Release Notes for Cisco Secure Malware Analytics Appliance (formerly Threat Grid Appliance) Version 2.17

First Published: 2022-01-17

Last Modified: 2022-06-14

Introduction

This document describes the new features, open issues, and closed issues in Cisco Secure Malware Analytics (formerly Threat Grid) Appliance Version 2.17.0

It also includes the Release Notes and What's New for Secure Malware Analytics portal software version 3.5.96.

User Documentation

The following Secure Malware Analytics (formerly Threat Grid) appliance user documentation is available:

Secure Malware Analytics Appliance User Documentation

Appliance user documentation is available on the Secure Malware Analytics appliance Install and Upgrade Guides page on the Cisco website.

Note Newer documentation is being made available from the Secure Malware Analytics 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 Secure Malware Analytics (formerly Threat Grid) appliance with newer versions, you must have completed the initial setup and configuration steps as described in the Appliance Setup and Configuration Guide, which are available on the Secure Malware Analytics 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.

Secure Malware Analytics Appliance updates are applied through the Admin UI 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 2.17.5

- Release Date: June 13, 2022
- Build Number: 2021.10.20220613T181318.srchash.ba4790fd75bb
- Fix appliance-doc release notes; Prevent M3s from getting new updates

Version 2.17.4

- Release Date: April 04, 2022
- Build Number: 2021.10.20220404T165213.srchash.f85f63a3cb59.rel
- ClamAV update; admin email address fix; firmware update check fix

Version 2.17.3

- Release Date: February 08, 2022
- Build Number: 2021.10.20220208T191641.srchash.c739ce59e223.rel
- kr VM update only

Version 2.17.2

- Release Date: January 26, 2022
- Build Number: 2021.10.20220126T220840.srchash.080c9309ed0b.rel
- ClamAV update; ES update; release notes rendering fix

Version 2.17.1

- Release Date: December 17, 2021
- Build Number: 2021.10.20211217T224748.srchash.c6eec0c8e294.rel
- Separate sync threads for each index type; cowboy sync service

Version 2.17.0

- Release Date: December 16, 2021
- Build Number: 2021.10.20211216T214940.srchash.e04020089b8c.rel
- Refresh to 3.5.96.

Fixes and Updates

Version 2.17.5

This release adds missing release notes for the 2.17.x series and is the final release for M3-based appliances.

- For more information on the end of software support for M3-based appliances, see End-of-Sale and End-of-Life Announcement for the Cisco AMP Threat Grid 5000 and 5500 Appliances

Version 2.17.4

This release updates ClamAV and the core application software.

- Updates ClamAV from 0.103.4 to 0.103.5.
- Addresses an issue that prevents certain email address domains from being used for admin roles in the application UI.
- Prevent spurious service notices about failed firmware updates.

Version 2.17.3

This release updates the Korean VM image to address a font-rendering issue.

- Only affects the customers with the Korean VM. Customers who are already on 2.17.2 and do not have the Korean VM enabled do not need this update.

Version 2.17.2

This release updates a few components aligning with upstream releases and allowing ongoing signature database updates. You must update the appliance to this release (or later) to continue receiving signature database updates.

- Updates the underlying Elastic Search release to 6.8.22 (from a locally patched variant of 6.8.20, which was effectively equivalent to the upstream 6.8.21 release).
- Updates ClamAV from 0.102.4 to 0.103.4, allowing new definitions to be used.
- Addresses an issue that could prevent release notes for a downloaded update from being displayed in the administrative interface.

Version 2.17.1

Fixes an issue that excludes the newly added data in the search results until the old data is reindexed (happens for 2.16.0 or later)

- Each class of data indexed for search now has its queues processed independently. The indexing of new samples are not blocked until other classes of data (like dispositions or report summaries) are fully indexed.
- Adds the 'cowboy-sync' service necessary for cases that requires manually trigger reindexing of old data, or to start a separate process indexing incoming data while old data is still being handled. For more information regarding its appropriate usage, contact customer support.

Version 2.17.0

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 3.5.96. Among numerous other enhancements, artifacts that were deleted or encrypted during sample execution can now be downloaded.
- ElasticSearch is upgraded to version 6.8.20, with some additional patches applied.
- Fixes a bug that stops the bootloader from updating after installing a new appliance release.
- Fixes minor issues that could lead to spurious error messages during the boot and configuration process.

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.

Secure Malware Analytics Portal Release Notes and What's New

This section includes the release notes and what's new for the Cisco Secure Malware Analytics (formerly Threat Grid) Portal.

Secure Malware Analytics (formerly Threat Grid) Portal Release 3.5.96

First released to Secure Malware Analytics Cloud portal on November 18, 2021.

Fixes and Updates

- Adds an **Options Template** that allows you to save frequently used options for easy reuse when you Submit Samples to Secure Malware Analytics for analysis.

Behavioral Indicators

- 8 New Behavioral Indicators.
- 3 Modified Behavioral Indicators.
- 2 Retired Behavioral Indicators.

What's New

For detailed information about what's new in Secure Malware Analytics release 3.5.96, see the online Help.