



Cisco IOS Release 15.6(3)M7 – Release Notes for Cisco CGR1000 Series Connected Grid Routers

The following release notes support the Cisco IOS 15.6(3)M7 release. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

Contents

This publication consists of the following sections:

- [Image Information and Supported Platforms, page 1](#)
- [Software Downloads, page 1](#)
- [Major Enhancements, page 2](#)
- [Related Documentation, page 3](#)
- [Caveats, page 3](#)

Image Information and Supported Platforms

Note: You must have a Cisco.com account to download the software.

Cisco IOS Release 15.6(3)M7 includes the following Cisco IOS images:

- System Bundled image: cgr1000-universalk9-bundle.SPA.156-3.M7
 - IOS Version: cgr1000-universalk9-mz.SPA.156-3.M7
 - Guest Operating System: cgr1000-ref-gos.img.1.2.5.2.gz
 - Hypervisor: cgr1000-hv.srp.SPA.2.1.16
 - FPGA: 2.D.0
 - BIOS: 17

Software Downloads

The latest image file for the CGR 1000 Series Cisco IOS image is:

<https://software.cisco.com/download/navigator.html?mdfid=284165761&flowid=75122>

Known Limitations

For details on the CGR1000 installation, please see:

<http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/release/notes/OL-31148-05.html#pgfld-9>

Warning about Installing the Image

Note: The bundle can be copied via Trivial File Transfer Protocol (TFTP) or SCP to the device, and then installed using the `bundle install flash:<image name>` command. The bin file can NOT be directly booted using the `boot system flash:/image_name.`

Known Limitations

This release has the following limitations or deviations from expected behavior:

Please ensure there is a minimum 30MB additional space in the flash: file system before attempting an upgrade or downgrade between releases. Otherwise, the FPGA/BIOS will not have enough space to store files and perform the upgrade. The bundle installation will error out with a message insufficient flash: space.

Major Enhancements

This section provides details on new features and functionality available in this release. Each new feature is preceded by the platform which it applies to.

PSIRT ADVISORY - Secure Boot for CGR1000

IMPORTANT INFORMATION - PLEASE READ!

FPGA and BIOS have been signed and updated to new versions.

Going forward, for the 15.6 Release Train, this image 15.6(3)M7 is considered as the baseline. Downgrade is **STRICTLY UNSUPPORTED to any versions dated prior to this release date!** A bundle install to previous releases will cause an error and fail if attempted. Any manual downgrade [non bundle operations] will impair router functionality thereafter.

Note: Due to FPGA/BIOS upgrade cycles, the normal router upgrade/boot time may seem longer than usual. This will occur only on this release. Do not power cycle the device and wait until the IOS prompt is available.

For additional information on the PSIRT see the following:

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot>

SD Card Password Protection Warning on the CGR1000

The SD Card password location has been changed, which results in an updated FPGA upgrade. As a result, the user is requested to DISABLE the SD Card password protection just prior to the upgrade process. Once upgraded, the user is requested to re-enable the same. This is **MANDATORY**.

Command Line Interface

To disable before upgrade:

```
CGR1K#config term
CGR1K#no sd-card password
CGR1K#exit
```

Save the configuration and reload for changes to take effect.

Related Documentation

To validate:

```
CGR1K#show sd-card password status
Password-protection: no
Reload-pending: no
```

To re-enable sd-card password protection POST UPGRADE:

```
CGR1K#config term
CGR1K#sd-card password <your_password>
CGR1K#exit
```

Save and reload

To validate after reload:

```
CGR1K#show sd-card password status
Password-protection: on
Reload-pending: no
```

Related Documentation

The following documentation is available:

- Cisco IOS cross-platform release notes:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-6m-and-t/release/notes/15-6m-and-t-book.html>

- All of the Cisco CGR 1000 Series Connected Grid Routers documentation can be found here:

<http://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/tsd-products-support-series-home.html>

- IoT Field Network Director

<https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/products-installation-and-configuration-guides-list.html>

- Cisco IOx Documentation is found here:

<https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html>

- Cisco IOx Developer information is found here:

<https://developer.cisco.com/docs/iox/>

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can [register for an account](#).

For more information about the Cisco Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

Caveats

Cisco IOS Release 15.6(3)M7

The following sections list caveats for Cisco IOS Release 15.6(3)M7:

Open Caveats

■ CSCvq71700

Reload-pending status still shows **yes** even after SD Card password is disabled and reloaded.

Impact: None, just display of status issue.

Workaround: None

■ CSCvo78253:

Description: iox hyp sched-policy 100 option does not work.

Workaround: Setting values up until 90 works.

■ CSCvr02717:

Description: DOT11 radio hard reset after sending/receiving traffic via Wifi port on CGR1120.

Symptoms: Results in the dot11 Radio 2/1 interface going into a “down down” state until a reload of the IOS.

```
*Aug 23 14:38:09.203: %LINK-3-UPDOWN: Interface Dot11Radio2/1, changed state to down
*Aug 23 14:38:10.203: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio2/1, changed state
to down
*Aug 23 14:38:35.225: %CGR1K_DOT11-3-RADIO_RESET: DOT11 radio hard reset
```

Workaround: Reload the router to recover the interface.

Resolved Caveats

The following caveats are fixed with this release:

■ CSCvo60928

SD Card password lock

Symptoms: In some scenarios, CMOS batteries would fail to work under extreme cold conditions and lock up SD Card password. As a solution, SD Card password has been moved to different location.

Workaround: None

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2019 Cisco Systems, Inc. All rights reserved.