



# Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco CG-OS Release CG1

---

**Last updated: January 2013**  
**Part Number: OL-28860-01**

These release notes contain the latest information about using Cisco CG-OS software with the Cisco 1000 Series Connected Grid routers, including this new information:

- Overview of new features added in this release. See [New Features in Cisco CG-OS Release CG1, page 2](#).
- Open and resolved caveats in releases CG1(6), CG1(5), CG1(4), CG1(3d), 5.2(1)CG1(3c), 5.2(1)CG1(3b), 5.2(1)CG1(2) and 5.2(1)CG1(1). See [Caveats, page 13](#).
- Release Note structure. See [Documentation Updates, page 30](#).

## Tell Us What You Think



Send your feedback about this document directly to the Connected Energy Documentation Team.

[Connected Energy Documentation Feedback Form](#)



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Contents

This release note includes the following sections

- [About the Cisco 1000 Series Connected Grid Routers, page 4](#)
- [System Requirements, page 6](#)
- [Installation Notes, page 6](#)
- [Important Notes, page 11](#)
- [Caveats, page 13](#)
- [Documentation Updates, page 30](#)
- [Related Documentation, page 30](#)
- [Obtaining Documentation and Submitting a Service Request, page 30](#)

## New Features in Cisco CG-OS Release CG1

[Table 1](#) lists the new features added in this release.

**Table 1**      ***New Features in Cisco CG-OS Release CG1***

<b>Release</b>	<b>Feature</b>	<b>Description</b>	<b>Related Documentation</b>
CG1(5) and later	Incremental software image upgrade	<p>The CG-OS software image files (kickstart and system image) are now available in two formats:</p> <ul style="list-style-type: none"> <li>• Full software image (large file)</li> <li>• Incremental software image (smaller patch file)</li> </ul> <p>The incremental image file contains only the differences between the previous software image and the new software image.</p> <p>Using the CLI, you can combine the incremental image file from the new release with the full image file from the previous release to get the equivalent of the full image file for the new release.</p> <p>The combined software image file can be used to upgrade the software on the Cisco CG-OS router with the <b>install all</b> command.</p> <p><b>Note</b> This feature is currently supported on CG3(1) and CG1(5) and later only. Therefore, you can upgrade from CG1(5) and later CG1 releases to CG3(1) and later releases, using this feature.</p>	See <a href="#">Generating Software Images Using Incremental Image Files</a> , page 10.
CG1(4) and later	Support for setting hostname and password for CDMA Simple IP authentication	<p>The CDMA module now includes Point-to-Point Protocol (PPP) Challenge Handshake Authentication Protocol (CHAP) type 6 and type 7 password support.</p> <p>CLI commands for Simple IP authentication have been added to enable you to configure a hostname and password on a cellular interface to be used for PPP negotiation.</p> <p>Currently, the password is not subject to password strength-check configuration because the Cisco CG-OS router acts as the PPP client rather than a server. Typically, the hostname and password are managed and set by the cellular network-side server with strength-check functionality.</p>	For feature overview and configuration details, see the <a href="#">Cisco Connected Grid Cellular 3G Module for CGR 1000 Series Installation and Configuration Guide</a> .

# About the Cisco 1000 Series Connected Grid Routers

Cisco 1000 Series Connected Grid Routers (Cisco CG-OS routers) are multi-service communications platforms designed for use in field area networks. The portfolio consists of two models – both ruggedized to varying degrees for outdoor and indoor deployments. Both models are modular and support a wide-range of communications interfaces such as 2G/3G, Ethernet, and WiFi.

## Features and Capabilities

- Rugged industrial design and compliance with IEC-61850-3 and IEEE 1613 for utility substation environments
- Feature-rich software capabilities including IPv6 and Quality of Service (QoS)
- Comprehensive security capabilities based on open standards
- Highly resilient design that optimizes communications network uptime and availability
- Network and device management tools for easy deployment, upgrades, and remote monitoring

## Command-Line Interface

The Cisco CG-OS software supports a command-line interface to configure and monitor the system.

## Network Management

The Cisco Connected Grid Device Manager (Device Manager) is a Windows-based application that field technicians can use to manage the Cisco CG-OS router remotely. The Device Manager connects to the Cisco CG-OS router by using a secure Ethernet or WiFi link.

