## CONTENTS

**LIST OF FIGURES** ........................................................................................................................................ iv

**INTRODUCTION** ................................................................................................................................... 2

Who This Guide Is For ............................................................................................................................... 2

Release Notes ........................................................................................................................................ 2

What’s New ............................................................................................................................................. 2

  - *Documentation Updates for 2.4.3 - 2.4.3.3* ....................................................................................... 2
  - *Network Exit Support* ......................................................................................................................... 2
  - *Clustering* .......................................................................................................................................... 2
  - *Using IPv4LL Address Space for the Dirty Interface is Unsupported* .................................................. 2
  - *Automatic License Retrieval* .............................................................................................................. 3
  - *More Windows Changes* ...................................................................................................................... 3
  - *Backups* ........................................................................................................................................... 3
  - *Windows XP Changes* ........................................................................................................................... 3
  - *Integrating with Third Party Detection and Enrichment Services* ...................................................... 3
  - *Multiple URLs for Disposition Update Service Manager* .................................................................... 3
  - *ClamAV Signatures Automatic Daily Update* ................................................................................. 4
  - *LDAP Authentication* .......................................................................................................................... 4
  - *Cisco UCS C220 M4 Server (TG5400)* ............................................................................................... 4
  - *AMP for Endpoints Private Cloud Integration* .................................................................................... 4
  - *Version 2.0* ..................................................................................................................................... 4

Support - Contacting Threat Grid ............................................................................................................... 4

  - *Support Mode* .................................................................................................................................. 5
  - *Start Support Mode - License Workaround Prior to Version 1.4.4* .................................................... 5

Support Servers ...................................................................................................................................... 6

Support Snapshots .................................................................................................................................. 7

**PLANNING** ......................................................................................................................................... 8

User Documentation and Online Help ....................................................................................................... 8

Browsers .................................................................................................................................................. 8

Environmental Requirements .................................................................................................................... 8

Hardware Requirements ............................................................................................................................ 8
**CONTENTS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Documentation</td>
<td>9</td>
</tr>
<tr>
<td>Network Requirements</td>
<td>9</td>
</tr>
<tr>
<td>DNS Server Access</td>
<td>10</td>
</tr>
<tr>
<td>NTP Server Access</td>
<td>10</td>
</tr>
<tr>
<td>Integrations – ESA/WSA/AMP for Endpoints etc.</td>
<td>10</td>
</tr>
<tr>
<td>DHCP</td>
<td>10</td>
</tr>
<tr>
<td>License</td>
<td>10</td>
</tr>
<tr>
<td>Rate Limits</td>
<td>11</td>
</tr>
<tr>
<td>Organizations and Users</td>
<td>11</td>
</tr>
<tr>
<td>Updates</td>
<td>11</td>
</tr>
<tr>
<td>User Interfaces</td>
<td>11</td>
</tr>
<tr>
<td>TGSHE Dialog</td>
<td>11</td>
</tr>
<tr>
<td>tgsh</td>
<td>12</td>
</tr>
<tr>
<td>OpAdmin Portal</td>
<td>12</td>
</tr>
<tr>
<td>Threat Grid Portal</td>
<td>12</td>
</tr>
<tr>
<td>CIMC</td>
<td>12</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>12</td>
</tr>
<tr>
<td>Admin Interface</td>
<td>12</td>
</tr>
<tr>
<td>Clust Interface</td>
<td>12</td>
</tr>
<tr>
<td>Clean Interface</td>
<td>13</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>13</td>
</tr>
<tr>
<td>CIMC Interface</td>
<td>14</td>
</tr>
<tr>
<td>Login Names and Passwords - Defaults</td>
<td>14</td>
</tr>
<tr>
<td>Web UI Administrator</td>
<td>14</td>
</tr>
<tr>
<td>OpAdmin and Shell user</td>
<td>14</td>
</tr>
<tr>
<td>CIMC (Cisco Integrated Management Controller)</td>
<td>14</td>
</tr>
<tr>
<td>Setup and Configuration Steps Outline</td>
<td>14</td>
</tr>
<tr>
<td>Time Required for Setup and Configuration</td>
<td>15</td>
</tr>
<tr>
<td>SERVER SETUP</td>
<td>16</td>
</tr>
<tr>
<td>Network Interface Connections Setup</td>
<td>16</td>
</tr>
<tr>
<td>C220 M3 Rack Server Setup</td>
<td>16</td>
</tr>
<tr>
<td>C220 M4 Rack Server Setup</td>
<td>18</td>
</tr>
<tr>
<td>Network Interface Setup Diagram</td>
<td>20</td>
</tr>
<tr>
<td>Firewall Rules Suggestions</td>
<td>21</td>
</tr>
<tr>
<td>Dirty Interface Outbound</td>
<td>21</td>
</tr>
</tbody>
</table>
## CONTENTS

- **Dirty Interface Inbound** .......................................................... 21
- **Clean Interface Outbound** ....................................................... 21
- **Clean Interface Outbound Optional** ........................................ 22
- **Clean Interface Inbound** .......................................................... 22
- **Admin Interface Outbound Optional** ........................................ 22
- **Admin Interface Inbound** .......................................................... 23
- **Dirty Interface for Non Cisco-Validated/Recommended Deployment** .......................................................... 23
- **Power On and Boot Up** ............................................................ 24

### INITIAL NETWORK CONFIGURATION – TGSH DIALOG .................................... 26

### CONFIGURATION WIZARD - OPADMIN PORTAL ........................................ 32

- **Configuration Workflow** .......................................................... 32
- **Login to the OpAdmin Portal** ..................................................... 32
- **Admin Password Change** .......................................................... 34
- **End User License Agreement** .................................................... 35
- **Network Configuration Settings** ................................................ 35
  - **Network Configuration and DHCP** ......................................... 36
  - **License Installation** ............................................................... 36
- **NFS Configuration** ................................................................. 38
- **Email Host Configuration** .......................................................... 39
- **Server Notifications Configuration** .......................................... 41
- **Syslog Configuration** .............................................................. 41
- **NTP Server Configuration** ........................................................ 43
- **Review and Install Configuration Settings** .................................. 43

### INSTALLING THREAT GRID APPLIANCE UPDATES .................................... 47

- **Appliance Build Number** .......................................................... 47
  - **Build Number/Version Lookup Table** ...................................... 48

### TEST THE APPLIANCE SETUP - SUBMIT A SAMPLE .................................... 53

### APPLIANCE ADMINISTRATION ............................................................ 54

### APPENDIX A – CIMC CONFIGURATION (RECOMMENDED) ................................ 55

### INDEX ........................................................................ 58
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OpAdmin Start a Live Support Session</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Cisco 1000BASE-T Copper SFP (GLC-T)</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Cisco UCS C220 M3 SFF Rack Server</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>Cisco UCS C220 M3 Rear View Details</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>Cisco UCS C220 M4 SFF Rack Server</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>Cisco UCS C220 M4 Rear View Details</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>Network Interfaces Setup Diagram</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>Cisco Screen During Boot Up</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>TGSH Dialog</td>
<td>25</td>
</tr>
<tr>
<td>10</td>
<td>TGSH Dialog - Network Configuration Console</td>
<td>26</td>
</tr>
<tr>
<td>11</td>
<td>Network Configuration In-Progress (clean and dirty)</td>
<td>27</td>
</tr>
<tr>
<td>12</td>
<td>Network Configuration In-Progress (admin)</td>
<td>28</td>
</tr>
<tr>
<td>13</td>
<td>Network Configuration Confirmation</td>
<td>29</td>
</tr>
<tr>
<td>14</td>
<td>Network Configuration - List of Changes Made</td>
<td>30</td>
</tr>
<tr>
<td>15</td>
<td>IP Addresses</td>
<td>31</td>
</tr>
<tr>
<td>16</td>
<td>OpAdmin Login</td>
<td>33</td>
</tr>
<tr>
<td>17</td>
<td>OpAdmin Change Password</td>
<td>34</td>
</tr>
<tr>
<td>18</td>
<td>License Page</td>
<td>35</td>
</tr>
<tr>
<td>19</td>
<td>License Page Prior to Installation</td>
<td>36</td>
</tr>
<tr>
<td>20</td>
<td>License Information After Successful Installation</td>
<td>37</td>
</tr>
<tr>
<td>21</td>
<td>NFS Configuration</td>
<td>38</td>
</tr>
<tr>
<td>22</td>
<td>Email Host Configuration</td>
<td>40</td>
</tr>
<tr>
<td>23</td>
<td>Notifications Configuration</td>
<td>41</td>
</tr>
<tr>
<td>24</td>
<td>Appliance is Installing</td>
<td>44</td>
</tr>
<tr>
<td>25</td>
<td>Successful Appliance Installation</td>
<td>45</td>
</tr>
<tr>
<td>26</td>
<td>Appliance is Rebooting</td>
<td>46</td>
</tr>
<tr>
<td>27</td>
<td>Appliance Is Configured</td>
<td>46</td>
</tr>
<tr>
<td>28</td>
<td>Appliance Build Number</td>
<td>47</td>
</tr>
<tr>
<td>29</td>
<td>Threat Grid Portal Login Page</td>
<td>53</td>
</tr>
<tr>
<td>30</td>
<td>The Cisco screen – F8 to enter the CIMC Configuration Utility</td>
<td>55</td>
</tr>
<tr>
<td>31</td>
<td>CIMC Configuration Utility</td>
<td>56</td>
</tr>
<tr>
<td>32</td>
<td>Cisco Integrated Management Controller (CIMC) Interface</td>
<td>57</td>
</tr>
</tbody>
</table>
INTRODUCTION

A Cisco Threat Grid appliance provides safe and highly secure on-premises advanced malware analysis, with deep threat analytics and content. Threat Grid Appliances provide the complete Threat Grid malware analysis platform, installed on a single UCS server: Cisco UCS C220-M3 (TG5000) or Cisco UCS C220 M4 (TG5400). They empower organizations operating under various compliance and policy restrictions, to submit malware samples to the appliance.

