AMP Threat Grid Appliance Frequently Asked Questions

Last Updated: 1/19/2017

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.

Contents

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 or UCS C220-M4) 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 AMP 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?

Support for OpenDNS is being discussed but is not yet road-mapped. The Threat Grid Cloud will probably be the first point of integration.

Upgrading a Threat Grid Appliance

Build Number/Release Version Lookup Table

Build Number	Release Version	Release Date	Notes
2016.05.20170105200233.32f70432.rel	2.1.6	1/7/2017	LDAP Authentication support for OpAdmin/tgsh-dialog
2016.05.20161121134140.489f130d.rel	2.1.5	11/21/2016	ElasticSearch5; CSA performance fix
2016.05.20160905202824.f7792890.rel	2.1.4	9/5/2016	Primarily of interest to Manufacturing
2016.05.20160811044721.6af0fa61.rel	2.1.3	8/11/2016	Offline update support key, M4 wipe support
2016.05.20160715165510.baed88a3.rel	2.1.2	7/15/2016	
2016.05.20160706015125.b1fc50e5.rel-1	2.1.1	7/6/2016	
2016.05.20160621044600.092b23fc	2.1	6/21/2016	
2015.08.20160501161850.56631ccd	2.0.4	5/1/2016	Starting point for the 2.1 update. You must be at 2.0.4 before you can update to 2.1.
2015.08.20160315165529.599f2056	2.0.3	3/15/2016	Introduces AMP integration, CA mgmt., and split DNS
2015.08.20160217173404.ec264f73	2.0.2	2/18/2016	
2015.08.20160211192648.7e3d2e3a	2.0.1	2/12/2016	
2015.08.20160131061029.8b6bc1d6	v2.0	2/11/2016	Force update to 2.0.1 from here
2014.10.20160115122111.1f09cb5f	v1.4.6	1/27/2016	Starting point for the 2.0.4 update
2014.10.20151123133427.898f70c2	v1.4.5	11/25/2015	
2014.10.20151116154826.9af96403	v1.4.4		

Build Number	Release Version	Release Date	Notes
2014.10.20151020111307.3f124cd2	v1.4.3		
2014.10.20150904134201.ef4843e7	v1.4.2		
2014.10.20150824161909.4ba773cb	v1.4.1		
2014.10.20150822201138.8934fa1d	v1.4		
2014.10.20150805134744.4ce05d84	v1.3		Important networking change: Prior to v1.3, ALL OUTBOUND is on the DIRTY INTERFACE. v1.3 introduces support for email on the Clean Interface. If you have previously incorporated a workaround, please review to see if it is still compatible with v1.3.
2014.10.20150709144003.b4d4171c	v1.2.1		
2014.10.20150326161410.44cd33f3	v1.2		
2014.10.20150203155143+hotfix1.b06f7b4f	v1.1+hotfix1		Force update from 1.1 NOTE: Only required when downloading updates over the Internet. Air-gapped (media) updates do not share this requirement.
2014.10.20150203155142.b06f7b4f	v1.1		

Build Number	Release Version	Release Date	Notes
2014.10.20141125162160+hotfix2.8afc5e2f	v1.0+hotfix2		Force update from 1.0 **NOTE:** The 1.0+hotfix2 is a **mandatory update** that fixes the update system itself to be able to handle large files without breaking. Only required when downloading updates over the Internet. Air-gapped (media) updates do not share this requirement.
2014.10.20141125162159+hotfix1.8afc5e2f	v1.0+hotfix1		
2014.10.20141125162158.8afc5e2f	v1.0		

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:

