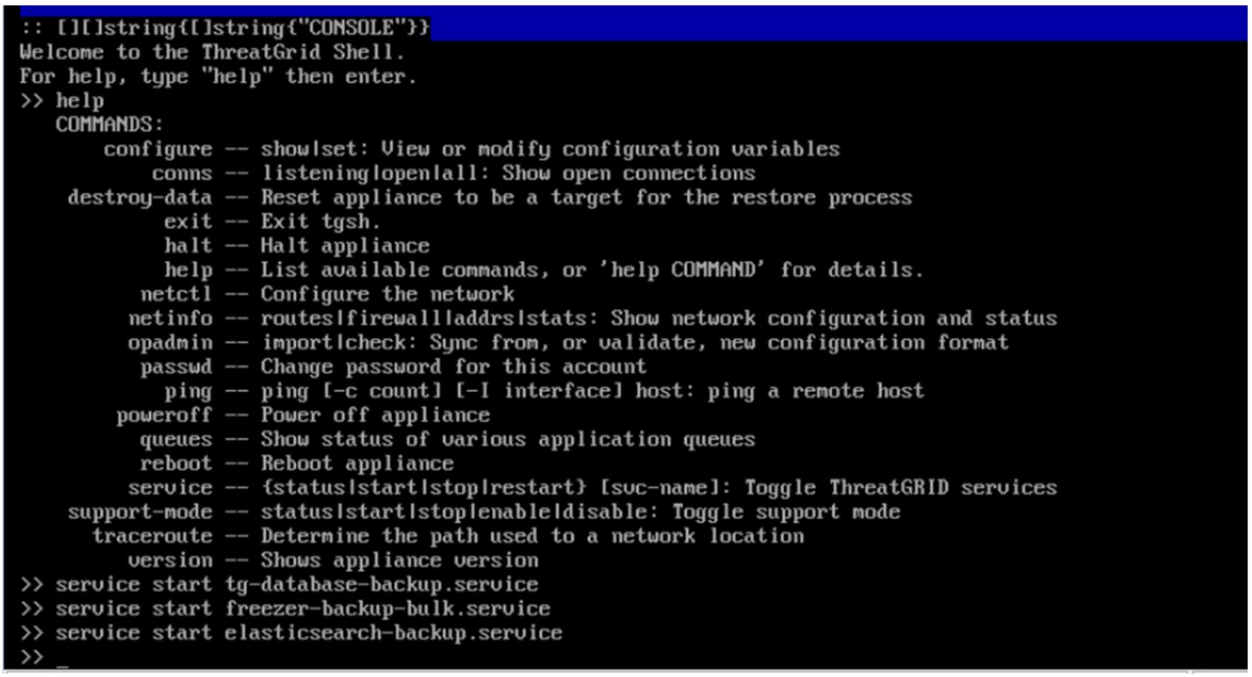
   This is done in tgsh by entering the following commands:

   ```
   service start tg-database-backup.service
   ```

   ```
   service start freezer-backup-bulk.service
   ```

```
service start elasticsearch-backup.service
```

**Figure 30 - Initiating a Backup of All Data to NFS**



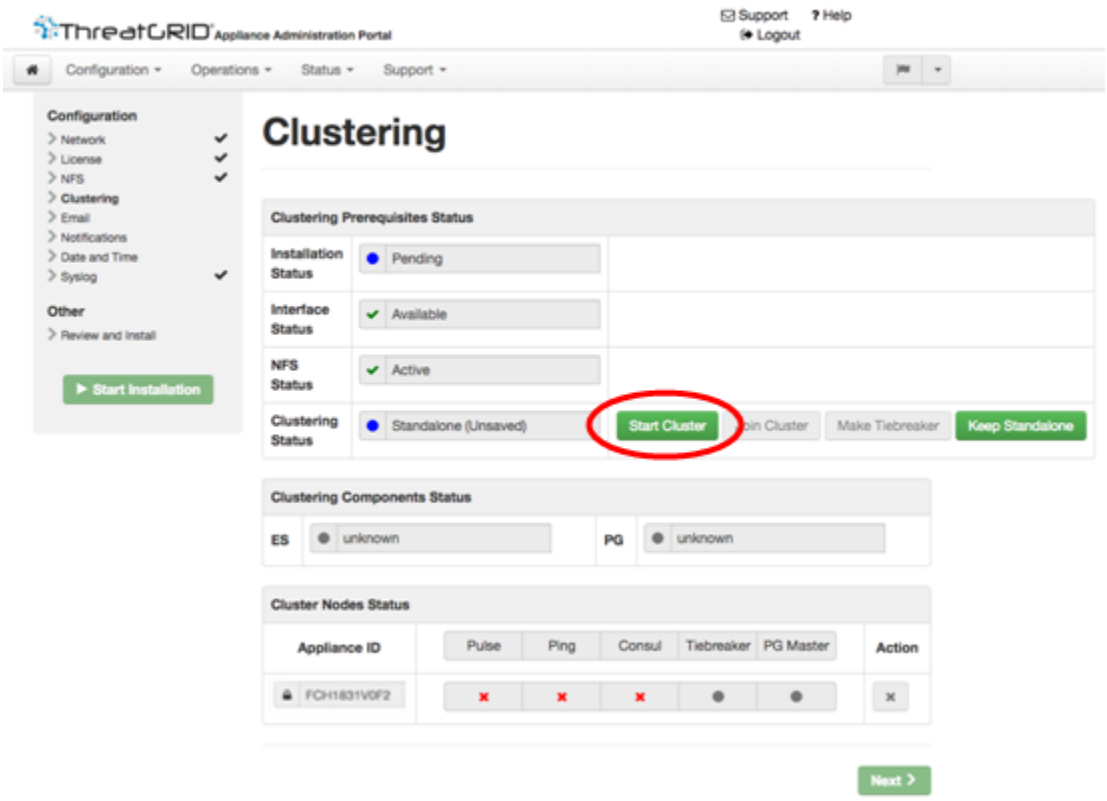

Wait for about 5 minutes after the last command returns.

5. Next, check for service notices in the appliance UI. If any notices indicate a backup process failure, such as a warning that there is no PostgreSQL backup yet, then DO NOT PROCEED.