Many organizations that handle sensitive data, such as banks, health services, etc., must follow various regulatory rules and guidelines that will not allow certain types of files, such as malware artifacts, to be sent outside of the network for malware analysis. By maintaining a Cisco Threat Grid Appliance on-premises, organizations are able to send suspicious documents and files to it to be analyzed without 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

Before a new appliance can be used for malware analysis, it must be set up and configured for the organization's network. This guide is for the security team IT staff tasked with setting up and configuring a new Threat Grid Appliance.

This document describes how to complete the initial setup and configuration for a new Threat Grid Appliance, up to the point where malware samples can be submitted to it for analysis.

For more information, please see the Cisco Threat Grid Appliance Administrator's Guide, which can be found on the Install and Upgrade page on Cisco.com.

Release Notes

For detailed updates information, see the Release Notes, which may be found in the OpAdmin Portal:

Operations menu > Update Appliance

The release notes are cumulative: the most recent version contains all previous notes. Formatted PDF versions are also available online with the other Threat Grid Appliance documentation:


Version Lookup Table

For a list of Threat Grid Appliance release information see the Build Number/Version Lookup Table on page 48

Note: To view the release notes for the Threat Grid Portal UI, click Help in the UI’s navigation bar.

What’s New

For a full description of new features always check the Release Notes and other release documentation such as Migration Notes and Data Retention Notes. Major highlights are included here.
Documentation Updates for 2.4.3 - 2.4.3.3

The main changes to this guide are listed in the following table:

<table>
<thead>
<tr>
<th>Section Heading</th>
<th>Page</th>
<th>Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Exit Support</td>
<td>2</td>
<td>New feature description</td>
</tr>
<tr>
<td>Using IPv4LL Address Space for the Dirty Interface is Unsupported</td>
<td>2</td>
<td>New section</td>
</tr>
<tr>
<td>tgsh</td>
<td>12</td>
<td>New section</td>
</tr>
</tbody>
</table>

Network Exit Support

Similar in concept to VPN, the Network Exit setting will make any outgoing network traffic that is generated during the analysis to appear to exit from that location. Network Exit Localization was added to the Threat Grid Cloud portal with the 3.4.61 release, and is now available on the appliance with v2.4.3.

This feature replaces tg-tunnel. 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.

For more information, see the Network Exit Configuration section in the Threat Grid Appliance guide.

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.

The main goal of clustering is to increase the capacity of a single system by linking multiple appliances (currently 2-5) into a cluster. Each appliance in the cluster saves data in the shared file system and will have the same data as the other appliances in the cluster.

For additional information about the clustering functionality currently available, see the Clustering section in the Threat Grid Appliance Administrator’s Guide, as well as the Clustering FAQ, which are available on the Threat Grid Appliance Install and Upgrade page on the Cisco.com website.

Using IPv4LL Address Space for the Dirty Interface is Unsupported

Although using IPv4LL address space (168.254.0.16) for the Dirty interface has never been documented as supported, from version 2.3.0 forward it is recognized as broken, and therefore explicitly unsupported.
Automatic License Retrieval

If an appliance is connected with the Internet, it can attempt to retrieve a license, or a replacement for an expired license, via the network. Note that automated retrieval is at present only available for licenses sold or renewed after the release of version 2.3 of the software (2017-08-11).

More Windows Changes

The 2.3 release includes the following Windows changes:

- Removes Windows XP, including from appliances that previously grandfathered it in.
- Windows 7 is now 64-bit only.
- Samples submitted to `winxp` or `win7-x86` VMs are still available. Note that any scripts or clients which hardcoded `winxp` should be changed.

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 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.)

We strongly encourage consulting the documentation prior to use. Extended documentation regarding the backup functionality is available. See the Backup Notes and FAQ, and the Backup section added to the Threat Grid Appliance Administrator’s Guide. Both documents are available on the Threat Grid Appliance Install and Upgrade page on the Cisco.com website.

Windows XP Changes

Threat Grid appliances manufactured on or after 2017-07-01 (July 1, 2017), will no longer include licensing or distribution of Windows XP, in compliance with Microsoft requirements. The 2.2.3 minor release allows new factory installations to be run without Windows XP.

Integrating with Third Party Detection and Enrichment Services

With version 2.2, OpenDNS, TitaniumCloud, and VirusTotal integrations can now be configured on the Appliance, in the new configuration page. In OpAdmin, select Configuration > Integrations to open this page. See the Threat Grid Administrator’s Guide for more information.

Multiple URLs for Disposition Update Service Manager

Version 2.2 also includes the ability to configure multiple URLs for the Disposition Update Service Manager.
ClamAV Signatures Automatic Daily Update

With version 2.2 the appliance can now automatically download updates to ClamAV signatures on a daily basis, improving recognition of known malware. This feature is enabled by default, and can be disabled from the newly-added Integrations page in OpAdmin.

LDAP Authentication

LDAP Authentication has been added to the OpAdmin and TGSH Dialog administrator interfaces with version 2.1.6, released on January 5, 2017, to support those customers with multiple appliance administrators who don't want them sharing the same login and password. See the Threat Grid Administrator's Guide for more information.

Cisco UCS C220 M4 Server (TG5400)

Released on November 17, 2016, the C220 M4 server (TG5400) includes a hardware refresh. Please contact us at support@threatgrid.com to discuss any questions you may have about upgrading.

Note: Threat Grid will continue to provide support for M3s until after the expiration of their contracted lifespan. All the same M4 features are available as over-the-wire updates for existing M3s, except as otherwise noted.

The M5 server upgrade is currently under development. We strongly encourage existing M3 and M4 customers to contact us at support@threatgrid.com to discuss any questions you may have about which server upgrade is best for your needs, as well as data migration, backups, rollout strategies, etc. We think the best approach for planning the upgrade path to the M5 is to address our customers' requirements on an individual basis.

AMP for Endpoints Private Cloud Integration

The 2.0.3 release contains features to facilitate Threat Grid Appliance integrations with Fire AMP Private Cloud (renamed as AMP for Endpoints Private Cloud), including the ability to split the DNS between the Clean and Dirty network interfaces, CA Management, and AMP for Endpoints Private Cloud Integration Configuration.

Generated SSL certificates now have the CN duplicated as a subjectAltName. This addresses an incompatibility with SSL clients, which ignore the CN field when at least one subjectAltName is present. It may be necessary to regenerate any previously appliance-generated certificates if using such tools.

Version 2.0

Version 2.0 is a major release, built upon an updated operating system. It includes enhancements that will support future hardware releases, and also brings the Threat Grid Portal UI more in line with the Cloud version. This includes significant numbers of new and updated Behavioral Indicators and other changes.

Please read the Threat Grid Portal Release Notes beginning with release 3.3.45 for details. (From the Portal UI Navigation bar select Help, then click on the link to the release notes.)

Support - Contacting Threat Grid

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. Enter your support case with the [Cisco Support Case Manager](https://www.cisco.com/c/en/us/support/index.html).

• **Call.** For Cisco phone numbers and contact information see the [Cisco Contact page](https://www.cisco.com/c/en/us/about/contact/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**.

**Note:** You can break out of the OpAdmin wizard task-flow to enable Support Mode, prior to licensing.

**Start Support Mode - License Workaround Prior to Version 1.4.4**

There is an issue with licenses that has been resolved in the Threat Grid Appliance v1.4.4. If your software version is prior to 1.4.4, you will need to have successfully connected to Support Mode servers at least once (after November 14th, 2015), in order for your license to be accepted. The connection does not need to be ongoing or active at the time of the license validation.

**Required:** The Dirty network needs to be up in order for this step to work.
Support Servers

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

- support-snapsshots.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. Verify that SSH is specified for Support Snapshot services.
2. From the Support menu, select Support Snapshots.
3. Take the snapshot.
4. 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.
PLANNING

A Cisco Threat Grid Appliance is a Linux server with Threat Grid software installed by Cisco Manufacturing prior to shipping. Once a new appliance is received, it must be set up and configured for your on-premises network environment. Before you begin, there are a number of issues to consider and plan. Environmental requirements, hardware requirements, and network requirements are described below.

User Documentation and Online Help

**Threat Grid Appliance** - Threat Grid Appliance user documentation, including this document, the *Threat Grid Appliance Administrator’s Guide*, Release Notes, integration guides, and more, can be found on the [Install and Upgrade page](https://www.cisco.com) on Cisco.com.

**Threat Grid Portal UI Online Help** - Threat Grid Portal user documentation, including Release Notes, “Using Threat Grid” Online Help, API documentation, and other information is available from the **Help** menu located in the navigation bar at the top of the user interface.