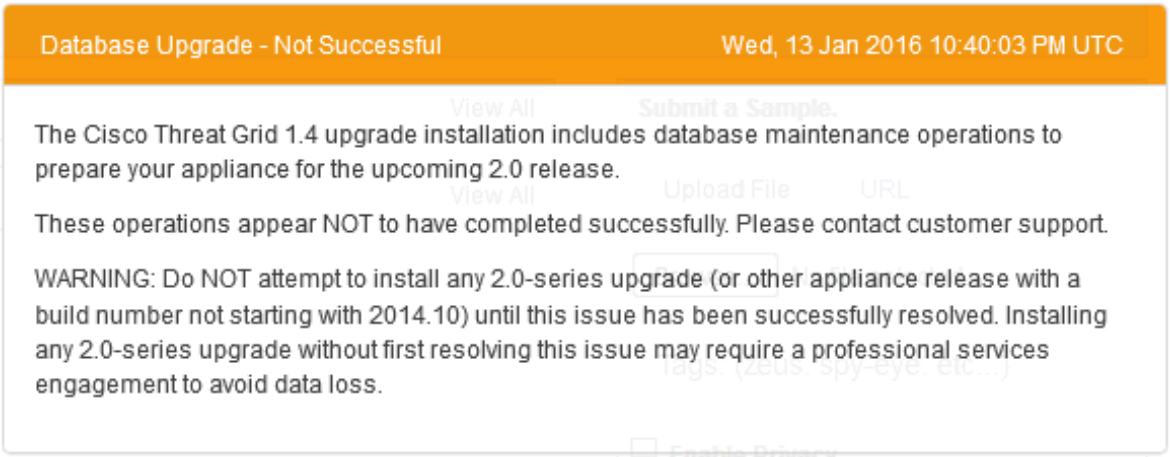

Figure 1 Database Upgrade Not Successful Notice

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 following file types may be submitted to Threat Grid for analysis:

- PE32 Files (detailed static forensics):
  - Executables (.EXE)
  - Libraries (.DLL)
- PE32+ files -- Available on the win7-x64 VM ONLY:
  - Executable (.EXE)
  - Libraries (.DLL)
- Java Archives (.JAR)

Note: JAR is a very imprecise filetype. The original Threat Grid file acceptance system would take anything that met the bare requirements for a JAR file, but our new one, PREP2, which was introduced in the [3.4.34 release](/doc/main/release_notes.html#3-.-4-.-34), does not. Instead, the new preparation process now checks further to see if the item actually meets the requirements of a child format for JAR (such as the Android APK files), which are JAR files, but will not run in the Threat Grid environment. Unfortunately, this means that what may look like a JAR file may actually be intended for the user's phone, not for Windows.

Therefore, we no longer accept APK files. Although they might look like JAR files, they just won't run in Threat Grid.

- JavaScript (.JS) -- Note that the file MUST have the .js extension.
- Portable Document Format (.PDF) (detailed static forensics, including Javascript resources) -- Please note changes to PDF handling in the 3.4.34 Portal Release Notes.
- Office Documents (.DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX) (limited static forensics)
- XML Based Office Document Types (.DOCX, .XLSX, .PPTX)
- XML - Extensible Markup Language (.XML)
  - XML that is from Office will be opened in the corresponding program (Office 2K3)
  - All other XML will be opened in IE
- Archive and Quarantine Formats:
  - ZIP (.ZIP) as a container, no nesting of archives, no password or 'infected'. We do not support nested ZIP archives due to known unpacking attacks, such as zip bombs and quines, including 42.zip, which is a well-known attack against AV services.
  - ZIP archives may contain a maximum of 100 files. Archives with more than 100 files will return no analysis, and will display an error stating that too many files were found. The maximum file size for each file within the ZIP archive is 25MB.

  - Quarantine (.VBN, .SEP)
  - xz (.xz), gzip (.gz), bzip2 (.bz2), tar (.tar) -- Note that the file MUST have the appropriate extension.
- Mime HTML Files (.MHTML)
- Flash Files (.SWF)
- URLs (As Internet Shortcut file, or submit the URL directly. Detailed static forensics or Javascript resources.)
- MSI - Microsoft Installer files (.MSI)
- LNK - Windows shortcut files (.LNK)
- Available on the win7-x64-jp VM ONLY (specific to Ichitaro). IMPORTANT NOTE - Not Available On Threat Grid Appliances:
  - .JTD, .JTT, .JTDC, .JTTC
- Available on the win7-x64-kr VM ONLY (specific to Hancom Office). IMPORTANT NOTE – Not Available On Threat Grid Appliances:
  - .HWP, .HWT, .HWPX
- Batch (.BAT) -- Note that the file MUST have the .bat extension.
- HTML Application (.HTA) -- Note that the file MUST have the .hta extension.
- Powershell (.PS1) -- Note that the file MUST have the .ps1 extension.
- Visual Basic Script (.VBS) -- Note that the file MUST have the .vbs extension.
- Windows Script File (.WSF) -- Note that the file MUST have the .wsf extension.
- Encoded JavaScript (.JSE) -- Note that the file MUST have the .jse extension.
- Encoded Visual Basic (.VBE) -- Note that the file MUST have the .vbe extension.
- Compiled HTML Help (.CHM) -- Microsoft Compiled HTML Help.

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.
- File size can be 0 bytes (i.e., empty), and no greater than 100MB in size.

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.