****Do not continue unless these processes have completed successfully.****

6. Navigate to the *Clustering* page **(Configuration > Clustering**):

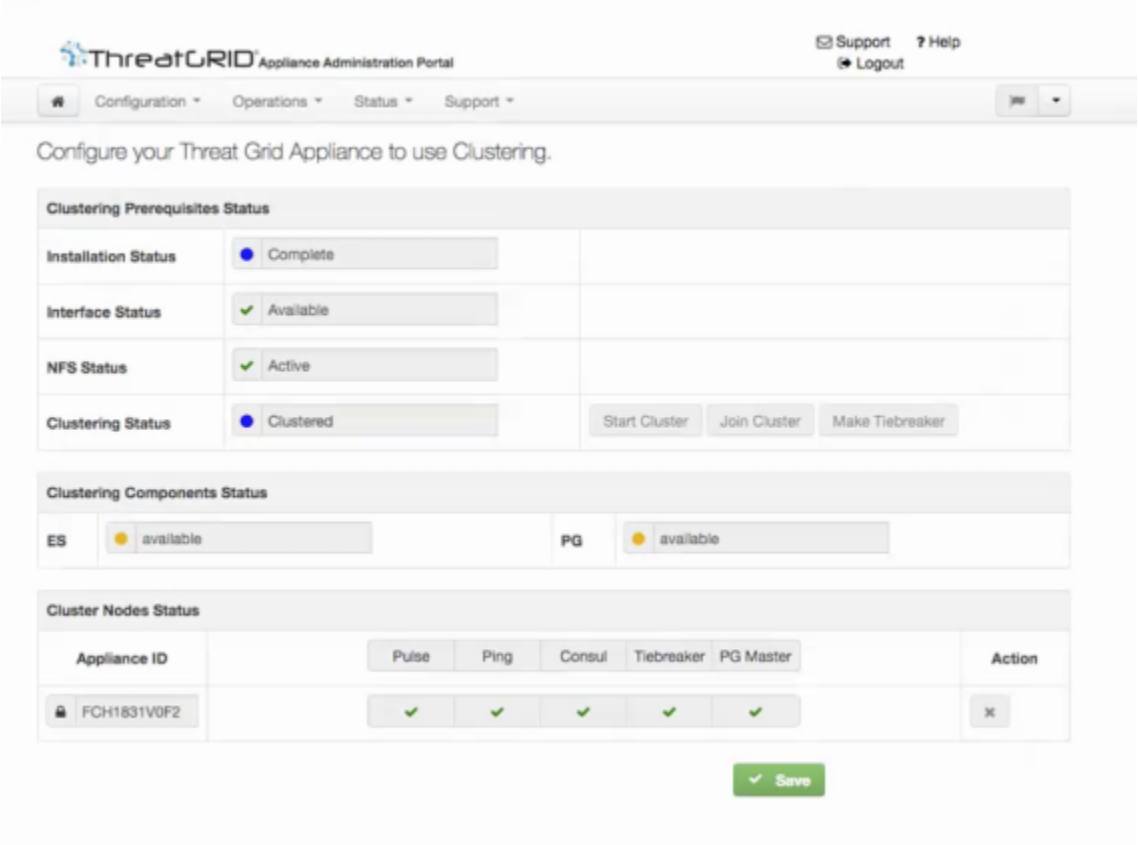
**Figure 31 - Start Cluster**




7. Click **Start Cluster**, and click OK in the confirmation popup The Clustering Status changes to **Clustered**.

Once the data restore is complete, return to the *Clustering* configuration page to check the health of the new cluster:

**Figure 32 - Clustering Status: Clustered**




8. Finish the installation. This will initiate a restore of the data in cluster mode.

Now you can begin joining other appliances to the new cluster, as described in the section, Joining Appliances to a Cluster on p. 81.

## Starting a Cluster with a New Appliance

This method of starting a cluster can be used for new appliances that are shipped with cluster-capable versions of the appliance software, or for existing appliances which have had their data reset.

**IMPORTANT NOTE:** We have just discovered an issue with the way database creation is handled when creating a new cluster from scratch. To minimize the number of customers that are affected by this, we encourage you to create a standalone appliance first and extend it into a cluster as described in the previous section, rather than following the procedure below. Please contact support@threatgrid.com if you have any questions.
-- The Threat Grid Appliance team, May 29, 2018

**Note:** Remove existing data with the previously documented `destroy-data` command. (Do NOT use Wipe Appliance.)

1. Set up and begin the OpAdmin configuration as normal.
2. Browse to the OpAdmin configuration Wizard's *NFS* page **(Configuration > NFS)**.

   **Note:** See the figures in the section Starting a Cluster with an Existing Standalone Appliance above.
3. Configure the Network and License.
4. In the **NFS** page, configure the NFS **Host** and **Path**, set **Status** to Enabled,

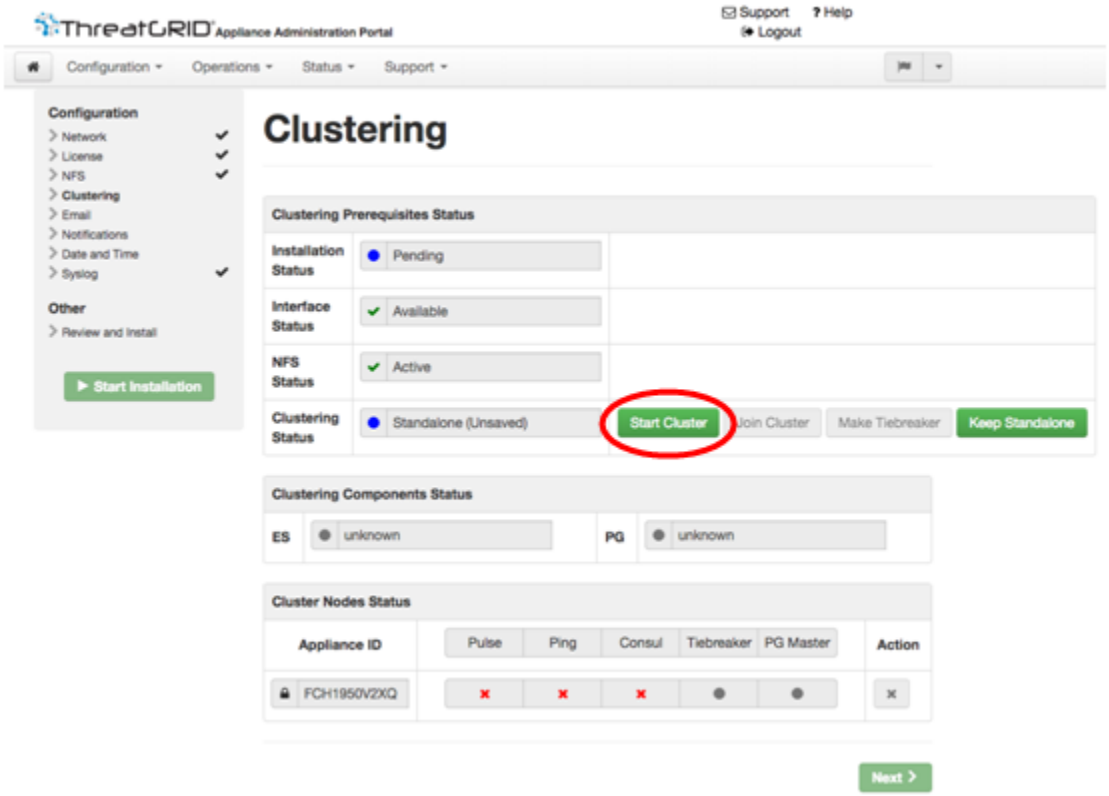
   **Host** - The NFSv4 host server . We recommend using the IP address.

   **Path** - The absolute path to the location on the NFS host server under which files will be stored. This does not include the Key ID suffix, which will be added automatically.