Browsers

Threat Grid recommends using the following browsers:

- Chrome
- Firefox
- Safari
- Microsoft Internet Explorer: **Not Supported - Do Not Use**. Microsoft Internet Explorer is **NOT** recommended and not supported.

Environmental Requirements

The Threat Grid Appliance is deployed on a UCS C220-M3 or UCS C220-M4 server. Before you set up and configure your appliance, make sure the necessary environment requirements for power, rack space, cooling, and other issues are met, according to the specification for your server.

Hardware Requirements

The form factor for the Admin interface is SFP+. If you are clustering appliances, each one will require an additional SFP+ module on the Cust interface.

**Note:** The SFP+ modules must be connected before the appliance is powered on for the session in which the configuration wizard is going to be run.

If there are no SFP+ ports available on the switch, or SFP+ is not desirable, then a transceiver for 1000Base-T can be used (for example, Cisco Compatible Gigabit RJ 45 Copper SFP Transceiver Module Mini -GBIC - 10/100/1000 Base-T Copper SFP Module.)
Figure 2 - Cisco 1000BASE-T Copper SFP (GLC-T)

Monitor: You can either attach a monitor to the server, or, if CIMC (Cisco Integrated Management Controller) is configured, you can use a remote KVM.

Hardware Documentation

Installation and Service Guide for Cisco UCS C220 M4 Server:
• Cisco UCS C220 M4 Server Installation and Service Guide

Installation and Service Guide for Cisco UCS C220 M3 Server:

Spec Sheet for Cisco UCS C220 M4 High-Density Rack Server (Small Form Factor Disk Drive Model):

Spec Sheet for Cisco UCS C220 M3 High-Density Rack Server (Small Form Factor Disk Drive Model):

Cisco has a power/cooling calculator, which you may also find useful:
• https://mainstayadvisor.com/Go/Cisco/Cisco-UCS-Power-Calculator.aspx

Network Requirements

The Threat Grid Appliance requires three networks:

ADMIN - The "Administrative" network. Must be configured in order to perform the appliance setup.
• OpAdmin Management Traffic (HTTPS)
• SSH
• NFSv4 (Outbound). If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.

CLEAN - The "Clean" network is used for inbound, trusted traffic to the appliance (requests). This includes integrated appliances. For example, the Cisco Email Security appliances and Web Security appliances (ESA/WSA) connect to the IP address of the Clean interface.
Note: The URL for the Clean network interface will not work until the OpAdmin portal configuration is complete.

The following specific, restricted kinds of network traffic can be outbound from Clean:

- Remote syslog connections
- Email messages sent by the Threat Grid Appliance itself
- Disposition Update Service connections to AMP for Endpoints Private Cloud devices
- DNS requests related to any of the above
- LDAP

DIRTY - The "Dirty" network is used for outbound traffic from the appliance (including malware traffic).

Note: We recommend using a dedicated external IP address (i.e., the "Dirty" interface) that is different from your corporate IP, in order to protect your internal network assets.

For network interface setup information and illustrations, see the Network Interfaces section, and the Network Interface Connections Setup sections that follow.

DNS Server Access

The DNS server used for purposes other than Disposition Update Service lookups, resolving remote syslog connections, and resolving the mail server used for notifications from the Threat Grid software itself needs to be accessible via the dirty network.

By default, DNS uses the Dirty interface. The Clean interface is used for AMP for Endpoints Private Cloud integrations. 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 the OpAdmin interface.

See the Threat Grid Appliance Administrator's Guide for additional information.

NTP Server Access

The NTP server needs to be accessible via the Dirty network.

Integrations – ESA/WSA/AMP for Endpoints etc.

Additional planning may be required if the Threat Grid Appliance is going to be used with other Cisco products, such as ESA/WSA appliances, AMP for Endpoints Private Cloud, etc.

DHCP

If you are connected to a network configured to use DHCP, then follow the instructions provided in the Using DHCP section of the Threat Grid Appliance Administrator's Guide.

License

You will receive a license and password from Cisco Threat Grid.
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.

Organizations and Users

Once you have completed the appliance setup and network configuration, you will need to create the initial Threat Grid Organizations and add user account(s), so people can login and begin submitting malware samples for analysis. This task may require planning and coordination among multiple organizations and users, depending on your requirements.


Updates

The initial appliance setup and configuration steps must be completed before installing any Threat Grid appliance updates.

We recommend that you check for updates immediately after completing the initial configuration described in this guide.

Updates must be done in sequence. Threat Grid Appliance updates cannot be downloaded until the license is installed, and the update process requires the initial appliance configuration to be completed. Instructions for updating the appliance are located in the Threat Grid Appliance Administrator's Guide.

Note: Verify that SSH is specified for updates.

User Interfaces

After the server has been correctly attached to the network and powered up, there are several user interfaces available for configuring the Threat Grid Appliance. Note that LDAP authentication is available for TGSH Dialog and OpAdmin with version 2.1.6.

TGSH Dialog

The first interface is the TGSH Dialog, which is used to configure the Network Interfaces. TGSH Dialog is displayed when the appliance successfully boots up.

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.

To reconnect to the TGSH Dialog, 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 Portal Configuration, which is described in the next section.

tgsh

Threat Grid Shell. This is an administrator's interface that is used for executing a couple of commands (including destroy-data and forced backup), as well as for expert, low-level debugging. To access tgsh, select CONSOLE in the TGSH Dialog.

NOTE: OpAdmin uses the same credentials as the Threat Grid user, so any password changes/updates made via tgsh will impact OpAdmin as well.

Caution: Network configuration changes made with tgsh are NOT supported unless specifically directed by Threat Grid support. OpAdmin or TGSH Dialog should be used instead.

OpAdmin Portal

This is the primary Threat Grid GUI configuration tool. Much of the appliance configuration can ONLY be done via OpAdmin, including licenses, email host, SSL Certificates, etc.

Threat Grid Portal

The Threat Grid user interface application is available as a cloud service, and is also installed on Threat Grid Appliances. There is no communication between Threat Grid Cloud service, and the Threat Grid Portal that is included with a Threat Grid Appliance.

CIMC

Another user interface is the Cisco Integrated Management Controller ("CIMC"), which is used to manage the server.

Network Interfaces

Admin Interface

- Connect to the Admin network. **Only inbound** from Admin network.
- OpAdmin UI traffic
- SSH (inbound) for tgsh-dialog
- NFSv4 for Backups and Clustering (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.) Must be accessible from all cluster nodes.

**Note:** The form factor for the Admin interface is SFP+. See Figure 2 - Cisco 1000BASE-T Copper SFP (GLC-T).

Clust Interface

The non-Admin SFP+ port that was formerly reserved, is now being used for clustering.

- Clust interface required for clustering (optional)
• Requires an additional SFP+ module for direct interconnect. This interface does not require any configuration. Addresses are automatically assigned.

Clean Interface

• Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet.
• UI and API traffic (inbound)
• Sample Submissions
• SMTP (outbound connection to the configured mail server)
• SSH (inbound for tgsh-dialog)
• Syslog (outbound to configured syslog server)
• ESA/WSA – CSA Integrations
• AMP for Endpoints Private Cloud Integration
• DNS – Optional.
• LDAP (outbound)

Dirty Interface

Connect to the Dirty network. Requires Internet access. **Outbound Only!**

You should not use your own DNS (private IP) for the Dirty Interface, because traffic sent to a private IP is dropped at the Network Exit Localization firewall.

• DNS
  **Note:** If you are setting up an integration with a AMP for Endpoints Private Cloud, and the AMP for Endpoints appliance hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in OpAdmin.
• NTP
• Updates
• Support Session in Normal Operations Mode
• Support Snapshots
• Malware Sample-initiated Traffic
• Recovery Mode Support Session (outbound)
• OpenDNS, TitaniumCloud, Virus Total, ClamAV
• SMTP Outbound connections are redirected to a built-in honeypot

**Note:** Although using IPv4LL address space (168.254.0.16) for the Dirty interface has never been documented as supported, from version 2.3.0 forward it is recognized as broken, and therefore explicitly unsupported.
CIMC Interface

Recommended. If the Cisco Integrated Management Controller (“CIMC”) interface is configured, it can be used for server management and maintenance. For more information see APPENDIX A – CIMC CONFIGURATION (RECOMMENDED).

Login Names and Passwords - Defaults

Web UI Administrator

- Login:  admin
- Password:  "changeme"

OpAdmin and Shell user

Use the initial Threat Grid/TGSH Dialog randomly generated password, and then the new password entered during the first step of the OpAdmin configuration workflow.

If you lose the password, follow the Lost Password instructions located in the Support section of the Threat Grid Appliance Administrator’s Guide.

CIMC (Cisco Integrated Management Controller)

- Login:  admin
- Password:  "password"

Setup and Configuration Steps Outline

The following setup and initial configuration steps are described in this document:

- Server Setup.
- Network Interface Connections Setup:
  - Admin
  - Clust
  - Clean
  - Dirty
- Initial Network Configuration - TGSH Dialog.
- Main Configuration – OpAdmin Portal.
- Install Updates.
- Test the Appliance setup: Submit a Sample for Analysis.
- Admin Configuration – Complete the remaining administrative configuration tasks (license installation, email server, SSL Certificates, etc.) in the OpAdmin Portal as documented in the Threat Grid Appliance Administrator’s Guide.
Time Required for Setup and Configuration

You should allow yourself approximately 1 hour to complete the server setup and initial configuration steps.

