



AMP Threat Grid Appliance Frequently Asked Questions



Last Updated: 9/14/2018
Version 2.5

All contents are Copyright © 2016-2018 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Cover photo Copyright © 2016 Mary C. Ecsedy. All rights reserved. Used with permission.

All contents are Copyright © 2016-2019 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Contents

Threat Grid Appliance Frequently Asked Questions.....	5
What is a Threat Grid appliance?.....	5
Where are the Threat Grid appliance Release Notes?	5
Where are the Threat Grid appliance User Guides?	5
What is the Threat Grid Portal?	5
Where are the Threat Grid Portal Release Notes and Online Help?	5
Where is the API documentation?.....	5
Do Threat Grid appliances need to be connected to the Internet, or can they be air-gapped?	6
Do Threat Grid appliances include Feeds?.....	6
How many samples can we submit per day?.....	6
What are the 3 Interface speed settings?.....	6
Where can I find the Storage Capacity of a Threat Grid Appliance?	6
Does Threat Grid support integration with OpenDNS?	6
Installing Updates	7
What is the Upgrade Path for an Old Threat Grid Appliance?.....	7
The 2.1 Upgrade.....	7
The 2.0.4 Upgrade.....	7
The 2.0 Upgrade.....	7
Upgrading from a Release Prior to 1.4.....	8
The 1.0+hotfix2 Update is Mandatory	8
What file types are supported?	9
What file types are NOT supported?	9
Are there any other file type restrictions?	9
Files should not be empty. Maximum file size is 100MB.....	9
How can I contact Threat Grid Support?	9
What are the main differences between the M3 and the M4 servers?	9

Where can I find information about migrating from an M3 to an M4 server? 10

Why can't we see the OpenDNS 'whois' information in the Domains entity tab on the Analysis Report in the Mask UI of the Portal? 10

Can the Admin and Clean interfaces be connected to the same L2 segment? 10

We have an upcoming maintenance in which the appliance will be powered off. Can we download the configuration for backup in case there is a problem when we power it back on?..... 10

Threat Grid Appliance Frequently Asked Questions

If you have a question and don't see it included in this document, please contact support@threatgrid.com. Thank you!

What is a Threat Grid appliance?

A Threat Grid appliance is a dedicated UCS server (UCS C220-M3 TG5000 or UCS C220-M4 TG5400), which used for local malware analysis backed by the full power of AMP Threat Grid's threat intelligence. It is intended for those organizations with a greater need for data privacy. For example, official agencies or institutions that handle sensitive data under strict privacy policy and other regulatory compliance guidelines, which prevent them from using the AMP Threat Grid Cloud-based solution.

By maintaining a Cisco Threat Grid appliance on-premises, these organizations are able to send potentially harmful documents and files to be analyzed without leaving the security and privacy of their own network.

Where are the Threat Grid appliance Release Notes?

OpAdmin Portal > Operations menu > Update Appliance

Formatted PDF version available online: Threat Grid Appliance Install and Upgrade Guides page on the Cisco website.

Where are the Threat Grid appliance User Guides?

Threat Grid Appliance user documentation is available on the Threat Grid Appliance Install and Upgrade Guides page on the Cisco website.

What is the Threat Grid Portal?

The Web-based interface to Threat Grid.

Where are the Threat Grid Portal Release Notes and Online Help?

Located under the Help menu on the navigation bar.

Where is the API documentation?

API documentation is available from the main Help page on the Threat Grid Portal.

Do Threat Grid appliances need to be connected to the Internet, or can they be air-gapped?

Although it is technically possible to run a Threat Grid appliance without Internet access, Internet access is required for the malware analysis to be effective. Without access, the analysis results will be greatly diminished, as some malware requires contact to its C2 server, SMTP server, etc.

Do Threat Grid appliances include Feeds?

No. Threat Grid appliances do not include the AMP Threat Grid Curated Feeds.

How many samples can we submit per day?

The maximum number of files analyzed per day is based on the AMP Threat Grid appliance license is as follows:

- Cisco AMP Threat Grid 5000 and 5004: 1,500 samples
- Cisco AMP Threat Grid 5500 and 5504: 5,000 samples.

What are the 3 Interface speed settings?

clean/dirty are 1Gb max, while admin can go up to 10Gb depending on how it's connected and what it's connected to

Where can I find the Storage Capacity of a Threat Grid Appliance?

OpAdmin > Configuration > Storage

Does Threat Grid support integration with OpenDNS?

Yes. In the new Analysis Report in the Portal Mask UI (version 3.4.36), the Domain page now includes OpenDNS `WHOIS` information.

Installing Updates

Before you can update the Threat Grid Appliance with newer versions, you must have completed the initial setup and configuration steps as described in the AMP Threat Grid Appliance Setup and Configuration Guide, which are available on the AMP Threat Grid Appliance product documentation page.

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

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

Threat Grid Appliance updates are applied through the OpAdmin Portal.

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

Updates are automatic. However, to verify that you have the most recent version, we recommend that you check again manually right away for new updates as soon as the latest one is completed, because sometimes there is a slight lag.

To test the update, submit a sample for analysis.

What is the Upgrade Path for an Old Threat Grid Appliance?

The upgrade path for old appliances is 1.0 -> 1.0+hotfix2 -> 1.4.6 -> 2.0.4 -> 2.1 -> 2.1.3

The 2.1 Upgrade

You must be at version 2.0.4 before you can upgrade to version 2.1.