   **Opts** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.

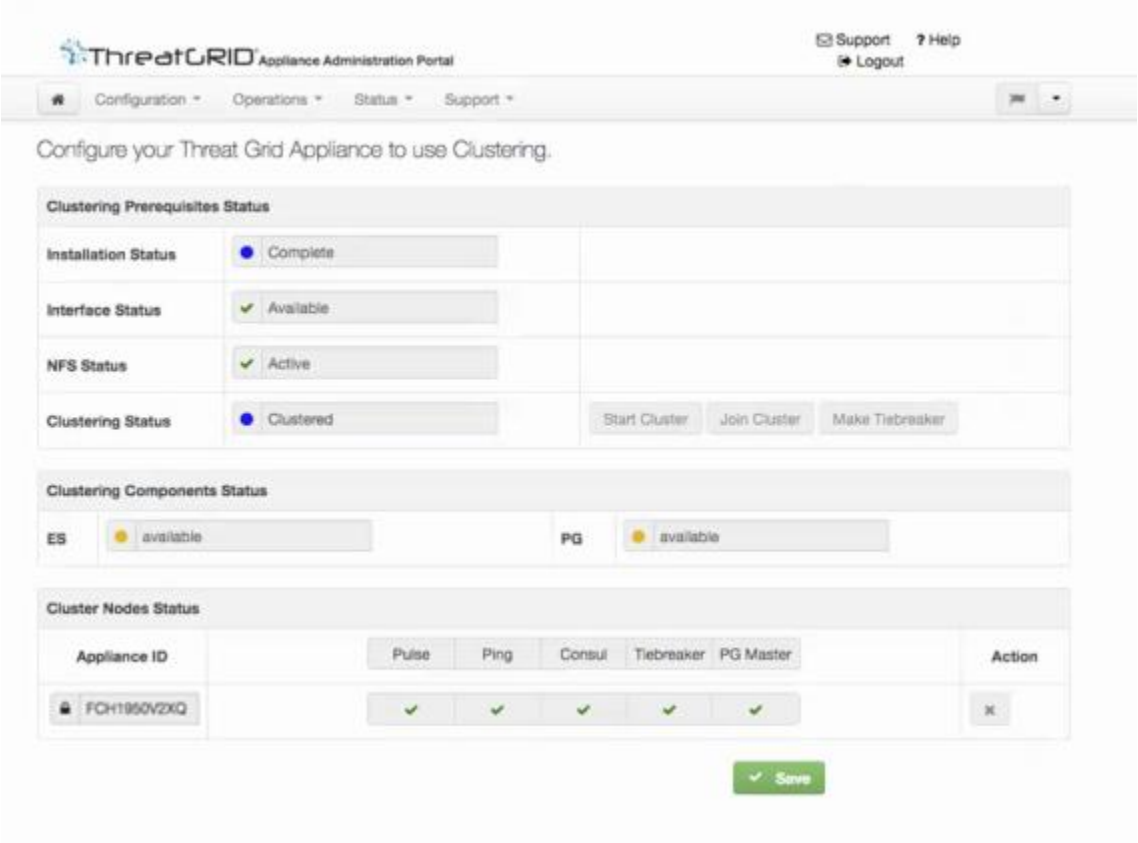
   **Status** - Select **Enabled (Pending Key)** from the dropdown.
5. Click **Next**. The page refreshes. The **Generate** and **Activate** buttons become available.
6. Click **Generate** to generate a new NFS encryption key.
7. Click **Activate**. The **Status** changes to **Active**.
8. Click **Download** to download a copy of the encryption key for safekeeping. You will need the key for joining additional nodes to the cluster.

**Figure 33 - Clustering Configuration Page**




9. Browse to the *Clustering* configuration page **(Configuration > Clustering)**:
10. Click **Start Cluster** and click **OK** in the confirmation popup. The Clustering Status changes to **Clustered**.
11. Complete the rest of Wizard and click **Start Installation**. This will initiate a restore of the data in cluster mode.
12. Open the *Cluster* configuration page to check the health of the new cluster:

**Figure 34 - Clustering Status: Clustered**




Now you may join new or existing appliance nodes to the cluster, as described in the next section, **Error! Reference source not found.**.

# Joining Appliances to a Cluster

This section describes how to join new and existing appliances to a cluster.

**Note:** An appliance may be joined to an existing cluster *only when it contains no data*. (Unlike the initial, 1st appliance, which may contain data.)

Also, it is critically important that the joining is only attempted with a machine on the very latest version. All appliances in a cluster must be running the same version. This may require setting up the appliance first, then update it, reset the data, and join it to the cluster.

Add one node at a time, and wait for Elasticsearch ("ES") and PostGres ("PG") to reach the state of "Replicated" before proceeding to the next node. "Replicated" is expected in clusters of 2 or more nodes. The wait for the state change for ES and PG to reach "Replicated" does not apply to the single-node case. (That being said, if you are initializing a single-node cluster from a backup you should wait for the restore to be completed and the application to be working/visible in the UI before proceeding to the second node.)

When joining an appliance to a cluster, the NFS and clustering must be configured during the initial setup run.

**Joining an Existing Appliance to a Cluster:**

When joining an existing appliance to a cluster, all of its data must be removed prior to being merged into the cluster.

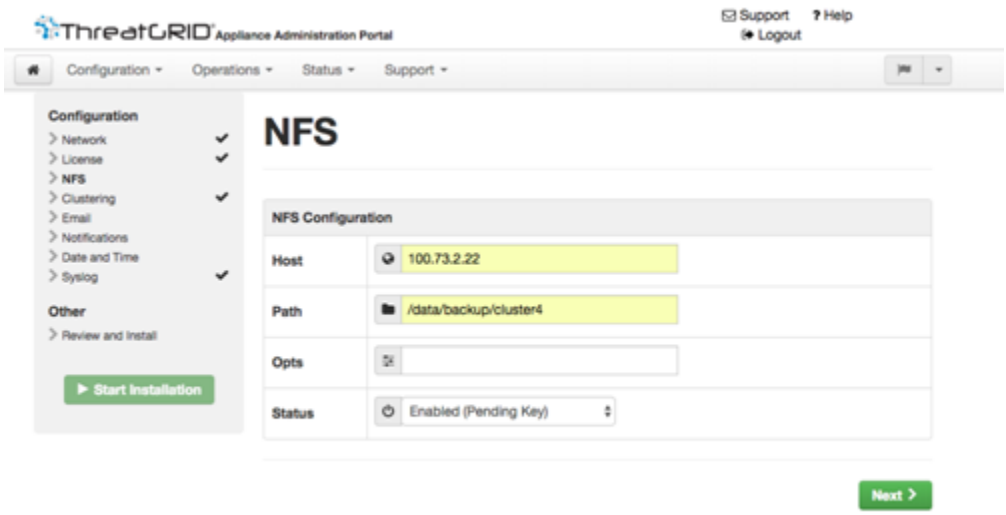
- Update the appliance to the latest version. This may require several update cycles depending on what version is running on it currently. All nodes in a cluster must be on the same version.
- Run the `destroy-data` command in `tgsh` to remove all data.

After running `destroy-data` on an existing appliance, it basically becomes a new node, and joining it to a cluster follows the same steps as joining a new appliance, as described in the next section:

**Joining a New Appliance to a Cluster:**

1. Set up and begin the OpAdmin configuration as normal.
2. Browse to the OpAdmin Wizard's NFS configuration page **(Configuration > NFS)**, and set up NFS with the same **Host** and **Path** as the 1st (initial) node in the cluster. Select the status **Enabled (Pending Key)**:

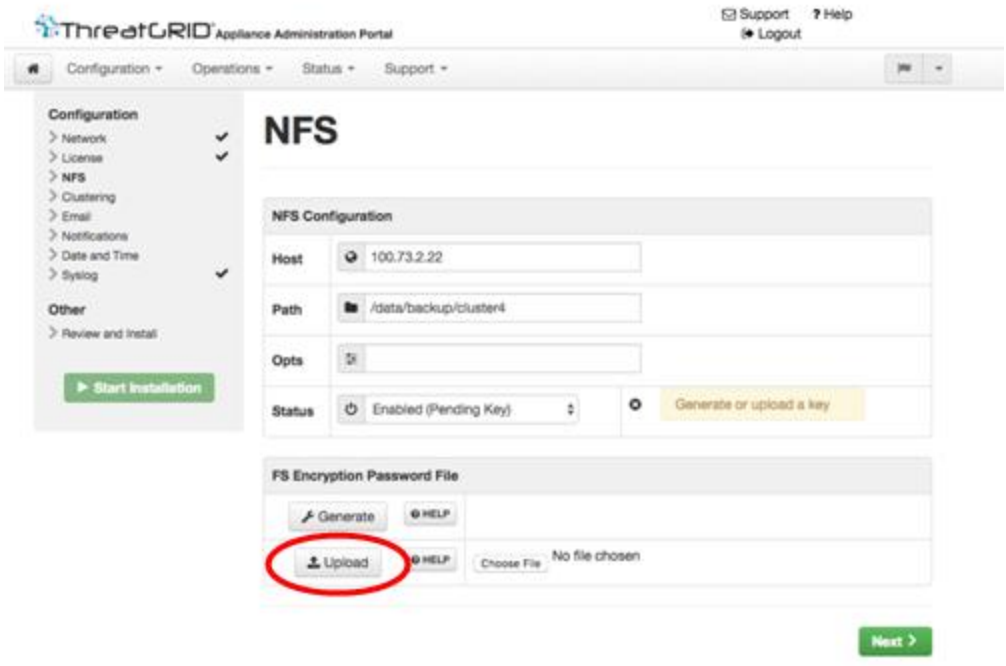
**Figure 35 - NFS for Joining a Cluster**