*Note:* Please be patient during the “Apply” sections of the TGSH Dialog during the initial Appliance configuration installation steps. These steps can sometimes take more than 10 minutes to complete.
SERVER SETUP

To begin, connect both power supplies on the back of your appliance and connect the included KVM adapter to an external monitor and keyboard and plug into the KVM port located at the front of the server, as illustrated in the figure below.

If CIMC is configured, you can use a remote KVM. For CIMC configuration see Configuring CIMC (Optional) in the Appendix.

Please refer to the server product documentation for detailed hardware and environmental setup information. Links to product documentation are provided in the Hardware Documentation section, above.

Network Interface Connections Setup

The SFP+ modules must be connected to the chassis before the appliance is powered on for the session in which the configuration wizard is going to be run. However, wiring the SFP up to the network can be done between poweron and configuration.

Find the SFP+ ports (there are two) and the three Ethernet ports on the back of the appliance and attach the network cables as illustrated below:

C220 M3 Rack Server Setup

![Figure 3 - Cisco UCS C220 M3 SFF Rack Server](image)

The interfaces must be properly connected and configured for the appliance to operate.

**Note:** The details of your appliance may differ from the image above. Please contact support@threatgrid.com if you have any questions.

**Note:** "Reserved" is the non-Admin SFP+ port, which is reserved for future use.
See the diagram below for more information about the C220 M3 server.

Figure 4 - Cisco UCS C220 M3 Rear View Details

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power supplies (up to two)</td>
</tr>
<tr>
<td>2</td>
<td>Slot 2: Low-profile PCIe slot on riser: (half-height, half-length, x16 connector, x8 lane width)</td>
</tr>
<tr>
<td>3</td>
<td>Two SFP+ Ports. Slot 1: Admin Slot 2: Reserved for backup and storage support.</td>
</tr>
<tr>
<td>4</td>
<td>VGA video connector</td>
</tr>
<tr>
<td>5</td>
<td>Serial port (RJ-45 connector)</td>
</tr>
<tr>
<td>6</td>
<td>One 10/100/1000 Ethernet dedicated management port</td>
</tr>
<tr>
<td>7</td>
<td>Dual 1-GbE ports (LAN1 and LAN2)</td>
</tr>
<tr>
<td>8</td>
<td>USB ports</td>
</tr>
<tr>
<td>9</td>
<td>Rear Identification button/LED</td>
</tr>
</tbody>
</table>

**Note:** For releases 1.0-1.2 a reboot may be needed if an interface was not plugged in at boot time. This is a pre-1.3 issue, except for any interface requiring an SFP, which will still need to be plugged in at boot time post 1.3. The network cable plugged into the SFP may be hot-plugged safely.
C220 M4 Rack Server Setup

Figure 5 - Cisco UCS C220 M4 SFF Rack Server

Note: Use port 3 Slot 2 for the (optional) Clust interface.

Note: The details of your appliance may differ from the image above. Please contact support@threatgrid.com if you have any questions.
Figure 6 - Cisco UCS C220 M4 Rear View Details

<table>
<thead>
<tr>
<th></th>
<th>Connections:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Admin, Clust</td>
</tr>
<tr>
<td>8</td>
<td>(left) Clean</td>
</tr>
<tr>
<td>8</td>
<td>(right) Dirty</td>
</tr>
<tr>
<td>6</td>
<td>CIMC</td>
</tr>
</tbody>
</table>
Network Interface Setup Diagram

This section describes the most logical/recommended setup for a Threat Grid Appliance. However, each customer's interface setup is different. Depending on your network requirements, you may well decide to connect the Dirty interface to the inside, or the Clean interface to the outside with appropriate network security measures in place, for example.

Figure 7 - Network Interfaces Setup Diagram

- Outbound Traffic ONLY!
- Sample-Initiated Traffic
- DNS for the appliance
- NTP for the appliance
- Software Updates
- User-Initiated Support Connections
- OpenDNS, TitaniumCloud, VirusTotal, ClamAV
- NOTE: Outbound SMTP connections are redirected to a built-in honeypot

- Threat Grid Portal
  - User Interface and API (HTTPS)
  - Sample Submissions
  - SMTP Traffic to Local Mail Server
  - Recovery Mode Support Connections
  - Syslog
  - DNS over Clean if configured
  - LDAP

- Out-of-Band Server Management
  - CpAdmin Management Traffic (HTTPS)
  - SSH
  - NFSv4 required for Backup and Clustering.
    (Outbound, if a NFS hostname is used instead of IP, this name will be resolved via the Dirty DNS.)
Firewall Rules Suggestions

**Note:** Implementing a restrictive outgoing policy on the Dirty interface for ports 22 and 39791 will require tracking updates over time and spending more time maintaining the firewall, etc. See the required destinations in the configuration sections below.

**Note:** Although using IPv4LL address space (168.254.0.16) for the Dirty interface has never been documented as supported, from version 2.3.0 forward it is recognized as broken, and therefore explicitly unsupported.

### Dirty Interface Outbound

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dirty Interface</td>
<td>Internet</td>
<td>ANY</td>
<td>ANY</td>
<td>Allow</td>
<td>Allow outbound traffic from samples. (To get accurate results it is required that malware be allowed to contact its command and control server using whatever port and protocol it is designed to use.)</td>
</tr>
</tbody>
</table>

### Dirty Interface Inbound

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>Dirty Interface</td>
<td>ANY</td>
<td>ANY</td>
<td>Deny</td>
<td>Deny all incoming connections</td>
</tr>
</tbody>
</table>

### Clean Interface Outbound

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean Interface</td>
<td>SMTP Servers</td>
<td>TCP</td>
<td>25</td>
<td>Allow</td>
<td>The appliance uses the clean interface to initiate SMTP connections to the configured mail server</td>
</tr>
</tbody>
</table>
Clean Interface Outbound Optional

The following depends on what services are configured.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean Interface</td>
<td>Corporate DNS Server</td>
<td>TCP/UDP</td>
<td>53</td>
<td>Allow</td>
<td>&quot;Optional, only required if Clean DNS is configured&quot;</td>
</tr>
<tr>
<td>Clean Interface</td>
<td>AMP Private Cloud</td>
<td>TCP</td>
<td>443</td>
<td>Allow</td>
<td>&quot;Optional, only required if AMP for Endpoints Private Cloud integration is used&quot;</td>
</tr>
<tr>
<td>Clean Interface</td>
<td>Syslog Servers</td>
<td>UDP</td>
<td>514</td>
<td>Allow</td>
<td>Allow connectivity to server designated to receive Syslog messages and Threat Grid notifications</td>
</tr>
<tr>
<td>Clean Interface</td>
<td>LDAP Servers</td>
<td>TCP/UDP</td>
<td>389</td>
<td>Allow</td>
<td>&quot;Optional, only required if LDAP is configured&quot;</td>
</tr>
<tr>
<td>Clean Interface</td>
<td>LDAP Servers</td>
<td>TCP</td>
<td>636</td>
<td>Allow</td>
<td>&quot;Optional, only required if LDAP is configured&quot;</td>
</tr>
</tbody>
</table>

Clean Interface Inbound

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Subnet</td>
<td>Clean Interface</td>
<td>TCP</td>
<td>22</td>
<td>Allow</td>
<td>Allow SSH connectivity to the tgsh-dialog</td>
</tr>
<tr>
<td>User Subnet</td>
<td>Clean Interface</td>
<td>TCP</td>
<td>80</td>
<td></td>
<td>Appliance API and Threat Grid user interface. This will redirect to HTTPS TCP/443</td>
</tr>
<tr>
<td>User Subnet</td>
<td>Clean Interface</td>
<td>TCP</td>
<td>443</td>
<td></td>
<td>Appliance API and Threat Grid user interface</td>
</tr>
<tr>
<td>User Subnet</td>
<td>Clean Interface</td>
<td>TCP</td>
<td>9443</td>
<td></td>
<td>Allow connectivity to the Threat Grid UI Glovebox</td>
</tr>
</tbody>
</table>

Admin Interface Outbound Optional

The following depends on what services are configured.
### Admin Interface Inbound

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Subnet</td>
<td>Admin Interface</td>
<td>TCP</td>
<td>22</td>
<td>Allow</td>
<td>Allow SSH connectivity to the TGSH Dialog</td>
</tr>
<tr>
<td>Admin Subnet</td>
<td>Admin Interface</td>
<td>TCP</td>
<td>80</td>
<td>Allow</td>
<td>Allow Access to the OpAdmin Portal interface. This will redirect to HTTPS TCP/443</td>
</tr>
<tr>
<td>Admin Subnet</td>
<td>Admin Interface</td>
<td>TCP</td>
<td>443</td>
<td>Allow</td>
<td>Allow Access to the OpAdmin Portal interface</td>
</tr>
</tbody>
</table>

