

# TIG-OS Release Notes

These firmware releases are available within GMC at <https://gmc.banduracyber.com>.

If you have any questions about these updates or have any problems downloading or installing the updates, you may contact Bandura Support at [support@banduracyber.com](mailto:support@banduracyber.com) or 1-855-PoliWall ([855-765-4925](tel:855-765-4925)).

**NOTE - If you are running ProACT on-premises, please contact support before updating to firmware version 3.70 or later.**

## Version 3.73.03920 (04 MAR 2021)

**Several extremely critical defects are addressed in this release. As such, we urge all of our customers in the strongest of terms to upgrade to this release as soon as possible.**

- **[CRITICAL]** Bug fix (DEV-2131) - The internal device ASN limits were reached, and we have extended them in this release. This is critical - devices without this fix will continue to use the ASN and country registration information as of February 19, 2021, and will not be able to receive updated ASN information from our central GMC management platform until this software release is installed.
- **[CRITICAL]** Bug Fix (DEV-2103) - Include fix for the highly-publicized CVE-2021-3156 Linux 'sudo' vulnerability
- **[CRITICAL]** Bug Fix (DEV-2110) - Fix issue where domains were not being checked against the lists in a case-insensitive manner
- **[CRITICAL]** Bug Fix (DEV-2099) - Fix issue where large threat intelligence feeds could get in a reset loop if they take too long to finish resetting
- Feature (DEV-2101) - Include per-bridge traffic statistics in healthcheck metadata
- Feature (DEV-2100) - Ensure all traffic passes in both directions if a device license expires

## Version 3.72.03876 (16 JUN 2020)

- Bug Fix - Fix issue where unnecessary HIPPIE alarms were being generated

## Version 3.72.03873 (04 MAY 2020)

- Bug Fix - Fix issue where the TIG could crash when coming out of bypass mode because of a property not being properly set on a flow record
- Bug Fix - Fix issue when acknowledging all alarms
- Bug Fix - Fix issue where enabling or disabling a blacklist or whitelist may not properly update the engine with the IP ranges from the list
- Update software download link

### **Version 3.72.03853 (07 FEB 2020)**

- Bug Fix - Fix issue where country and ASN info for IPv6 traffic isn't processed correctly and could cause a crash

### **Version 3.72.03848 (31 JAN 2020)**

- Bug Fix - Reduce IO slowdowns on certain models
- Bug Fix - Fix issue where stats are not being reported to GMC
- Bug Fix - Fix issue where certain hardware platforms were not properly handling VLAN traffic

### **Version 3.72.03803 (14 NOV 2019)**

- Bug Fix - Fix issue where packet logs may stop being exported to syslog
- Bug Fix - Fix issue where certain hardware platforms would enter bypass mode under heavy load

### **Version 3.72.03772 (09 SEP 2019)**

- Support for new hardware models
- Handles firmware updates better when the device is heavily loaded

### **Version 3.72.03712 (28 MAY 2019)**

- NOTE - If you are running version 3.70 or earlier, please contact [support@bandurasystems.com](mailto:support@bandurasystems.com) prior to upgrading so we can ensure everything is available on the new GMC servers.
- Feature- Improved display tables for larger Blacklists, Whitelists, and Threat lists.
- Feature- Improved Domain Whitelisting functionality and IP resolution.
- Feature- Increased the length of log messages in order to capture more fidelity in actions and errors
- Bug Fix - Various UI tweaks and fixes

### **Version 3.72.03551 (27 SEP 2018)**

- NOTE - If you are running version 3.70 or earlier, please contact [support@bandurasystems.com](mailto:support@bandurasystems.com) prior to upgrading so we can ensure everything is available on the new GMC servers.
- Feature - Add better pagination and searching to Threat lists, Blacklists, Whitelists, and REACT
- Feature - Include additional information in certain packet log records
- Feature - Add *disconnect* as an option for power off mode to hardware models that support it. Disconnect mode will disconnect the interfaces

instead of entering bypass mode when the system is powered off or there is a system failure.

- Bug fix - Various UI tweaks and fixes.

### **Version 3.71.03454 (31 AUG 2018)**

- NOTE - If you are running version 3.70 or earlier, please contact [support@bandurasystems.com](mailto:support@bandurasystems.com) prior to upgrading so we can ensure everything is available on the new GMC servers.
- Bug fix - Fix issue where configuration databases were being locked too frequently
- Bug fix - Fix issue where a network process could hang if the network connection is interrupted
- Bug fix - Fix a rare issue where certain hardware models would unexpectedly enter bypass mode

### **Version 3.71.03291 (22 JUN 2018)**

- NOTE - If you are running version 3.70 or earlier, please contact [support@bandurasystems.com](mailto:support@bandurasystems.com) prior to upgrading so we can ensure everything is available on the new GMC servers.
- Feature - Better synchronization with GMC servers

### **Version 3.70.02869 (07 DEC 2017)**

- Bug fix - Fix performance issue during initial load of large domain blacklists

### **Version 3.70.02861 (19 OCT 2017)**

- Bug fix - Fix issue processing DNS packets on certain hardware models
- Bug fix - Better error handling when pulling updates from BanduraOne
- Update http server configuration to include fewer version details

### **Version 3.70.02849 (19 SEP 2017)**

- Bug fix - Fix issue where the password change page was not redirecting properly

### **Version 3.70.02844 (31 JUL 2017)**

- Feature - New look and feel
- Feature - New dashboard showing top countries, ASNs, threat categories, and IP addresses

- Feature - Ability to sync Resource Group Policies down from a central BanduraONE server
- Feature - Ability to block outgoing DNS requests based on blacklisted domain names
- Feature - New log searching functionality

#### **Version 3.60.02374 (04 MAY 2017)**

- Bug fix - Fixes an issue where an established session could be re-evaluated against an incorrect resource group after a policy update

#### **Version 3.60.02183 (04 AUG 2016)**

- Adds support for support for automated synchronization of Blacklists
- Adds Service Groups to simplify the configuring of Resources
- Adds global Whitelists which whitelist addresses for all Resource Groups
- Adds support for sending Alarms out via email.
- Adds ability to set bypass mode for each bridging pair independently for hardware models with multiple bridging pairs
- Adds descriptions to Exception List and Whitelist entries

#### **Version 3.50.01703 (11 MAY 2016)**

- Bug fix - Fixed issue where PoliWall was not properly filtering VLAN tagged traffic.

#### **Version 3.50.01669 (07 APR 2016)**

- New information added to the Check IP Policy page
- Bug fix related to syncing data from a ProACT server
- Bug fix - banner settings are now properly loaded when importing a new config

#### **Version 3.50.01626 (07 MAR 2016)**

- Adds support for connecting to a ProACT server
- Adds support for looking up the ASN of connections and includes the ASN number and name in the log files.
- Updates the System Provider to pull updates from <https://support.bandurasystems.com>.