3. Click **Next**. The page refreshes and **Upload** becomes available:

   **NOTE:** If the key correctly matches the one used to create a backup, the Key ID displayed in OpAdmin after upload will match the name of a directory in the configured path. Backups cannot be restored without the encryption key. The configuration process includes the process of mounting the NFS store, mounting the encrypted data, and initializing the appliance's local datastores from the NFS store's contents.

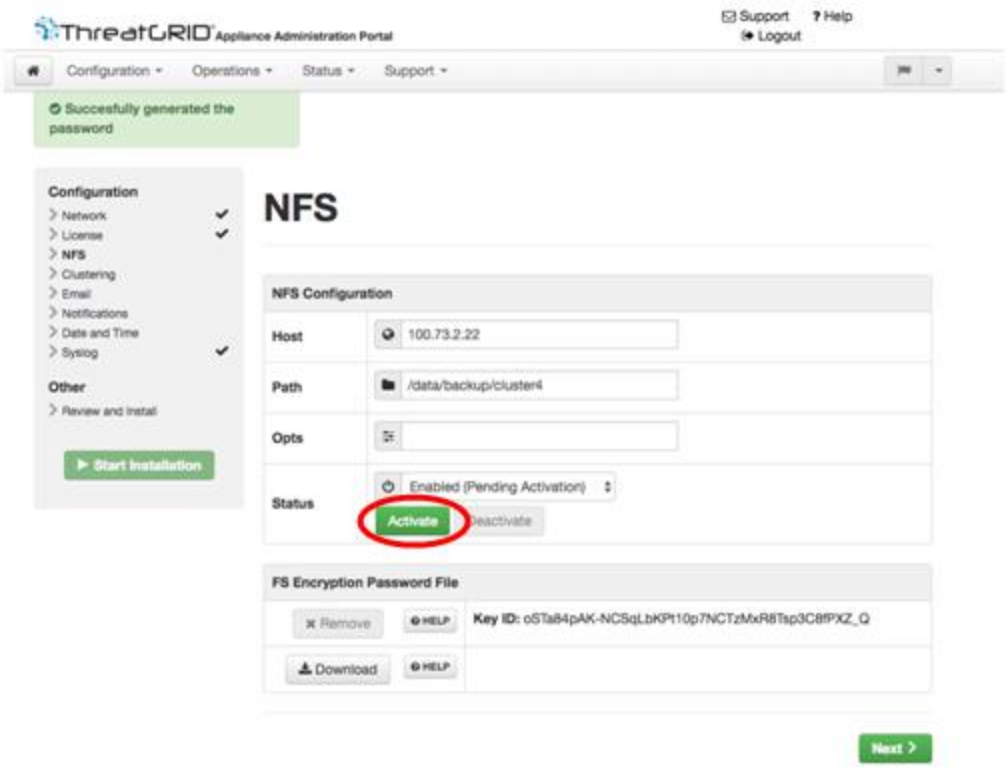
**Figure 36 - Upload the NFS Encryption Key**



4. Click **Upload**, and select the NFS encryption key you downloaded from the first node when you started the new cluster.

5. Click **Next.** The page refreshes. The Key ID is displayed, and **Activate** becomes available:

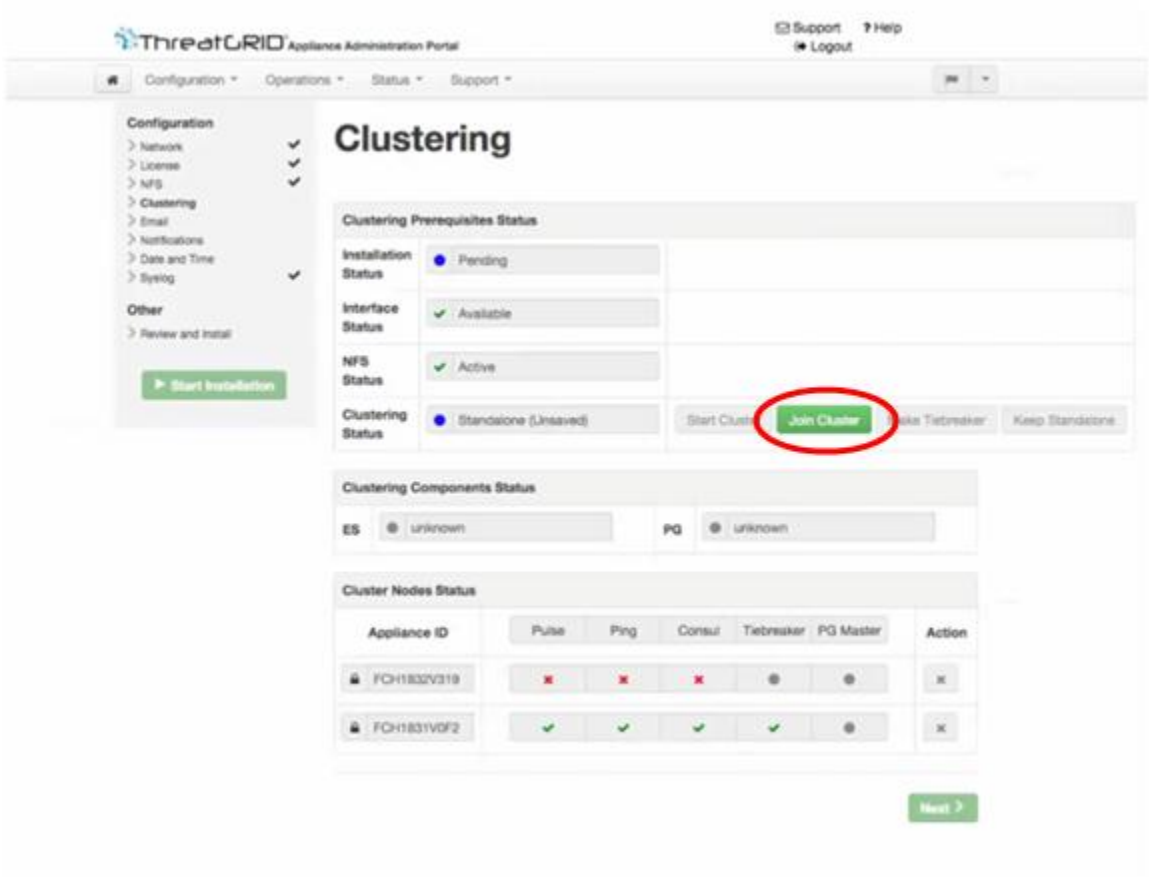
**Figure 37 - Activate the NFS Encryption Key of the Joining Appliance**




6. Click **Activate**. This will take a few seconds (the status indicator is located in the lower left corner).The Status becomes **Active**.