### Dirty Interface for Non Cisco-Validated/Recommended Deployment

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Action</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dirty Interface</td>
<td>Internet</td>
<td>TCP</td>
<td>22</td>
<td>Allow</td>
<td>&quot;Update, support snapshot, and licensing services&quot;</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>Internet</td>
<td>TCP/UDP</td>
<td>53</td>
<td>Allow</td>
<td>Allow outbound DNS</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>Internet</td>
<td>UDP</td>
<td>123</td>
<td>Allow</td>
<td>Allow outbound NTP</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>Internet</td>
<td>TCP</td>
<td>19791</td>
<td>Allow</td>
<td>Allow connectivity to Threat Grid support</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>Cisco Umbrella</td>
<td>TCP</td>
<td>443</td>
<td>Allow</td>
<td>Connect with 3rd party detection and enrichment services</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>VirusTotal</td>
<td>TCP</td>
<td>443</td>
<td>Allow</td>
<td>Connect with 3rd party detection and enrichment services</td>
</tr>
<tr>
<td>Dirty Interface</td>
<td>TitaniumCloud</td>
<td>TCP</td>
<td>443</td>
<td>Allow</td>
<td>Connect with 3rd party detection and enrichment services</td>
</tr>
</tbody>
</table>
Power On and Boot Up

Once you have connected the server peripherals and the network interfaces (don't forget to attach the power cables and plug it in!), turn on the appliance and wait for it to boot up. The Cisco screen is displayed briefly:

Figure 8 - Cisco Screen During Boot Up

Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration, <F12> Network Boot

Bios Version : C220M3.2.0.5.0.050120140402
Platform ID : C220M3

Cisco IMC IPv4 Address : 198.16.2.21
Cisco IMC MAC Address : 50:07:09:87:70:04

\ Loading LSI EFI SAS Driver
Total Memory = 512 GB Effective Memory = 512 GB
Memory Operating Speed 1866 Mhz

Entering CIMC Configuration Utility...

Note: If you want to configure this interface, press F8 after the memory check is completed, and follow the instructions provided in Appendix A, Configuring CIMC.

The TGSH Dialog is displayed on the console when the server has successfully booted up and connected:
The Admin URL shows as unavailable - the network interface connections are not yet configured and the OpAdmin Portal cannot be reached yet to perform this task.

**Note:** Make a note of the administrator Password into a separate text file for convenience (copy-paste) during the OpAdmin Portal configuration steps.

**IMPORTANT:** The **TGSH Dialog** displays the initial administrator password, which will be needed in order to access and configure the OpAdmin Portal interface later in the configuration workflow steps.
INITIAL NETWORK CONFIGURATION – TGSH DIALOG

The initial network configuration is completed in the TGSH Dialog. The goal is to complete the basic configuration that will allow access to the OpAdmin interface tool to finish the remaining configuration, including the license, email host, SSL Certificates, etc.

**DHCP Users:** The following steps assume that you are using static IP addresses. If you are using DHCP to obtain your IPs, then please see the *Threat Grid Appliance Administrator’s Guide* for more information.

1. In the TGSH Dialog interface, select **CONFIG_NETWORK**. The Network Configuration console opens:

   ![Figure 10 - TGSH Dialog - Network Configuration Console](image)

2. Complete the blank fields according to the settings provided by your network administrator for the Clean, Dirty, and Admin interfaces.

3. Change **DHCP Enabled** from **Y** to **N**.
   
   **Note:** You need to **BACKSPACE** over the old character before you can enter the new one.
4. **DNS NAME.** If your network is using a DNS name for the Clean network, then enter the name here.

5. Leave **Configure Non-Default Routes?** set to the default of **N** (unless additional routes are needed).

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

---

Figure 11 - Network Configuration In-Progress (clean and dirty)
7. After you finish entering all 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:
8. Select **Apply** to apply your configuration settings.

Have patience. This step may take 10 minutes or more to complete.

The console will become a blank grey box, and the screen may display scrolling configuration information as the settings are applied, and then it will list detailed information about the configuration changes that have been made:
9. Select **OK**.

The Network Configuration Console refreshes again and displays the IP addresses you entered:
You have completed the network configuration of your appliance.

**Note:** The URL for the Clean interface will not work until the OpAdmin portal configuration is complete.

**Next Setup Step:**

The next step in the appliance setup is to complete the remaining configuration tasks using the workflow in the OpAdmin portal, as described in the next section.
CONFIGURATION WIZARD - OPADMIN PORTAL

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

The OpAdmin Portal is the recommended tool for configuring your appliance, and in fact, much of the appliance configuration can only be done via the OpAdmin portal interface, including:

- OpAdmin Portal administrator's password
- Email servers
- DNS servers
- NTP servers
- SSL Certificates
- Clustering
- Other server settings
- https://<adminIP>/ OR https://<adminHostname>/

Note: Not all of these settings are completed in the initial OpAdmin portal configuration wizard workflow. Some, such as SSL Certificates and Clustering, are configured in separate steps, as described in the Threat Grid Appliance Administrator's Guide, located on the Threat Grid Appliance documentation page on cisco.com.

Configuration Workflow

The steps in the following sections should be completed in one session to reduce the chance of an interruption to the IP address during configuration.

Login to the OpAdmin Portal

1. Point your browser at the OpAdmin Portal interface (the Admin URL with the "https"). The Threat Grid OpAdmin login screen opens:
2. Enter the initial Admin Password that you copied from the TGSH Dialog and click **Login**. The *Change Password* page opens.

Continue with the next section:
Admin Password Change

The initial administrator's password was generated randomly during the pre-ship Threat Grid installation, and is visible as plain text in the TGSH Dialog. You must change the initial Admin password before you may continue with the configuration workflow.

Figure 17 - OpAdmin Change Password

1. Enter the password from the TGSH Dialog into the Old Password field. (You should have this in a text file for use at this moment.)

2. Enter and confirm a new password.

3. Click Change Password.

The password is updated. The End User License Agreement page opens.

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

If you lose the password, follow the Lost Password instructions located in the Support section of the Threat Grid Appliance Administrator’s Guide.
Continue with the next section:

End User License Agreement

1. Review the End User License Agreement.
2. Scroll down to the end, and click I HAVE READ AND AGREE. The License page opens:

![License Page](image)

We recommend that you follow the configuration workflow, and configure the networks before you install the license, as described in the next section, Network Configuration Settings.

Network Configuration Settings

If you configured your static network settings in the TGSH Dialog, the IP addresses displayed in the Network Configuration page will reflect the values you entered in the TGSH Dialog during the appliance network configuration.
Network Configuration and DHCP

If you used DHCP for your initial connection and now need to change the Clean and Dirty IP networks to static IP addresses, then follow the steps in the section: Networking > Using DHCP, located in the Threat Grid Appliance Administrator’s Guide.

Continue with the next section:

License Installation

After the networks are configured, you are ready to install the Threat Grid license. (In versions older than v1.4.4, you will need to start Support Mode in order for your license to be accepted. See Start Support Mode - License Workaround Prior to Version 1.4.4 for more information.)

Figure 19 - License Page Prior to Installation

1. Click on License in the left column. The License page opens as shown above. No license has been installed.

2. Under Upload New License, click Chose File, and select the license from your file manager.

   Retrieve License From Server - Alternatively, the 2.3 release adds the ability to select Retrieve. If the appliance has network access when being installed, selecting this option will retrieve a license over the network.

3. Enter the license password you were given into the Passphrase field.
4. Click **Upload** to install. The page refreshes, and you should see your license information:

**Figure 20 - License Information After Successful Installation**

<table>
<thead>
<tr>
<th>Appliance ID</th>
<th>FCH1832V32N</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td></td>
</tr>
<tr>
<td>Licensee</td>
<td>No Name Provided <a href="mailto:provision@threatgrid.com">provision@threatgrid.com</a></td>
</tr>
<tr>
<td>Business</td>
<td>25f18e8d-dd45-4397-9533-3c6d38239c32</td>
</tr>
<tr>
<td>Validity</td>
<td>Fri, 22 Sep 2017 14:47:46 +0000 - Mon, 21 Sep 2020 14:47:46 +0000</td>
</tr>
<tr>
<td>Product SKU</td>
<td></td>
</tr>
<tr>
<td>Daily Submissions</td>
<td>1500</td>
</tr>
</tbody>
</table>

**Upload New License**

- **Choose File**: No file chosen
- **Passphrase**

**Retrieve License From Server**

- **Retrieve**

Click **Next** to continue. The **Email** page opens.

Continue with the next section:
NFS Configuration

The next step in the workflow is NFS configuration. This task is required for backups, and also for clustering. (See NFS Requirements in the Threat Grid Appliance Guide section on Backups for more information.)

Figure 21 - NFS Configuration

1. Click on NFS in the left column. The NFS page opens.
2. Configure the page as follows:
   - **Host** - The NFSv4 host server. We recommend using the IP address.
   - **Path** - The absolute path to the location on the NFS host server under which files will be stored.
   - **Opts** - NFS mount options to be used, if this server requires any deviations from standard Linux defaults for NFSv4.
   - **Status** - Select Enabled from the dropdown (Pending Key).
3. Click Next. The page will refresh, with a **FS Encryption Password Key ID** now available.

The first time you configure this page, options to **Remove** or to **Download** the encryption key become visible. **Upload** is available if you have NFS enabled but no key created. Once you create a key, **Upload** is changed to a **Download** button. (If you delete the key, the **Download** button becomes **Upload** again.)

**NOTE:** If the key correctly matches the one used to create a backup, the **Key ID** displayed in OpAdmin after upload will match the name of a directory in the configured path. As already noted, backups cannot be restored without the encryption key.

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.

