# Release Notes for Cisco Secure Malware Analytics Appliance (formerly Threat Grid Appliance) Version 2.16

**First Published:** 2021-10-27

**Last Modified:** 2022-01-18

## Introduction

This document describes the new features, open issues, and closed issues in Cisco Secure Malware Analytics (formerly Threat Grid) Appliance Version 2.16.

It also includes the Release Notes and What's New for Secure Malware Analytics portal software version 3.5.92.

## 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 2.16.3

- Release Date: December 06, 2021
- Build Number: 2021.09.20211206T201821.srchash.cbcc16d1dec1.rel
- Fixes 2.16.2 migration support for appliances w/ very large numbers of indices

### Version 2.16.2ag

- Release Date: November 20, 2021
- Build Number: 2021.09.20211202T023412.srchash.63318d710bc8.rel
- One-off with support for direct airgap upgrade from 2.11.4.

### Version 2.16.2

- Release Date: October 27, 2021
- Build Number: 2021.09.20211129T222728.srchash.c6f610e1458e.rel
- Support for upgrading from 2.11.4; fix ES index name migration

### Version 2.16.1

- Release Date: November 12, 2021
- Build Number: 2021.09.20211112T203609.srchash.ec656ef64ba7.rel
- RADIUS fix. Some tgsh-tui cosmetic enhancements. Report fs types to update server.

### Version 2.16.0

- Release Date: October 27, 2021
- Build Number: 2021.09.20211027T202636.srchash.d964c8041222.rel
- Refresh to 3.5.92. Rebrand. Replace tgsh-dialog with tgsh-ui. Socket activation. gocryptfs 2.x.

# Fixes and Updates

### Version 2.16.3

This release patches the data migration reimplemented in 2.16.2 to fix support for appliances with an exceptionally large number of Elasticsearch indices.

**Note** This release is not required for any customer that already has 2.16.1 or 2.16.2 installed and is not experiencing a fault that makes their appliance inoperable.

### Version 2.16.2

This release provides additional support for an Elasticsearch data migration that was performed for most customers during the legacy 2.13.x release series.

Customers who skipped the 2.13.x release series in order to avoid a bug that could leave an appliance unusable in the presence of a hardware fault (which is now harmless with newer software releases), may have missed the Elasticsearch migration. If this issue is present, the core application software is unable to start. The 2.16.2 release resolves this issue.

**Note** This release is not required for any customer that already has 2.16.1 installed and is not experiencing a fault that makes their appliance inoperable.

- Direct upgrades from 2.11.4 are now supported, unlike prior 2.16.x releases.

**Note** **IMPORTANT:** A data-loss scenario has been observed while a standalone appliance is being transformed into the initial node of a cluster. This is not newly introduced in 2.16.2, and can be observed in several prior releases as well. Until a release is published that is explicitly documented to resolve this concern, clusters should be created by initially installing the first node as a single-node cluster, rather than installing a standalone node and later promoting it to a cluster.

### Version 2.16.1

This release fixes an unintended change in RADIUS authentication, and makes several cosmetic enhancements to the new textual UI on tty1 introduced with 2.16.0. It also adds some additional metadata to the update-server handshake in preparation for appliance 3.0.

- In 2.16.0, the NAS-Identifier passed to a configured RADIUS server for login attempts from the core Secure Malware Analytics application changed from `Threat Grid UI` to `Malware Analytics UI`. This point release reverts to the old name, for compatibility with both documented configuration guidelines and preexisting installations.
- When communicating with the update server, the system now conveys the type of filesystem used for both OS and data drives. This allows the update server to determine whether a given appliance will be

able to install appliance 3.0 without a data reset operation; the information gathered may be used to contact customers with guidance on how to prepare their system for upgrade to 3.0, where required.

- Several changes to the new textual UI on tty1 have been made:
  - A dark blue color that could be difficult to read has been replaced with a light cyan.
  - A bug which prevented some configuration fields from being cleared if previously set to a non-empty value has been addressed.
  - Debugging information visible in the textual UI has been cleaned up and is no longer exposed.
  - System logs are now routed to tty7 on the console, preventing them from overlaying the menu on tty1.

### Version 2.16.0

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 3.5.92.
- License enforcement is updated. Expired licenses cannot be installed, but having one installed will not block reconfiguration actions in the Admin UI. (As always, appliances with expired licenses present a service notice and cannot download updates, and expired _demo_ licenses prohibit samples from being run).
- The legacy **tgsh-dialog** textual UI has been replaced with a modern **tgsh-ui** replacement which interacts with the same backend server as the web UI administrative interface.
- Restarts of core application services are now less disruptive to clients: To the extent possible, HTTP requests will be queued and passed to the new instance when it has fully started up and is ready to handle requests.
- The software used for encrypting NFS storage has been updated to a release with a lower-overhead backend.
- The freezer-backup-bulk service no longer uses an aggressively parallel implementation; the number of files it attempts to concurrently read and write is dramatically reduced.
- The Admin UI now reflects more detailed status for support mode: Not just whether the service is running, but also whether it has actually succeeded in connecting to the support servers; and if it has, which server it is connected to.
- The **tg-backfill** service (generating Advanced Search indices for data first created using appliance versions that predate Advanced Search) has been removed, as Advanced Search has been available since the 2.11.x release series.

## 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 3.5.92

First released to Secure Malware Analytics Cloud portal on September 23, 2021.

### Fixes and Updates

- **Sample Manager** - Adds drag and drop functionality that allows you to customize the display order of the table columns in the sample manager.
- Login via Cisco Security Accounts is now disabled. It is replaced with SecureX Sign-On.

### Behavioral Indicators

- 8 New Behavioral Indicators.
- 7 Modified Behavioral Indicators.

### What's New

For detailed information about what's new in Secure Malware Analytics release 3.5.92, see the online Help.