7. Click **Next** to continue to the Wizard's **Clustering** configuration page:

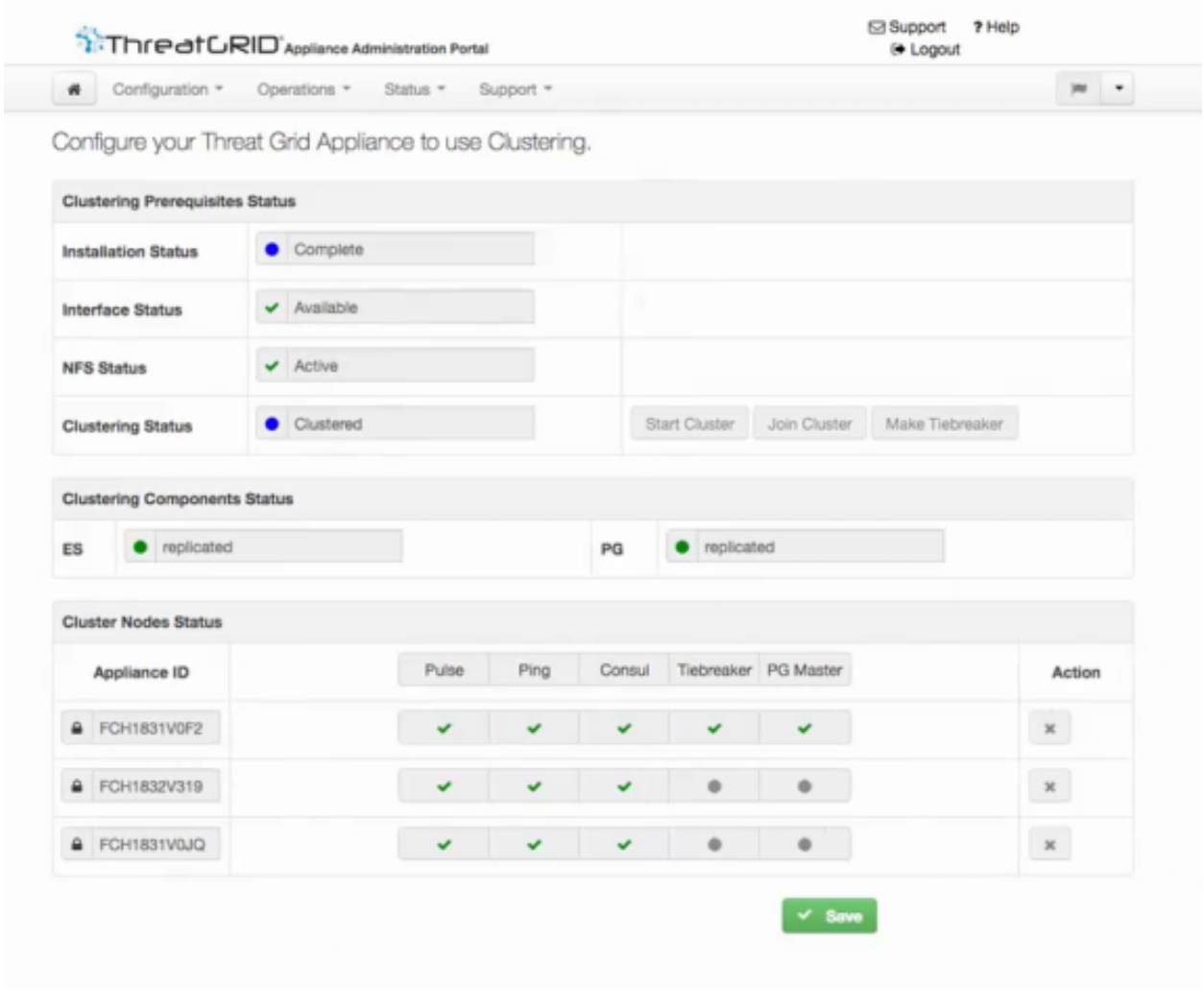
**Figure 38 - Join Cluster**




8. Click **Join Cluster**, and click **OK** in the confirmation popup. The Clustering Status changes to **Clustered**.
9. Finish the installation. This will initiate a restore of the data in cluster mode.

Repeat these steps for each node you wish to join to the cluster.

**Figure 39 - An Active, Healthy 3-Node Cluster**



## Designating a Tiebreaker Node

When a cluster is configured to contain an even number of nodes, the one designated as the tiebreaker gets a "second vote" in the event of an election to decide which node has the primary database.

Each node in a cluster contains a database, but only the database on the primary node is actually used: the others just have to be able to take over if and when the primary node goes down. Having a tiebreaker can prevent the cluster from being down when exactly half the nodes have failed, but only when the tiebreaker is not among the failed nodes.

We recommend 3-, 5-, or 7-node clusters. Having tiebreaker support is part of an ongoing effort to mitigate the loss of reliability in moving from a standalone appliance to a 2-node cluster.

When a cluster is completely healthy and the current node is not the tiebreaker, the Make Tiebreaker button is active. Clicking Make Tiebreaker will cause a brief service disruption, after which the current node will be the one which is not allowed to fail, and the other node can be shut down without breaking the cluster.In the event of a permanent failure of the tiebreaker node without being able to modify the designation ahead of time, either reset the surviving node and restore from backup, or contact support@threatgrid.com for assistance.

To designate a cluster as the tiebreaker, in the **Clustering** configuration page, click **Make Tiebreaker**.

## Removing a Cluster Node

To remove an appliance node from a cluster, use the **Remove** button on the *Clustering* configuration page.

Removing a cluster indicates that it should no longer be considered part of a cluster, rather than a node that is temporarily down. Remove an appliance when it is being decommissioned; that is, when the appliance is either replaced with different hardware, or will be rejoined to a cluster only after its data has been reset. Removing an appliance indicates to the system that you are not going to re-add a node, or if you *do* re-add it, it will have been reset.

An appliance is not marked as having been permanently removed from a cluster if it has pulse (is actively writing to NFS), or is active on consul (part of the consensus store).

On the **Clustering** configuration page, click **Remove**.

To replace a still-live node (in a cluster with less than 7 nodes): add the new node, wait for the cluster to go green, then remove the old one offline, using the **Remove** button to alert the system that it's not coming back.

When you first take the node offline, the cluster status will change to yellow. After you click Remove, the status will revert back to green (since the cluster will resize such that it no longer expects the now-removed node to be present.

## Resizing a Cluster

When a node is removed from a cluster by using the **Remove** button, the cluster will resize, which may affect the number of failures it is expected to tolerate. If a cluster is resized in such a way as to change the number of expected failure tolerances (as defined in the Failure Tolerances table in the next section), it will force an Elasticsearch restart, which will cause a brief service interruption.

**Exception:** The above does NOT include a system other than the PostgreSQL master being rebooted or having a transient failure. Disruption should be minimal in that case except for clients actively using that node, or if samples are running on it. If you add an appliance that was not part of the cluster already, or if you click **Remove**, and this changes the cluster size such that the number of tolerated failures is changed, then there will be a brief interruption as the rest of the cluster reconfigures.

## Failure Tolerances

In the event of a failure, clustered appliances will not lose any data, with the exception of any analysis being actively run by the failed node, and will recover service with a minimal (less than one minute) service disruption period and no user involvement.

Most failures will recover in less than a minute so long as the number of nodes that are available is not smaller than the number in the **Nodes Required** column; or will recover after the number of available nodes increases to meet that count; so long as the cluster was in a healthy state prior to those failures (as indicated by services listed as "Replicated" in the *Clustering* page).