4. Click Next. The **Email** page opens.

Continue with the next section:

**Email Host Configuration**

The next step in the workflow is to configure the email host.
Figure 22 - Email Host Configuration

1. Click on Email in the left column. The Email page opens.
2. Enter the name of the Upstream Host (email host).
3. Change the port from 587 to 25.
4. Leave the other settings at the defaults.
5. Click Next. The Notifications page opens.

Continue with the next section:
Server Notifications Configuration

The next step in the workflow is to configure notifications that can be delivered periodically to one or more email addresses. System notifications are displayed in the Threat Grid portal interface, but this page allows you to set up notifications that are also sent via email.

Syslog Configuration

Update v1.3 includes a page to configure a Syslog server to receive syslog messages and Thread Grid notifications. See the Threat Grid Appliance Admin Guide for more information.

**Figure 23 - Notifications Configuration**

1. First, set the Critical Notification Frequency and the Notification Frequency by selecting them from the dropdown lists.
2. Next, in Notification Recipients, enter one or more email addresses separated by commas.
3. Click Next. The Date and Time page opens.
Continue with the next section:
NTP Server Configuration

This is where you identify the NTP ("Network Time Protocol") servers.

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

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

2. Ignore Current System Time and Synchronize with Browser.

3. Click **Next**.

   The **Review and Install** page opens with checkboxes next to all of the Configuration steps.

Continue with the next section:

Review and Install Configuration Settings

Now that you have entered your network configuration settings, you must install them as described below.

1. In the **Review and Install** page, click **Start Installation**.

   Configuration scripts are installed and you see the message: "The appliance is installing...”.

   **Note:** Have patience. Please allow 10+ minutes for this step to complete. The screen will display configuration information as it is applied.
2. After successful installation, the State changes from the orange **Running** to a green **Successful** message confirming success. The **Reboot** button changes to green, and the configuration output is displayed:
Figure 25 - Successful Appliance Installation

3. Click **Reboot** after the successful installation. You will see the message that "The appliance is rebooting". Rebooting may take up to 5 minutes.

Please do not make any changes while the Appliance is rebooting.
Once the appliance has successfully rebooted, you will see the following confirmation that the Appliance is configured:

Your appliance is now setup and the initial configuration is complete.
INSTALLING THREAT GRID APPLIANCE UPDATES

After you complete the initial Threat Grid Appliance setup we recommend that you install any available updates before continuing.

Threat Grid Appliance updates are applied through the OpAdmin Portal.

From the Operations menu, select Update Appliance. The updates page opens, displaying the current build of the appliance.

Click Check/Download Updates. The software checks to see if there is a more recent update/version of the Threat Grid Appliance software, and if so, it is downloaded. This may take some time.

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

For more information about installing updates, see the Threat Grid Appliance Administrator's Guide.

Appliance Build Number

The build number of an appliance can be viewed on the Updates page: OpAdmin Operations > Update Appliance:

Figure 28 - Appliance Build Number

Your appliance can be updated to the latest available version. Have an up-to-date backup before updating.

appliance is currently running:

2014.10.20150203155142.b06f7b4f

Check/Download Updates

Run Update

This appliance has never been updated.
## 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 version numbers:

<table>
<thead>
<tr>
<th>Build Number</th>
<th>Release Version</th>
<th>Release Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017.12.20180601200650.e0c052b0.rel</td>
<td>2.5</td>
<td>9/14/2018</td>
<td>Win10, sample deletion, Refresh to 3.5.11</td>
</tr>
<tr>
<td>2017.12.20180601200650.e0c052b0.rel</td>
<td>2.4.3.3</td>
<td>6/1/2018</td>
<td>Fix cluster initialization, prune ancient ES/PG migration support</td>
</tr>
<tr>
<td>2017.12.20180501005218.4e3746f4.rel</td>
<td>2.4.3.1</td>
<td>5/1/2018</td>
<td>PG schema reporting for DDL error detection at update check</td>
</tr>
<tr>
<td>2017.12.2018042723427.e616a2f2.rel</td>
<td>2.4</td>
<td>4/27/2018</td>
<td>Remote Virtual Exit Localization; direct standalone-to-cluster migration</td>
</tr>
<tr>
<td>2017.12.201803202174440.097e2883.rel</td>
<td>2.4</td>
<td>3/2/2018</td>
<td>Clustering</td>
</tr>
<tr>
<td>2017.12.20180219033533.4b76549b.rel</td>
<td>2.4.1</td>
<td>2/19/2018</td>
<td>Clustering support in OpAdmen. Refreshes the portal software to 3.4.59</td>
</tr>
<tr>
<td>2017.12.20180130110951.rel</td>
<td>2.4.0.1</td>
<td>1/30/2018</td>
<td>Security update to ClamAV only</td>
</tr>
<tr>
<td>2017.12.20171214191003.4b76ea16.rel</td>
<td>2.4</td>
<td>12/14/2017</td>
<td>Clustering EFT. jp/kr contsubs. Refresh portal to 3.4.57.</td>
</tr>
<tr>
<td>2016.05.201711300223355.147bdo23.rel</td>
<td>2.3.3</td>
<td>11/30/2017</td>
<td>Starting point for 2.4 upgrade</td>
</tr>
</tbody>
</table>
### INSTALLING THREAT GRID APPLIANCE UPDATES

<table>
<thead>
<tr>
<th>Build Number</th>
<th>Release Version</th>
<th>Release Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016.05.20171007215506.0700e1db.rel</td>
<td>2.3.2</td>
<td>10/7/2017</td>
<td>ElasticSearch shard count reduction.</td>
</tr>
<tr>
<td>2016.05.20170828200941.e5eab0a6.rel</td>
<td>2.3.1</td>
<td>8/28/2017</td>
<td>Bug fixes.</td>
</tr>
<tr>
<td>2016.05.20170810212922.28c79852.rel</td>
<td>2.3</td>
<td>8/11/2017</td>
<td>Automates license download. Refreshes the portal software to 3.4.47.</td>
</tr>
<tr>
<td>2016.05.20170710175041.77cob12f.rel</td>
<td>2.2.4</td>
<td>7/10/2017</td>
<td>This release introduces Backup functionality.</td>
</tr>
<tr>
<td>2016.05.20170519231807.db2f167e.rel</td>
<td>2.2.3</td>
<td>5/20/2017</td>
<td>This minor release allows new factory installations to be run without Windows XP.</td>
</tr>
<tr>
<td>2016.05.20170508195308.b8dc88ed.rel</td>
<td>2.2.2</td>
<td>5/8/2017</td>
<td>Minor release of changes to network configuration and operating-system components to support upcoming features.</td>
</tr>
<tr>
<td>2016.05.20170323020633.f82e66fe.rel</td>
<td>2.2.1</td>
<td>3/24/2017</td>
<td>Disables SSLv3, fixes a resource issue</td>
</tr>
<tr>
<td>2016.05.201703082111223.c92516ee.rel</td>
<td>2.2mfg</td>
<td>3/8/2017</td>
<td>Manufacturing-only changes. No customer impact. Not deployed via update server.</td>
</tr>
<tr>
<td>2016.05.20170303034712.1b205359.rel</td>
<td>2.2</td>
<td>3/3/2017</td>
<td>Storage migration, Pruning, Mask UI, Multi-disposition update</td>
</tr>
<tr>
<td>2016.05.20170105200233.32f70432.rel</td>
<td>2.1.6</td>
<td>1/7/2017</td>
<td>LDAP Authentication support for OpAdmin/tgsh-dialog</td>
</tr>
<tr>
<td>2016.05.20161121134140.489f130d.rel</td>
<td>2.1.5</td>
<td>11/21/2016</td>
<td>ElasticSearch5; CSA performance fix</td>
</tr>
<tr>
<td>Build Number</td>
<td>Release Version</td>
<td>Release Date</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------</td>
<td>--------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>2016.05.20160905202824.f7792890.rel</td>
<td>2.1.4</td>
<td>9/5/2016</td>
<td>Primarily of interest to Manufacturing</td>
</tr>
<tr>
<td>2016.05.20160811044721.6af0fa61.rel</td>
<td>2.1.3</td>
<td>8/11/2016</td>
<td>Offline update support key, M4 wipe support</td>
</tr>
<tr>
<td>2016.05.20160715165510.baed88a3.rel</td>
<td>2.1.2</td>
<td>7/15/2016</td>
<td></td>
</tr>
<tr>
<td>2016.05.20160706015125.b1fc50e5.rel-1</td>
<td>2.1.1</td>
<td>7/6/2016</td>
<td></td>
</tr>
<tr>
<td>2016.05.20160621044600.092b23fc</td>
<td>2.1</td>
<td>6/21/2016</td>
<td></td>
</tr>
<tr>
<td>2015.08.20160501161850.56631ccd</td>
<td>2.0.4</td>
<td>5/4/2016</td>
<td>Starting point for the 2.1 update. You must be at 2.0.4 before you can update to 2.1.</td>
</tr>
<tr>
<td>2015.08.20160315265529.599f2056</td>
<td>2.0.3</td>
<td>3/15/2016</td>
<td>Introduces AMP integration, CA mgmt., and split DNS</td>
</tr>
<tr>
<td>2015.08.20160217173404.ec264f73</td>
<td>2.0.2</td>
<td>2/18/2016</td>
<td></td>
</tr>
<tr>
<td>2017.12.20180302174440.097e2883.rel</td>
<td>2.4.2</td>
<td>3/2/2018</td>
<td>Clustering</td>
</tr>
<tr>
<td>2017.12.20180219033153.bb5e549b.rel</td>
<td>2.4.1</td>
<td>2/19/2018</td>
<td>Clustering support in OpAdmen. Refreshes the portal software to 3.4.59.</td>
</tr>
<tr>
<td>2017.12.20180130110951.rel</td>
<td>2.4.0.1</td>
<td>1/30/2018</td>
<td>Security update to ClamAV only</td>
</tr>
<tr>
<td>2015.08.20160211192648.e7d2e3a</td>
<td>2.0.1</td>
<td>2/12/2016</td>
<td></td>
</tr>
<tr>
<td>2015.08.201601301061029.8b6bc1d6</td>
<td>2.0</td>
<td>2/11/2016</td>
<td>Force update to 2.0.1 from here</td>
</tr>
<tr>
<td>2014.10.20160115122111.1f09cb5f</td>
<td>1.4.6</td>
<td>1/27/2016</td>
<td>Starting point for the 2.0.4 update</td>
</tr>
<tr>
<td>2014.10.20151123133427.898f70c2</td>
<td>v1.4.5</td>
<td>11/25/2015</td>
<td></td>
</tr>
</tbody>
</table>
### INSTALLING THREAT GRID APPLIANCE UPDATES

