Release Notes for Cisco Threat Grid Appliance Version 2.13

First Published: 2021-06-14

Last Modified: 2021-07-23

Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.13.

It also includes the Release Notes and What's New for Cisco Threat Grid Portal software version 3.5.74.

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 2.13.2

- Release Date: July 23, 2021
- Build Number: 2021.01.20210723T002541.srchash.a3363aac9927.rel
- Fixes ES migration issue, inability to disable accounts.

Version 2.13.1

- Release Date: July 9, 2021
- Build Number: 2021.01.20210709T162338.srchash.a5569640efad.rel
- Includes miscellaneous fixes to issues and security updates; enables Documentation in Admin Portal; drops nginx.

Version 2.13.0

- Release Date: June 24, 2021
- Build Number: 2021.01.20210614T213034.srchash.49f47ced5638.rel
- Refreshes to 3.5.74, includes preparation for ES v6 to v7 migration.

Fixes and Updates

Version 2.13.2

This release includes the following fixes and updates:

- An issue that could prevent the core application from starting successfully after installing a v2.13.x release on a system with search indexes lacking a date component has been resolved.

Note For customers who have already upgraded successfully to appliance 2.13.1, and who do not know that they are impacted by one of the bugs addressed below, 2.13.2 may not be necessary. When 2.14.0 is released (in the near future), it will be installable as an update directly from 2.13.1, without 2.13.2 as a mandatory prerequisite.

- A regression which could prevent user accounts from being disabled has been addressed.

Version 2.13.1

This release includes the following fixes and updates:

- An error that could cause Elastic Search data migration to fail has been addressed.
- A regression in OpenDNS Investigate support that prevented configuration from being successfully read has been corrected.
- A race condition whereby the UI could attempt to display data for a sample before that sample is reflected in the database has been addressed.
- Product documentation is now built into the appliance for viewing in a web browser, under the **Documentation** tab in the administrative interface. The documentation included with this release is somewhat less comprehensive than the version on cisco.com; this will be addressed over time.
- Disabling the interface actively being used for NFS (which would typically cause an appliance to hang or otherwise fail) is no longer possible in the Admin UI when the admin interface is disabled and the clean interface is being used for NFS.
- Previously, the Admin UI would throw an error when (as by default) the list of email addresses to send notifications to was empty, but notification frequency was not set to None. As of this release, having an empty recipient list for notifications automatically disables the frequency selection drop-down menus.
- The frontend web server is now Traefik. Not only is this significantly newer than the version of Nginx that was previously shipped, but it changes the underlying TLS implementation from OpenSSL to Google's Go crypto/tls.
- The operating system kernel has been updated (to Linux 4.19.193 during general operation, and Linux 5.10.44 during early boot).

Version 2.13.0

This release includes the following fixes and updates:

- The core application software has been updated to match cloud version 3.5.74.
- Custom SSH Timeouts are now configurable via the administrative user interface.
- Administrative users are now able to set a custom *Message Of The Day* style SSH and web interface banner text that will be displayed to users when they complete authentication.
- DTLS library for RADIUS proxy has been updated to fix some bugs.
- Elasticsearch migration work in anticipation of updating ES from ES6 to ES7.
- Enabled Threat Grid Search API v3 on appliances.
- OpenDNS integration is now native and no longer running as a separate service.
- React components used for the administrative user web interface has been updated.
- The clustering interface will no longer appear as operable when it is not connected on an appliance and the option to enable clusters will be disabled if the cluster interface is not properly cabled.

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.

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 3.5.74

First released to Threat Grid Cloud portal on January 14, 2021.

Fixes and Updates

- **Device Groups** - This release introduces a new feature, Device Groups. Devices such as Cisco Email Security Appliances, Web Security Appliances, and more, can be added to one or more groups for the purpose of setting rate limits. The Org Admin or Device Admin user can apply a single rate limit to multiple devices at the same time by creating a group with a rate limit and adding devices to it.

  - **Devices Page** - Adds enhancements to support the device groups feature. To open this page as the Device Admin, click the **Administration** tab and choose **Devices**. You can also access this page as an Org Admin by entering the URL directly.

    New features include the ability to filter by the Device user type, a new **Device Groups** column, and a **Manage Groups** link.

  - **Device Groups Page** - A new **Device Groups** page that allows Org Admins and Device Admins to add, edit, and delete device groups and to set group rate limits. To open as the Device Admin or Org Admin, click the **Manage Groups** link located next to **Feedback**. Use this page to add and manage device groups, including the group rate limit. Devices that are part of a group still can have their own rate limit if needed, for example if a device is taking up a huge amount of resources. Individual devices within the group can be disabled if needed.

  - **Users Page Update** - The device **Users** page is updated with a **Device Group** selector for adding the device to one or more groups, and a drop-down list of available groups.

Important The ability to do multi-select on this page is temporarily removed.

Behavioral Indicators

- 9 New Behavioral Indicators.
- 10 Modified Behavioral Indicators.

What's New

For detailed information about what's new in Threat Grid Portal release 3.5.74, see the online Help.