The number of failures a cluster of a given size is expected to tolerate:

**Figure 40 - Failure Tolerances Table**

| Cluster Size | Failures Tolerated | Nodes Required |
|---|---|---|
| 1 | 0 | 1 |
| 2 | 1* | 1* |
| 3 | 1 | 2 |
| 4 | 1 | 3 |
| 5 | 2 | 3 |
| 6 | 2 | 4 |
| 7 | 3 | 4 |

*Non-Tiebreaker Only

These figures represent best-case scenarios. If the cluster is not showing green across the board when all nodes are up, then it may not be able to tolerate the full failure count indicated.

For example: If you have a 5-node cluster size with 2 failures tolerated and 3 nodes required, and all 5 appliances are actively processing data, the cluster will be able to reconfigure itself and continue operation without human administrative action if up to 2 failures take place.

Something else to consider: In a 5-, 6-, or 7-node cluster, the +1 in the number of failures tolerated means that the percentage of nodes that can fail is higher, which is particularly important as the number of nodes acts as a multiplier to the failure rate. (If you have two nodes, and each has a hardware fault once every 10 years, then you just changed your hardware fault rate to once every 5 years).

## Failure Recovery

Most failures with recover automatically. If not, then you will need to either contact Threat Grid support (support@threatgrid.ccom), or restore the data from backups. See Restoring Backed-Up Contents for more information.

## API/Usage Characteristics

Status of samples submitted to any node in a cluster may be queried from any other node in the cluster; there is no need to track to which individual node a submission took place.

Processing of sample submissions made to one node will be split across all nodes in the cluster; there is no need to actively load-balance from the client side.

## Operational/Administrative Characteristics

In a 2-node cluster, one of the nodes is “tiebreaker”, and acts as a single-point-of-failure. However, the other node may be removed from the cluster without ill effect (beyond transient failures during cutover). When a 2-node cluster is healthy (both nodes are fully operational), the tiebreaker designation may be modified by the user, to alter which of the nodes is a single point of failure.

Service may be temporarily disrupted during a failover event; samples which were actively running during a failover will not be automatically rerun.

Inasmuch as “capacity” is referred to in the context of clustering, this refers to throughput, not storage. A 3-node cluster prunes data to the same maximum storage levels as a single appliance. Consequently, a cluster of 3 5000-sample appliances – with a total 15,000-samples/day rate limit – will, when used at full capacity, have retention minimums 33% shorter than the 10,000-sample/day estimates provided in the **Threat Grid Appliance Data Retention Notes**, located with other appliance documentation on cisco.com.

## Sample Deletion

Support for deleting samples is available on appliances starting with the 2.5.0 release, which includes the portal updates for deleting samples: a "Delete" option is added to the **Actions** menu in the samples list, and a **Delete** button is available in the upper-right corner of the sample analysis report.

Note that it may take up to 24 hours for backup copies of deleted samples to be removed from all nodes.

Deleted samples are removed from the shared NFS store immediately; removed from the node processing the deletion request immediately, but the other nodes will lag until the nightly cron job is run. That being said, in clustered mode the NFS store is considered the primary source for samples, so even if the sample is not physically removed from other nodes, it should no longer be retrievable from any of them.

# Network Exit Configuration

Geographic location is often an important issue for malware analysis. Some types of malware behave differently depending on geographic location, while other types may target a specific area. Similar in concept to VPN, the Network Exit setting will make any outgoing network that is generated during sample analysis to appear to exit from that location.

## tg-tunnel Replacement

The "`tg-tunnel`" solution was provided for Threat Grid appliance users who need to avoid disclosing location during analysis. tg-tunnel has been replaced in version 2.4.3 by the Network Exit Localization feature. The functionality is the same, but has been replaced with a customer-controlled toggle and automatic configuration pull/installation.

Configuration files are automatically distributed, it is no longer necessary to have support staff manually install or update them.

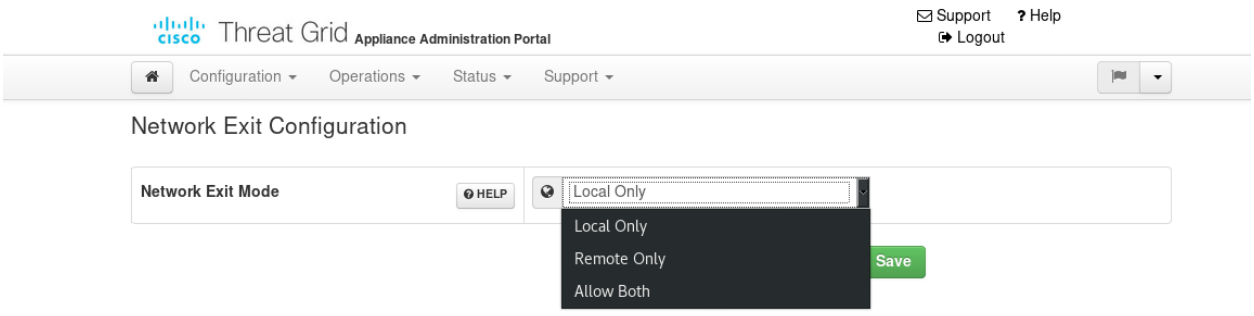
**Note:** Customers who were previously using tg-tunnel will need to permit outbound traffic to 4.14.36.142:21413 and 63.97.201.68:21413 before installing the 2.4.3 release. Otherwise, that traffic only needs to be permitted before enabling remote exit use.

Users do not get their choice of exits. It's the same functionality as you're getting with tg-tunnel today, but as a customer-controlled toggle and automatic configuration pull/installation.

The toggle is on by default for any customer who previously had a tg-tunnel config manually installed, to avoid risk of bad traffic leaking on networks where they don't want it.

Select **OpAdmin > Configuration > Network Exit**. The Network Exit Configuration page opens:

