Release Notes for Cisco Threat Grid Appliance Version 2.15

First Published: 2021-09-24

Last Modified: 2022-01-27

Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.15.

It also includes the Release Notes and What's New for Cisco Threat Grid Portal software version 3.5.89.

User Documentation

The following Threat Grid Appliance user documentation is available:

Threat Grid Appliance User Documentation

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

Note Newer documentation is being made available from the Threat Grid appliance Products and Support page.

Backup FAQ

Please see the Backup Notes and FAQ for technical information and instructions.

Clustering Overview and FAQ

Please see the Clustering Overview and FAQ for additional 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 inthe AMP Threat Grid Appliance Setup and Configuration Guide, which are available on the Threat Grid Appliance Install and Upgrade Guides page on the Cisco website.

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

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

Threat Grid Appliance updates are applied through the OpAdmin Portal.

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

To test the update, submit a sample for analysis.

Version Information

Version 2.15.0ag

- Release Date: September 28, 2021
- Build Number: 2021.08.20210928T204235.srchash.a6fc1fe6a633.rel
- One-off with support for direct airgap upgrade from 2.11.4.

Version 2.15.0

- Release Date: September 24, 2021
- Build Number: 2021.08.20210924T181619.srchash.e20146e4ccbd.rel
- Refreshes to 3.5.89, SOCKS5, email test button, cluster licenses.

Fixes and Updates

Version 2.15.0

This release updates the core application software and adds a variety of fixes and enhancements:

- The core application software has been updated to match cloud version 3.5.89. Notably, this uses an enhanced disk-analysis engine that improves both analysis speed and quality of results.
- A SOCKS5 proxy can now be used for downloading updates.
- The Admin UI now provides a button which can be used to send a test email, permitting validation of configured SMTP settings.
- Newly-installed licenses are now immediately reflected in available quota, without requiring reconfiguration. (This is coupled with changes that will allow other license-related enhancements.)
- When downloading updates, newly-downloaded content (including optional VM images when enough space exists) is mirrored to the OS drive array, rather than stored only on the data array. Moreover, this mirror is checked for errors, and any corrupted files are replaced. This improves robustness against failures and reduces the amount of preparation required for the data-reset operation, at the cost of more time being required for update downloads to finish.1
- 3DES-based ciphers are no longer permitted during TLS negotiation with the core Threat Grid application, avoiding the potential for downgrade attacks. This fixes a regression introduced with appliance release 2.13.0.

- The Admin UI has had several minor improvements. Among these:
    - The Admin UI now provides a visual cue to allow users to understand whether a RADIUS private key has been installed.
    - Empty notifications which could sometimes be displayed are removed.
    - During password changes, text can no longer be modified while changes are actively being saved.
-

Known Issues

- Like its immediate predecessor, this release creates backup copies of the VM images on the RAID-1 storage array, to be used in the event of a reset following a bulk-storage failure. Early Cisco Threat Grid Appliance models (based on the UCS C220-M3 platform) have less storage than later models, and are more likely than other units to have less than 25% of disk space remaining available on the RAID-1 filesystem after installing this release, which will trigger a service notice.

  For later model hardware, being at less than 25% remaining storage on the RAID-1 array after installing this release is abnormal and may be raised to customer support.

  Starting with the 2.12 release, the amount of hard drive space is constant for a given release. The only differences across machines relate to whether they have the optional JP/KR control subjects licensed. (Note that this applies to the OS drive array. The data array's usage will vary depending on the appliance's history, number of samples, etc.)
- Firmware updates may sometimes fail to apply during the update process itself. Should this happen, these updates will be retried during the reboot process following any successful reconfiguration run.

Threat Grid Portal Release Notes and What's New

This section includes the release notes and what's new for Cisco Threat Grid Portal.

Threat Grid Portal Release 3.5.89

First released to Threat Grid Cloud portal on August 12, 2021.

Fixes and Updates

- Adds a **Theme** toggle to the **My Account** dropdown, as a convenient way for you to select a **Light** or **Dusk** background color.

Behavioral Indicators

- 3 New Behavioral Indicators.
- 10 Modified Behavioral Indicators.

What's New

For detailed information about what's new in Threat Grid Portal release 3.5.89, see the online Help.