Release Notes for Cisco Threat Grid Appliance Version 2.10

First Published: 2020-01-28

Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.10.

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 2.10

Release Date: January 28, 2020

Build Number: 2019.12.20200128T085836.srchash.5bec2ec5b74c.rel

This release updates core Threat Grid software to follow the cloud 3.5.45 release; introduces support for RADIUS-based authentication for both appliance administration and application use; fixes a critical bug in password reset automation; and improves Elasticsearch behavior under heavy load.

Fixes and Updates

The following fixes and updates are included in Version 2.10:

- The core Threat Grid application is updated to release 3.5.45.
- Support for RADIUS authentication (using Cisco Identity Services Engine with DTLS enabled) is introduced.
- The **exit** command no longer needs to be run before reboot (from tgsh in recovery mode) for a password reset to take effect.
- A bug wherein licenses containing literal single-quote characters could fail to validate is addressed.
- Adjustments have been made to how Elasticsearch behaves when the queue of search operations exceeds its allowed length.
- The application of airgap updates will no longer fail if the installed license has expired, as long as an unexpired (and otherwise valid) license is present on the update media.
- The mechanism by which file ownership and permissions are enforced during an upgrade has been enhanced to ensure consistency across upgrade paths and usage scenarios.

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.
- 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. A future release may provide a service notice when this has occurred.