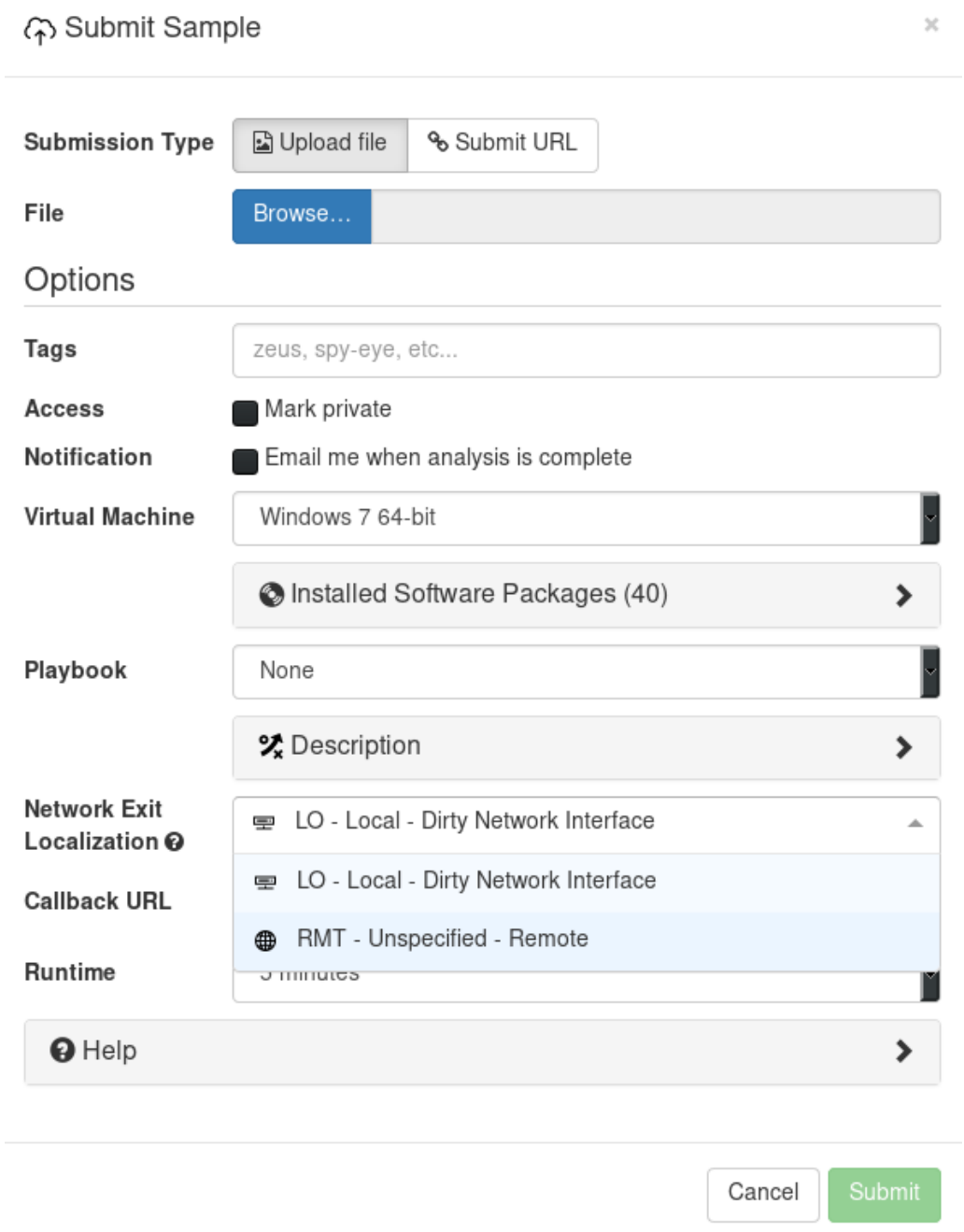
**Figure 41 - Network Exit Configuration**




The options selected and saved here will determine which Network Exit Localization options will be available in the application, such as when submitting samples in the UI. If set to **Local Only** or **Remote Only**, then the application will only make those options available to users.

Accessing private networks, even for DNS lookup, is not allowed even for Network Exit Localization. All malware traffic comes out of the Dirty interface, using the Dirty DNS server configured.

**Figure 42 - Network Exit Localization Options**

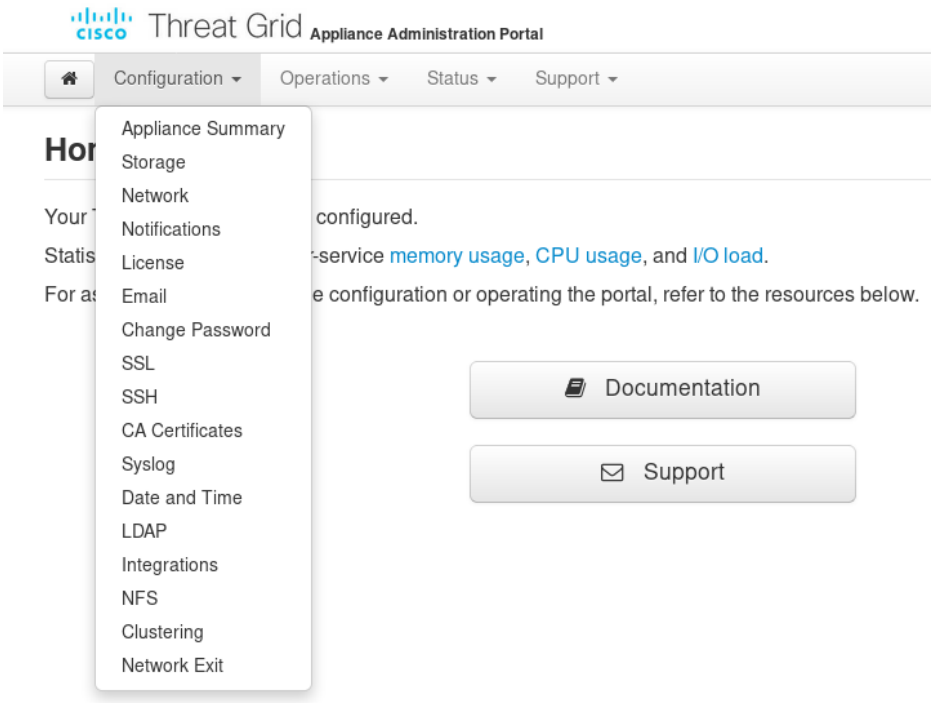


# APPENDIX - OPADMIN MENUS

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

## Configuration Menu

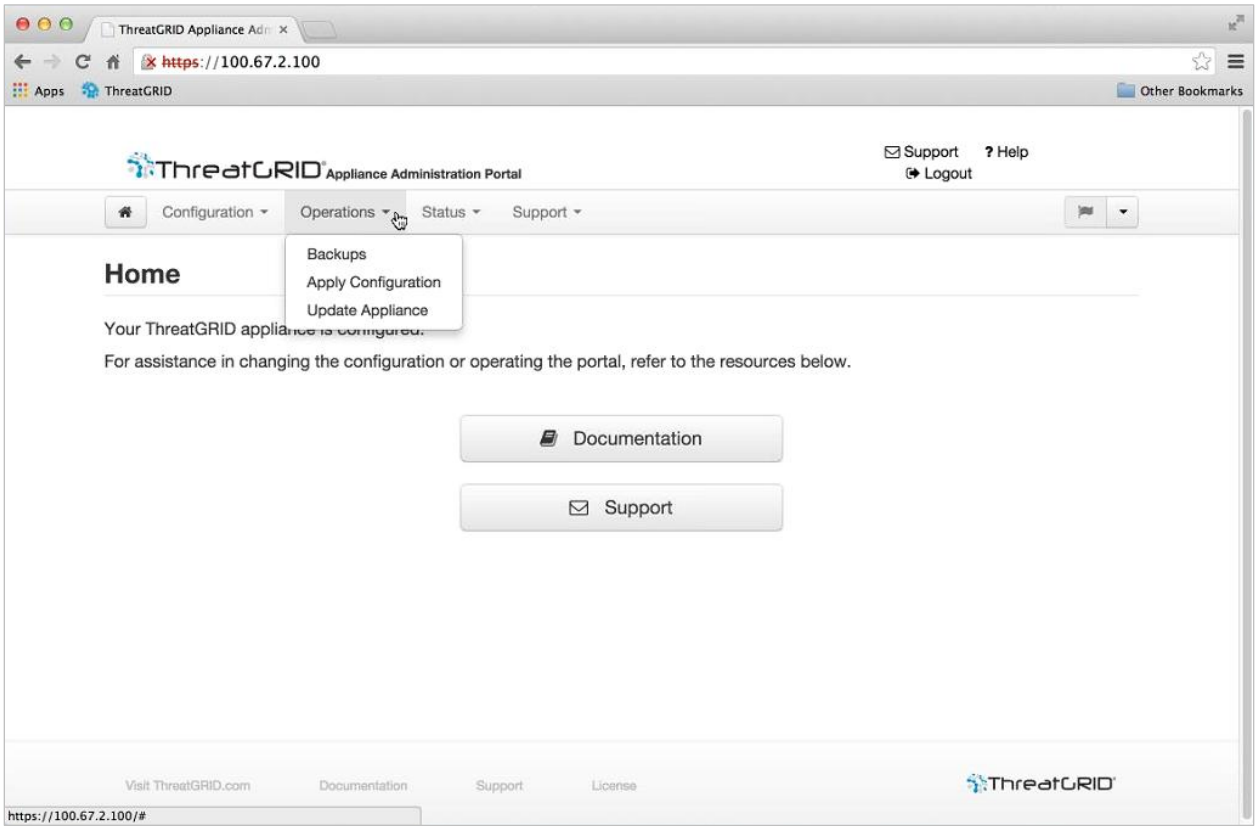
**Figure 43 - OpAdmin Configuration Menu**