The 2.0.4 Upgrade

You must be at version 1.4.6 or newer before you can complete the 2.0.4 update.

The 2.0 Upgrade

First, complete the 1.4.6 upgrade, which is the immediate step before 2.0.

After the 1.4.6 upgrade is complete, and before continuing on to the 2.0 upgrade, check the notices in the Threat Grid Portal to verify whether or not the following error has occurred:

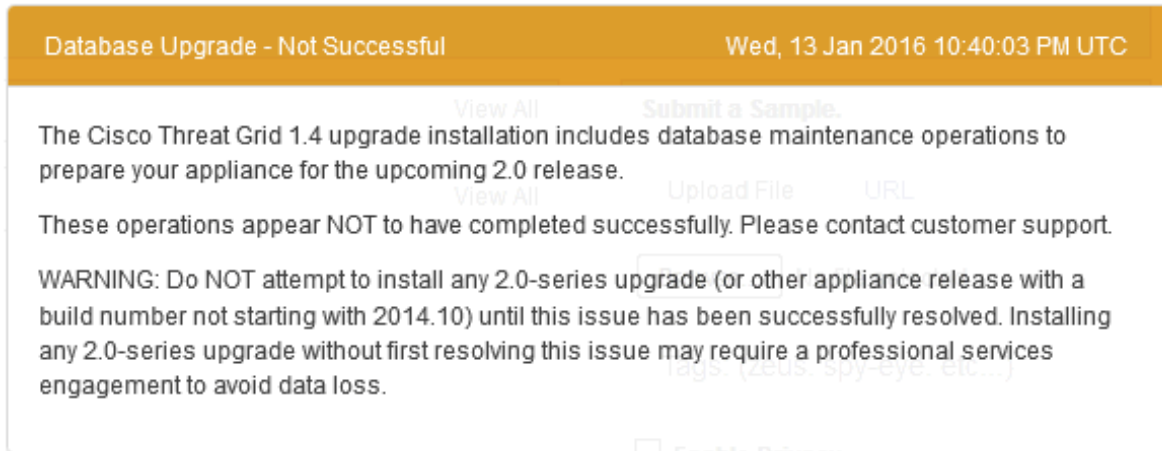


Figure 1 Database Upgrade Not Successful Notice

A "Database Upgrade - Not Successful" message means that a new appliance is running an older version of PostgreSQL than it's supposed to, and the automatic database migration process has failed.

If you do not see the error notice, then you may proceed with the 2.0 upgrade.

Time Required for 2.0 Upgrade

Please note that the 2.0 upgrade can take some time - up to several hours - with a large ElasticSearch database.

DO NOT interrupt the upgrade before it is completed, as doing so may require support remediation. The best method for checking on the status of an ongoing upgrade is via console access.

Upgrading from a Release Prior to 1.4

If upgrading from a release prior to 1.4, be sure to read the section in the release notes.

The 1.0+hotfix2 Update is Mandatory

The 1.0+hotfix2 is a mandatory update that fixes the update system itself to be able to handle large files without breaking.

NOTE: This update is only required when downloading updates over the Internet. Air-gapped (media) updates do not share this requirement.

What file types are supported?

The list of sample file types that can be submitted to Threat Grid for analysis is updated frequently. For the current list please see the file, *Sample File Types*, which may be found listed on the Portal online Help. If you need to be able to use a particular file type and don't see it on that list – or you would like to verify its status – please contact Threat Grid Support (support@threatgrid.com).

What file types are NOT supported?

Other file types will be rejected by the malware sandbox upon submission, and flagged with "Filetype not supported" in the Threat Grid portal interface and the API.

NOTE: .TXT is NOT supported.

Also, Threat Grid does not analyze email headers. We do look at the body and essentially treat it as a network artifact, so there are some checks run on it. For example if a file is emailed.

Are there any other file type restrictions?

Yes:

- Sample filenames cannot be more than 59 Unicode characters in length.

Files should not be empty. Maximum file size is 100MB. How can I contact Threat Grid Support?

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

Email: support@threatgrid.com

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.

Call - See: <http://www.cisco.com/c/en/us/support/index.html>

What are the main differences between the M3 and the M4 servers?

The C220-M4 upgrade (in November, 2016) consists primarily of a hardware refresh, and the addition Secure Boot. Threat Grid will continue providing support for M3s until after the expiration of their contracted lifespan. All the same features on the M4 are available as over-the-wire updates for existing M3s.

Where can I find information about migrating from an M3 to an M4 server?

We strongly encourage existing M3 and M4 customers to contact us directly at support@threatgrid.com to discuss any questions you may have about which server upgrade is best for your needs, about data migration, backups, rollout strategies, etc.

Why can't we see the OpenDNS 'whois' information in the Domains entity tab on the Analysis Report in the Mask UI of the Portal?

If the integration with OpenDNS is not configured in the OpAdmin Integrations Configuration page (**OpAdmin > Configuration > Integrations**), then the OpenDNS 'whois' details will not be visible in the Mask Analysis Report Domains entities page.

Can the Admin and Clean interfaces be connected to the same L2 segment?

As long as your network practices don't call for them to be separate, it's fine as far as the Threat Grid appliance is concerned. Unlike Dirty, the decision of whether to segment Admin and Clean is up to you.

We have an upcoming maintenance in which the appliance will be powered off. Can we download the configuration for backup in case there is a problem when we power it back on?

A support snapshot will include the system's configuration.