Release Notes for Cisco Secure Malware Analytics Appliance (formerly Threat Grid Appliance) Version 2.20

First Published: 2026-05-13

Last Modified: 2026-05-13

Introduction

This document describes the Release Notes, and Known Issues in Cisco Secure Malware Analytics (formerly Threat Grid) Appliance Version 2.20.0.

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.

Fixes and Updates

Version 2.20.0

- Core application updated to cloud version 3.5.149.
- Default PostgreSQL version upgraded to 13.5, with an upgrade tool provided for multi-node clusters.
- ElasticSearch version upgraded to 7.17.
- Added a confirmation prompt before initiating an update.
- Appliance serial number is now constantly visible in the upper right corner of the OpAdmin interface.
- Added Prometheus data, logs, and OpAdmin clj output to support snapshots.
- Increased PostgreSQL database backup retention to 10 backups, taken every other day.
- Disabled transparent_hugepage without using a signed command to avoid performance degradation during bursts of submissions.
- Enhanced clustering menu to support PostgreSQL upgrade.
- Improved administrator documentation in OpAdmin.
- Added a note that a reboot is necessary after reconfiguration when activating a new OpenDNS key.
- Fixed restore from NFS for emergency recovery of a cluster.
- Fixed an issue where the connection failure page would appear during reboot to apply an update.
- Fixed flag API operations.
- Fixed an issue causing "Date out of range" to appear in the "Close On" field when viewing service notice details.
- Restricted ciphers and HMACs to mitigate CVEs.
- Blocked new certificates with SHA-1 hashes or abnormally large RSA keys (>8192 bits) from being configured in OpAdmin as a mitigation for CVE-2023-39533.
- Fixed an issue where changes to RADIUS authentication certificates or keys would not apply without a reboot.
- Fixed service notices being created for consul-transient and consul-tiebreaker when they should not be.

- Fixed an issue where changes to Notification settings would not apply without a reboot.
- Added NFS statistics on the storage status page.
- Fixed OpenDNS configuration changes to take effect without a reboot.

Known Issues

- Failure during Elasticsearch migration: After updating, if the appliance is reconfigured while Elasticsearch migration is underway, the migration may fail. Avoid reconfiguring until the Elasticsearch Migration service notice is cleared. If migration fails due to reconfiguration, retry via the shell/console using the command service restart elasticsearch-migrate-precheck. Ensure no further reconfiguration is performed until migration completes, as it may cause repeated failures. If you cannot access the shell/console, please contact support. See CSCwu05983 in CDETS for more information.

Upgrade Notes

- This release includes an upgrade of the PostgreSQL database on the appliance. Standalone nodes and clusters with only one node will be automatically upgraded upon updating the appliance to version 2.20.0. However, multi-node clusters require manual intervention by the administrator in OpAdmin once all appliances in the cluster have been updated to 2.20.0. Refer to the 2.20.0 administration manual for detailed procedures.
- The upgrade requires ElasticSearch index migration, which the appliance performs automatically once all cluster nodes are upgraded to 2.20.0. During migration, API-reported submission statuses may lag while the current month's index is updated; such delays should resolve within a few hours after migration begins. After successful index migration, the system should be rebooted during a maintenance window.
- Note that although creation of new certificates with SHA-1 hashes or abnormally large RSA keys (>8192 bits) is not allowed in OpAdmin, any existing certificates will continue to function with a warning.
- Customers must ensure their VirusTotal (VT) API key supports the /api/v3/intelligence/search endpoint as of release 2.20.0. For details on VT API keys, please refer to the VirusTotal's official documentation.

Early Warning Advisory

- Starting with Secure Malware Analytics 3.0.0 release and later, NFS will only be supported on RHEL and Ubuntu-based distributions.