**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

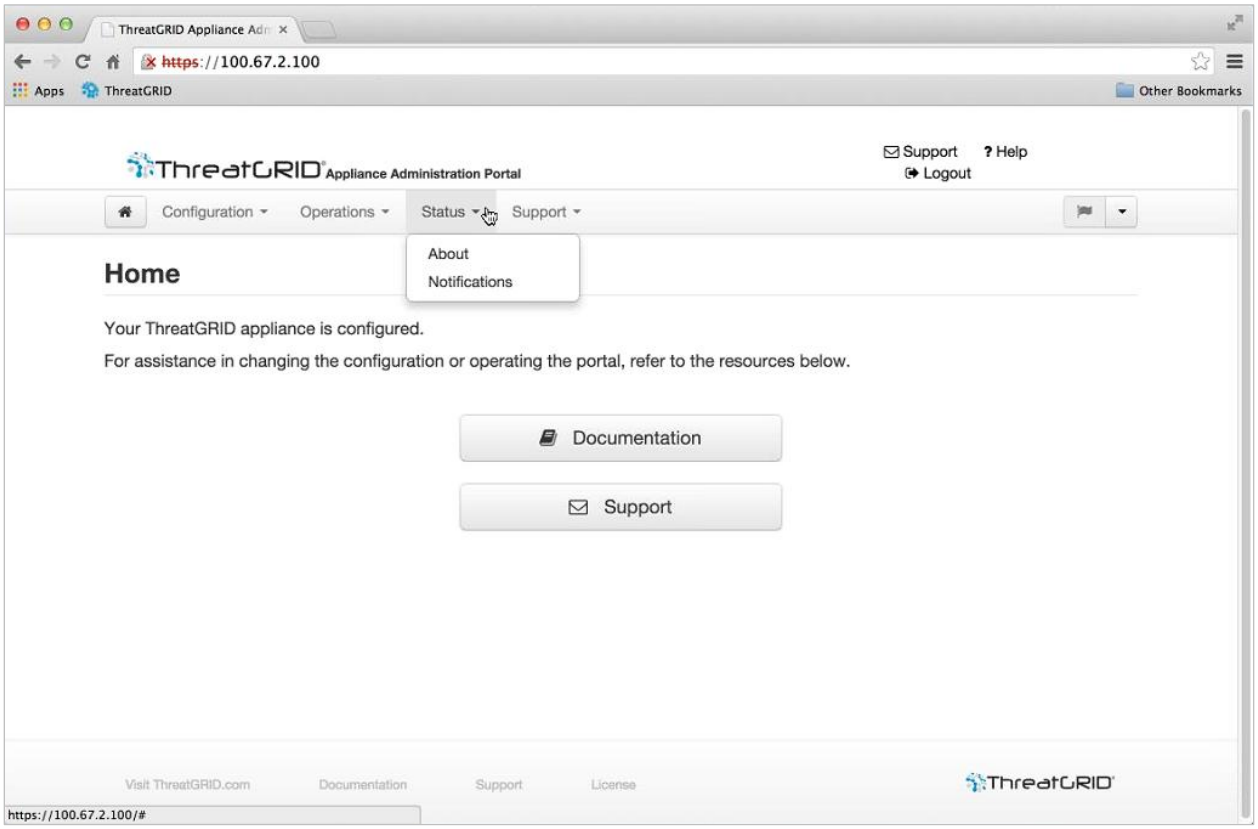
**Figure 44 - OpAdmin Operations Menu**




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

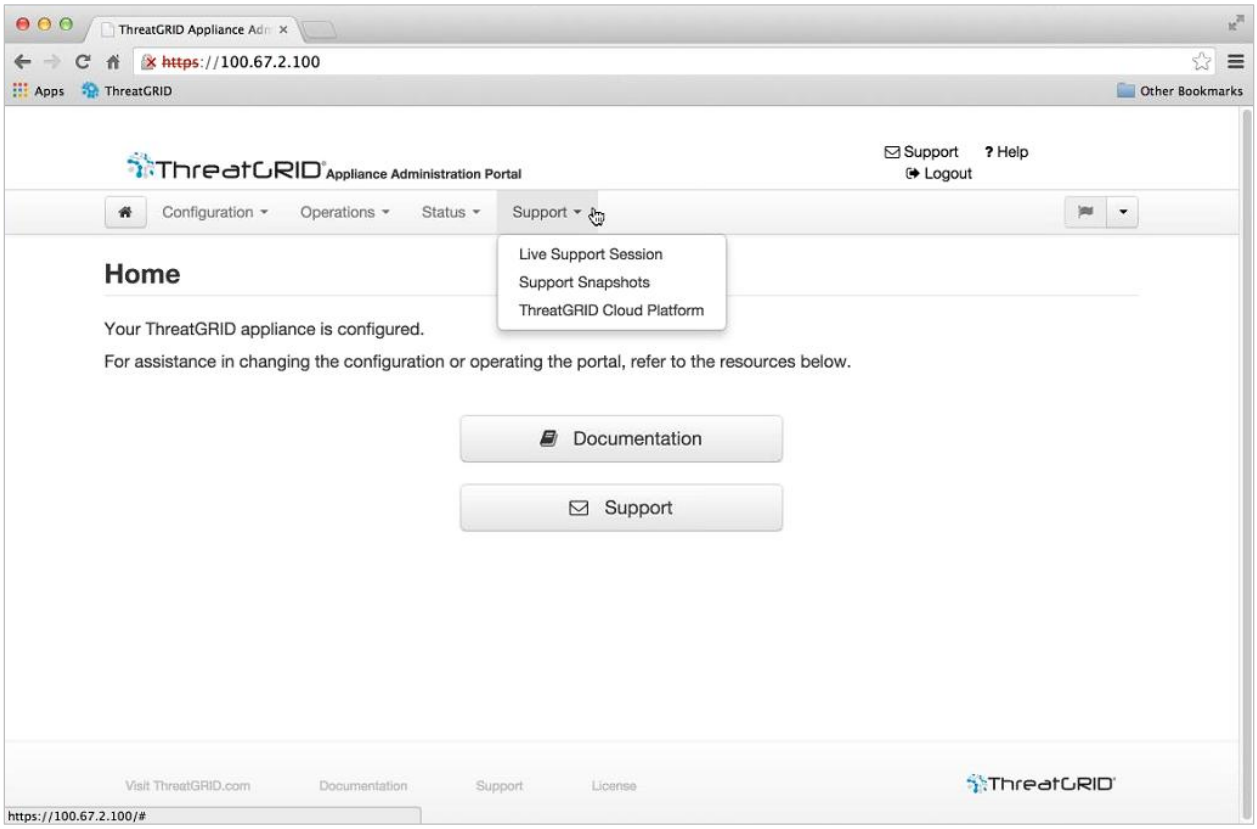
# Status Menu

**Figure 45 - OpAdmin Status Menu**



# Support Menu

**Figure 46 - OpAdmin Support Menu**




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

# INDEX