<table>
<thead>
<tr>
<th>Build Number</th>
<th>Release Version</th>
<th>Release Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014.10.20151116154826.9af96403</td>
<td>v1.4.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20151020111307.3f124cd2</td>
<td>v1.4.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150904134201.ef4843e7</td>
<td>v1.4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150824161909.4ba773cb</td>
<td>v1.4.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150822201138.8934fa1d</td>
<td>v1.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150805134744.4ce05d84</td>
<td>v1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150709144003.b4d4171c</td>
<td>v1.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150326161410.44cd33f3</td>
<td>v1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150203155143+hotfix1.bo6f7b4f</td>
<td>v1.1+hotfix1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20150203155142.bo6f7b4f</td>
<td>v1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014.10.20141125162160+hotfix2.8afc5e2f</td>
<td>v1.0+hotfix2</td>
<td><strong>NOTE:</strong> The 1.0+hotfix2 is a mandatory update that fixes the update system itself to be able to handle large files without breaking.</td>
<td></td>
</tr>
<tr>
<td>2014.10.20141125162158.8afc5e2f</td>
<td>v1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** For release versions 1.0-1.2 a reboot may be needed if an interface was not plugged in at boot time. This is a pre-v1.3 issue, except for any interface requiring an SFP, which will still need to be plugged in at boot time post v1.3. The network cable plugged into the SFP may be hot-plugged safely.

**Note:** Updating from 1.0 to 1.0+hotfix2 takes approximately 15 minutes. Applying a full update from 1.0 to 1.3 (without data migration) takes about 30 minutes.
TEST THE APPLIANCE SETUP - SUBMIT A SAMPLE

Once the Threat Grid Appliance is updated to the current version, the final test that your appliance has been configured properly is to submit a malware sample using the Threat Grid software.

1. Sign into the Threat Grid Portal by visiting the address you configured as the Clean interface. The Threat Grid login page opens:

Figure 29 - Threat Grid Portal Login Page

2. Enter the default Login and Password: admin/changeme

3. Click Login. The main Threat Grid Sample Analysis page opens.

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

5. Click Upload Sample. The Threat Grid sample analysis process is launched.

You should see your sample going through several stages of analysis. During analysis, the sample is listed in the Submissions section. Once analysis is completed, the results should be available in the Samples section, with details in the Analysis Report.
APPLIANCE ADMINISTRATION

Once the Threat Grid Appliance has been setup and initial configuration is completed, it is ready for the appliance administrator.

Release notes, Updates, SSL Certificates, adding users, and other administrator tasks and topics are documented in the Threat Grid Appliance Administrator's Guide.
APPENDIX A – CIMC CONFIGURATION (RECOMMENDED)

The first window displayed as the server is booting is the Cisco window, which allows you to enter the Cisco Integrated Management Controller ("CIMC") Configuration Utility. The CIMC interface can be used for remote server management.

You will need a monitor and keyboard attached directly to the appliance.

1. Power on the server. The Cisco screen opens:

   **Figure 30 - The Cisco screen – F8 to enter the CIMC Configuration Utility**

   ```
   Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC Configuration, <F12> Network Boot
   
   BIOS Version: C220M3.2.0.3.0.080120140402
   Platform ID: C220M3
   
   Cisco IMC IPv4 Address: 190.16.2.21
   Cisco IMC MAC Address: 50:67:03:07:70:04
   
   Loading LSI EFI SAS Driver
   Total Memory = 512 GB Effective Memory = 512 GB
   Memory Operating Speed 1666 MHz
   
   Entering CIMC Configuration Utility...
   ```

2. After the memory check is completed press F8 to enter the CIMC configuration utility:
3. In the CIMC configuration utility, set up an IP address that will be used for remote server management.

   When complete, Save, and then Exit.
   
   At this point the server can be managed remotely by using a Web browser to https://<CIMC-IP address>/
   
   The initial user name is "admin", with a password of "password".
The CIMC interface can now be used to view the server health as well as open a KVM to complete the remaining setup steps remotely.
INDEX

about Threat Grid appliances ....................................2
adding organizations ..............................................11
adding users .........................................................11
Admin interface ......................................................12
  form factor .......................................................8
  settings ..........................................................26
Admin network requirements ....................................9
administrator password
  changing ...........................................................34
  initial ............................................................25, 33
administrator tasks .................................................54
after successful installation .....................................44
  reboot .............................................................45
AMP for Endpoints Private Cloud ..............................4, 10
  DNS configured on Clean ....................................13
  formerly called FireAMP Private Cloud .................4
API
  rate limits .......................................................11
API documentation ................................................8
API traffic (inbound) ..............................................13
appliance
  administration ................................................54
appliance build number ........................................47
appliance server
  UCS C220-M3 ...................................................8
  UCS C220-M4 ...................................................8
appliance setup
  testing ..........................................................53
Apply
  configuration settings .......................................29
  automatic license retrieval ................................3
  backups ........................................................3
    NFSv4 .........................................................12
  boot up ........................................................24
  browsers
    do not use Microsoft Internet Explorer ..............8
    recommended ..............................................8
build number
  release version lookup table ..............................48
build number ....................................................47
C220 M3 rack server setup ....................................16
C220 M4 rack server setup ....................................18
Change Password .................................................34
  checking for updates .......................................11
  Chrome .........................................................8
  CIMC ..........................................................12
  configuring ......................................................55
CIMC configuration utility ....................................56
CIMC interface ....................................................14
  configuring ......................................................24
Cisco Integrated Management Controller ("CIMC") ........12
Cisco UCS C220 M4 server .....................................4
ClamAV
  Dirty interface ................................................13
  ClamAV signatures ............................................4
Clean interface ...................................................13
  DNS .............................................................10
    settings ......................................................26
Clean interface outbound
  firewall rules ................................................21
Clean interface outbound optional
  firewall rules ................................................22
Clean network
  DNS Name .....................................................27
  Clean network requirements .............................9
Clust interface ...................................................12, 18
  clustering ......................................................2
  Clust interface required ..................................12
  NFSv4 .........................................................12
CONFIG_NETWORK ..................................................26
configuration .....................................................12
  email host ...................................................12
    licenses ......................................................12
    server notifications ....................................41
  SSL Certificates .............................................12
    syslog ........................................................41
configuration changes
  detailed list of .............................................29
configuration settings
  applying ........................................................29
configuration wizard
  OpAdmin ........................................................32
configuration workflow
  install license after networks are configured ..........35
  NFS .............................................................38
  NTP servers ..................................................43
    review and install configuration settings ...........43
    server notifications ....................................41
    the email host ..........................................39
Configure Non-Default Routes? .................................27
Configuring CIMC .................................................24
contacting support ..............................................4
INDEX

