# Release Notes for Cisco Threat Grid Appliance Version 2.11

**First Published:** 2020-05-08

**Last Modified:** 2020-06-26

## Introduction

This document describes the new features, open issues, and closed issues in Cisco Threat Grid Appliance Version 2.11, 2.11.1, 2.11.2, 2.11.3, and 2.11.4. It also includes the release notes and what's new for Cisco Threat Grid Portal.

## 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 2.11.4

- Release Date: June 26, 2020
- Build Number: 2020.01.20200626T131623.srchash.ac455a52b3a3.rel
- This release addresses an issue which could make the Admin UI temporarily unusable during initial installation, and upgrades 3rd-party components to address a number of subcritical security issues.

### Version 2.11.3

- Release Date: June 10, 2020
- Build Number: 2020.01.20200610T150909.srchash.1f7ea0f0a0fe.rel
- Description: This release addresses various security issues with 3rd-party dependencies, the most serious of which could allow users with legitimate Admin UI credentials to attack the system or each others' browsers.

### Version 2.11.2

- Release Date: May 22, 2020
- Build Number: 2020.01.20200522T024707.srchash.2d8262113089.rel
- Description: This release fixes a very low-prevalence bug which could leave an appliance unable to be successfully configured, should the recovery partition be unmounted while the `run-config-backup` process is ongoing. It also addresses some issues which could prevent the `reconfigure with-reinstall` tool from working as-intended.

  For customers already running 2.11.1, it is safe to defer or avoid installation of 2.11.2 until and unless a bug it fixes is encountered.

### Version 2.11.1

- Release Date: May 15, 2020
- Build Number: 2020.01.20200515T174913.srchash.bba5cd602e0e.rel
- Description: This release fixes some minor issues which were found in 2.11.0. If upgrading from a release prior to 2.11.0, be sure to read the full release notes.

### Version 2.11

- Release Date: May 8, 2020

- Build Number: 2020.01.20200508T182337.srchash.6ad6bcb81659.rel
- This release updates core Threat Grid software to follow the cloud 3.5.50 release; introduces a new and modernized configuration UI; and fixes important bugs in remote exit support and the data-reset mechanisms.

# Fixes and Updates

### Version 2.11.4

The following fixes and updates are included in Version 2.11.4:

- When the textual configuration tools save an updated network configuration, they now instruct the graphical Admin UI to immediately load that configuration, preventing a situation wherein network configuration could not be changed from the Admin UI without a service restart.
- libtiff is updated to address CVE-2019-17546.
- ncurses is patched to address CVE-2019-17594 and CVE-2019-17595.
- glibc is patched to address CVE-2020-1752 and CVE-2020-10029.
- redis is updated to address CVE-2020-14147.
- icu4c is updated to address CVE-2020-10531.
- pcre2 is updated to address CVE-2019-20454.

### Version 2.11.3

The following fixes and updates are included in Version 2.11.3:

- `json-c` is updated to address CVE-2020-12762.
- `sqlite` is updated to address CVE-2019-16168, CVE-2019-19645, CVE-2019-19646, CVE-2020-11655, CVE-2020-11656, CVE-2020-13434, CVE-2020-13435, CVE-2020-13630, CVE-2020-13631, and CVE-2020-13632.
- `kibana` is updated to address CVE-2020-7013 and CVE-2020-7015.
- An issue which could prevent deferred jobs in the Admin UI from being correctly marked as failed has been resolved.

### Version 2.11.2

The following fixes and updates are included in Version 2.11.2:

- The configuration-backup process now runs in its own filesystem namespace, to prevent mount-table changes made by other processes from interfering with execution.
- The process of ensuring that an appliance's software loaded precisely matches the factory loadout no longer explicitly exempts mount points from enforcement, allowing the console command `reconfigure with-reinstall` to fix issues caused by stray files being left under what should be empty mount points.

Some other issues which could interfere with `reconfigure with-reinstall` (requiring additional steps to bring a system into fully-usable state after repair with this tool) are also addressed.

### Version 2.11.1

The following fixes and updates are included in Version 2.11.1:

- Online help is more clear that certificates and private keys are expected to be uploaded in PEM format.
- Private keys in PEM-encoded PKCS#8 format are now supported by the new admin UI.
- Support snapshot view has been enhanced: A race condition that could cause errors to be reported during view creation has been resolved; and filename extensions for snapshot and snapshot view files more appropriately reflect their types. Note that snapshots from before the update may no longer have their content available to view or submit.
- tcpdump and libpcap have been updated to address CVE-2018-16301 and others.

### Version 2.11

The following fixes and updates are included in Version 2.11:

- The core Threat Grid application is updated to release 3.5.50.
- A service notice is added to inform customers who will need to perform a data reset prior to the installation of appliance 3.0.
- The appliance Admin UI is completely modernized. Among the features added by this new UI is the ability to view historical system logs, which were previously only accessible to customers providing a remote syslog server.
- The option to disable the admin network interface outright (or re-enable it when disabled) has been moved from tgsh to the web-based admin UI.
- When the admin network interface is disabled, the admin UI is now accessible on the clean network interface not just on port 8443 (as before), but also on port 18443. This prevents conflicts with legacy behavior where port 8443 could also serve the primary Threat Grid UI and API (when the admin network interface was not in fact disabled).
- A RADIUS bug impacting configuration of non-ECC keys is addressed.
- Remote exit support fixes a DHCP table leak (particularly severe on appliances with unreliable connections to the exit servers in use).
- The data reset mechanism fixes a bug which could result in an inoperable appliance when the reset is run from recovery mode rather than regular operation.
- Time synchronization is now managed by systemd-timesyncd rather than ntpd.
- When generating self-signed SSL certificates with no DNS name set, the default is now the appliance serial number (with an additional SubjectAltName for the IP address), rather than the hardcoded value `pandem`.
- The validation requirements for the admin UI password are now a superset of those for the primary Threat Grid application, preventing a case where installation could fail due to an unacceptably weak initial password being selected.

- Network packets which could not be successfully translated to use the network address of the dirty interface as their source address could be emitted via the dirty interface with source addresses in the IPv4 link-local reserved range. This never posed a security risk, but could cause unwanted monitoring alerts; such packets are now dropped.
- A service notice regarding CIMC configuration on M5 hardware is now correctly cleared when the fault is confirmed to no longer be present.

# 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 Release 3.5.50

First released to Threat Grid Cloud portal on February 13, 2020.

### Fixes and Updates

- **Dusk Mode** - The UI now includes a **Dusk** theme option for those users who prefer working with a dark background. Dusk mode can be enabled/disabled in the User Management** page: under Preferences choose the Dusk theme to enable the dark background.
- **Behaviorial Indicatiors** - 38 new and 8 modified behavioral indicators.

### What's New in Threat Grid Portal 3.5.50

**Dusk Mode**

Staring at small print against a bright white monitor background can be hard on the eyes. The Threat Grid UI now offers the option to select a dark background theme. The Dusk theme can be enabled/disabled in the User page:

1. From the login name drop-down menu, choose **My Account** to open the **User** page.
2. In the **Preferences** section, click **Dusk** to enable the dark background theme colors. The change goes into effect right away.

© 2020 Cisco Systems, Inc. All rights reserved.