creating organizations ..............................................11
Critical Notification Frequency ..............................41
Cust interface
form factor ..........................................................8
Date and Time page .............................................41
DHCP ....................................................................10
DHCP Enabled .......................................................26
DHCP used for initial connection
changing Clean and Dirty to static IP addresses ....36
diagram of network interfaces ..............................20
Dirty DNS ................................................................9
Dirty interface ......................................................13
Dirty interface inbound
firewall rules ........................................................21
Dirty interface outbound
firewall rules ........................................................21
Dirty interface settings .........................................26
Dirty network
DNS Name ............................................................27
NTP server ............................................................10
requirements .........................................................10
support mode .........................................................5
Disposition Update Service connections
to AMP for Endpoints Private Cloud devices ......10
Disposition Update Service Manager .................3
DNS .......................................................................13
requests ...............................................................10
server access .........................................................10
DNS NAME ............................................................27
documentation
appliance admin guides .......................................8
hardware guides ...................................................9
Download
encryption key .......................................................39
e-mail
sent by the appliance ..........................................10
Email ......................................................................40
e-mail host configuration .......................................39
Email page ..........................................................37, 39
enabling support mode ........................................5, 6
encrypted backups ...............................................3
encryption key
removing, downloading, uploading ....................39
required for backup restore ................................39
End User License Agreement ................................35
End User License Agreement page ......................34
environmental requirements ...............................8
ESA/WSA appliances ............................................10
establishing a support session ..............................6
ethernet ports ......................................................16
FireAMP Private Cloud
renamed AMP for Endpoints Private Cloud .........4
Firefox ..................................................................8
firewall rules
Clean interface outbound .......................................21
Clean interface outbound optional ......................22
Dirty interface inbound .........................................21
Dirty interface outbound ......................................21
firewall rules suggestions .....................................21
form factor ..........................................................8
FS Encryption Password Key ID ............................39
getting started .....................................................16
hardware documentation ....................................9
hardware requirements ........................................8
Help
for Threat Grid portal UI .....................................2, 8
hot-plugged ..........................................................17
inbound traffic .......................................................9
initial configuration to access OpAdmin ..............26
installing the Threat Grid license .......................36
installing updates ................................................11, 47
integrations ..........................................................3, 10
AMP for Endpoints Private Cloud .....................4, 10, 13
CSA (ESA/WSA/etc.) ..........................................13
ESA/WSA appliances ..........................................10
OpenDNS ..............................................................3
Titanium Cloud ....................................................3
VirusTotal .............................................................3
interface settings ..................................................26
interfaces .............................................................11
IP addresses ........................................................26
obtaining with DHCP ..........................................26
IP addresses entered ............................................30
IPv4LL address space
unsupported for Dirty interface .........................21
KVM
opening .............................................................57
remote ...............................................................16
LDAP .................................................................10
LDAP (outbound) ................................................13
LDAP authentication ..........................................4, 11
license ...............................................................10
password ...........................................................36
retrieve from server ..........................................36
retrieve or replace automatically .......................3
upload new ..........................................................36
INDEX

planning .......................................................... 8
  time required for setup .................................... 15
portal user documentation .................................. 8
  ports
    M3 ............................................................ 16
    M4 ............................................................ 18
  power on ....................................................... 24
protecting network assets .................................. 10
rash server ..................................................... 6
rate limits ........................................................ 11
Reboot
  after successful installation .............................. 45
  rebooting ...................................................... 45
receiving syslog messages .................................. 41
reconnecting to the TGSH Dialog ......................... 11
recovery mode .................................................. 13
Release Notes
  Threat Grid appliance ...................................... 2
  Threat Grid portal UI ...................................... 2
release version
    build number lookup table ............................... 48
remote access to the appliance ............................ 5
remote KVM ..................................................... 11
remote syslog connections .................................. 10
Remove
  encryption key ................................................ 39
requirements ..................................................... 8
  environmental ............................................... 8
  hardware ...................................................... 8
network ........................................................ 9
Reserved port ................................................... 16
reset for backup preparation ............................... 3
Retrieve License From Server ............................... 36
Review and Install page ..................................... 43
reviewing and installing configuration settings ........ 43
Safari .................................................................... 8
Sample Analysis page ......................................... 53
sample submissions ........................................... 13
server
  environmental requirements ................................ 8
server notifications
    configuring .................................................... 41
server setup .................................................... 16
setup and configuration
  basic ............................................................ 26
  getting started ............................................... 16
M3 rack server .................................................. 16
M4 rack server .................................................. 18
  network interface connections ......................... 16
  network interface diagram .............................. 20
SFP+ modules ..................................................... 16
time required .................................................... 15
setup and configuration steps ............................... 14
SFP
  hot-plugged .................................................... 17
SFP Transceiver Module Mini ................................. 8
SFP+ ports ......................................................... 8, 16
Clust ............................................................. 12
  non-Admin ...................................................... 16
unavailable ....................................................... 8
SMTP ............................................................. 13
snapshots
  support .......................................................... 7
SSH
  for support snapshots ...................................... 7
  SSH (inbound) for tgsh-dialog .......................... 12
  SSLv3 disabled ............................................... 49
Start Installation .................................................. 43
Start Support Session .......................................... 5
starting a live support session ............................ 5
starting support mode ........................................ 5
static IP addresses
  using ............................................................ 26
  static network configuration ............................ 26
Submit a Sample .................................................. 53
support ............................................................ 4
  support mode ................................................... 5
  Dirty network ................................................ 5
  support servers ............................................. 6
  support session in normal operations mode .......... 13
  support snapshots ......................................... 7, 13
Support Snapshots ................................................ 7
syslog
  configuration ................................................ 41
  Syslog (outbound) .......................................... 13
tsending syslog messages
  receiving ........................................................ 41
testing the appliance setup ................................ 53
TG5400
  M4 ............................................................... 4
tgsh .............................................................. 12
TGSH Dialog ..................................................... 11
  network configuration, initial ........................... 26
  opening ........................................................ 24
  reconnecting ............................................... 11
tg-tunnel

All contents are Copyright © 2015-2018 Cisco Systems, Inc. and/or its affiliates. All rights reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit outbound traffic</td>
<td>2</td>
</tr>
<tr>
<td>replaced by Network Exit</td>
<td>2</td>
</tr>
<tr>
<td>The appliance is rebooting</td>
<td>45</td>
</tr>
<tr>
<td>Threat Grid</td>
<td></td>
</tr>
<tr>
<td>license</td>
<td>10</td>
</tr>
<tr>
<td>license installation</td>
<td>36</td>
</tr>
<tr>
<td>password</td>
<td>10</td>
</tr>
<tr>
<td>Portal UI</td>
<td>12</td>
</tr>
<tr>
<td>portal UI Help</td>
<td>8</td>
</tr>
<tr>
<td>support</td>
<td>4</td>
</tr>
<tr>
<td>Threat Grid shell</td>
<td>12</td>
</tr>
<tr>
<td>time required</td>
<td></td>
</tr>
<tr>
<td>for setup</td>
<td>15</td>
</tr>
<tr>
<td>to apply configuration settings</td>
<td>29</td>
</tr>
<tr>
<td>TitaniumCloud</td>
<td></td>
</tr>
<tr>
<td>Dirty interface</td>
<td>13</td>
</tr>
<tr>
<td>TitaniumCloud integrations</td>
<td>3</td>
</tr>
<tr>
<td>turning on the appliance</td>
<td>24</td>
</tr>
<tr>
<td>UCS C220 M3 server</td>
<td></td>
</tr>
<tr>
<td>ports</td>
<td>17</td>
</tr>
<tr>
<td>UCS C220 M4 server</td>
<td></td>
</tr>
<tr>
<td>ports illustration</td>
<td>18</td>
</tr>
<tr>
<td>UI traffic</td>
<td>13</td>
</tr>
<tr>
<td>Update Appliance</td>
<td></td>
</tr>
<tr>
<td>updates</td>
<td>47</td>
</tr>
<tr>
<td>installing</td>
<td>47</td>
</tr>
<tr>
<td>updating the appliance</td>
<td>11</td>
</tr>
<tr>
<td>Upload</td>
<td></td>
</tr>
<tr>
<td>encryption key</td>
<td>39</td>
</tr>
<tr>
<td>license</td>
<td>37</td>
</tr>
<tr>
<td>Upload New License</td>
<td>36</td>
</tr>
<tr>
<td>Upload Sample</td>
<td>53</td>
</tr>
<tr>
<td>uploading support snapshots</td>
<td>7</td>
</tr>
<tr>
<td>Upstream Host</td>
<td>40</td>
</tr>
<tr>
<td>user documentation</td>
<td>8</td>
</tr>
<tr>
<td>user interfaces</td>
<td>11</td>
</tr>
<tr>
<td>CIMC</td>
<td>12</td>
</tr>
<tr>
<td>OpAdmin Configuration Portal</td>
<td>12</td>
</tr>
<tr>
<td>TGSH Dialog</td>
<td>11</td>
</tr>
<tr>
<td>Threat Grid Portal</td>
<td>12</td>
</tr>
<tr>
<td>users</td>
<td></td>
</tr>
<tr>
<td>adding</td>
<td>11</td>
</tr>
<tr>
<td>Using DHCP</td>
<td>10</td>
</tr>
<tr>
<td>using DHCP to obtain your IP addresses</td>
<td>26</td>
</tr>
<tr>
<td>Validate</td>
<td></td>
</tr>
<tr>
<td>configuration settings</td>
<td>28</td>
</tr>
<tr>
<td>version lookup table</td>
<td>48</td>
</tr>
<tr>
<td>viewing server health</td>
<td></td>
</tr>
<tr>
<td>using the CIMC interface</td>
<td>57</td>
</tr>
<tr>
<td>VirusTotal integrations</td>
<td>3</td>
</tr>
<tr>
<td>win7-x86 samples</td>
<td></td>
</tr>
<tr>
<td>still available after 2.3</td>
<td>3</td>
</tr>
<tr>
<td>Windows 7</td>
<td></td>
</tr>
<tr>
<td>64-bit only in 2.3</td>
<td>3</td>
</tr>
<tr>
<td>Windows XP</td>
<td></td>
</tr>
<tr>
<td>no longer licensed or distributed</td>
<td>3</td>
</tr>
<tr>
<td>removed in 2.3</td>
<td>3</td>
</tr>
<tr>
<td>winxp samples</td>
<td></td>
</tr>
<tr>
<td>still available after 2.3</td>
<td>3</td>
</tr>
<tr>
<td>wipe process</td>
<td>3</td>
</tr>
</tbody>
</table>