[Table 2](#) provides an overview of the software features supported on the Cisco CG-OS router.

**Table 2**      **Software Feature Support on the Cisco CG-OS Router**

Feature	Description
QoS feature support includes: classification, marking, and priority queuing to manage traffic flow.	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide</i> at <a href="http://www.cisco.com/go/cgr1000-docs">www.cisco.com/go/cgr1000-docs</a>
Layer 3 Unicast Routing feature support includes: IPv4, IPv6, IP Services (DNS, DHCP), Open Shortest Path First version 2 (OSPFv2) and OSPFv3 routing, and Static Routing.	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide</i> at <a href="http://www.cisco.com/go/cgr1000-docs">www.cisco.com/go/cgr1000-docs</a>
Security feature support includes: Authentication, Authorization, and Accounting (AAA) using RADIUS and TACACS+, SSHv2 and Telnet secure access, IPSec static virtual tunnel interface, IKEv2, role-based access control (RBAC) for user accounts, and IP access control lists (ACLs) to filter traffic.	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide</i> at <a href="http://www.cisco.com/go/cgr1000-docs">www.cisco.com/go/cgr1000-docs</a>

**Table 2**      **Software Feature Support on the Cisco CG-OS Router (continued)**

Feature	Description
System management feature support includes: Network Time Protocol (NTP), System Message Logging, and Backhaul Manager.	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide</i> at: <a href="http://www.cisco.com/go/cgr1000-docs">www.cisco.com/go/cgr1000-docs</a>
Remote wireless access to the Cisco CG-OS router from a laptop client for diagnostic and troubleshooting by field personnel.	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers WiFi Software Configuration Guide</i> at: <a href="http://www.cisco.com/go/cgr1000-docs">www.cisco.com/go/cgr1000-docs</a>


[Table 3](#) provides an overview of the hardware features and interfaces supported on the Cisco CG-OS router.

**Table 3**      **Hardware Feature Support on the Cisco CG-OS Router**

Feature	Description
Hardware feature support includes: GPS, real-time clock, and battery backup and support for WiFi, cellular, and Ethernet interfaces.	<p>For feature overview and configuration details for the hardware features as well as mounting and installation details for the Cisco CG-OS router see the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i>.</p> <p>For software and hardware configuration details for the interfaces, see the following documents:</p> <ul style="list-style-type: none"> <li>Cellular interfaces (CDMA and GSM): <i>Cisco Connected Grid Cellular 3G Module for CGR 1000 Series Installation and Configuration Guide</i></li> <li>Ethernet interface: Hardware details addressed in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> and feature-specific software configuration addressed in the <i>Cisco 1000 Series Connected Grid Software Configuration Guide Set</i> as detailed in <a href="#">Table 2</a>.</li> </ul>
Small Form-Factor Pluggable (SFP) Modules	<p>The following SFP modules are supported on the Cisco 1240 CG-OS router:</p> <ul style="list-style-type: none"> <li>GLC-SX-MM-RGD</li> <li>GLC-LX-SM-RGD</li> <li>GLC-FE-100LX-RGD</li> <li>GLC-FE-100FX-RGD</li> <li>GLC-ZX-SM-RGD</li> </ul>

[Table 4](#) lists the limitations in this release for hardware features that are described in detail in the *Cisco 1240 Connected Grid Router Hardware Installation Guide*.

**Table 4**      **Hardware Limitations**

Feature	Label	Limitation Description
WPAN Connected Grid Module	---	This module is currently supported in router slot 4 only. For more information, refer to the chapter “Installing Connected Grid Modules” in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> , at <a href="http://www.cisco.com/go/cgr1000-docs">www.cisco.com/go/cgr1000-docs</a> .
Alarm port	ALARM	Currently not supported. Supports an external alarm system for monitoring system errors and events.
IRIG-B timing port	IRIG_B	Currently not supported. Provides timing output to a connected device.
Serial ports (2)	SER 1/1 SER 1/2	Currently not supported. S232/RS485 ports for connecting the router to DTE or DCE devices.
USB ports (2)	0  1	Currently not supported. For connecting external USB devices. Connect USB devices (such as a flash drive) directly to these ports or by using a USB cable

## System Requirements

Table 5 lists the hardware and software associated versions with this release.

**Table 5**      **Minimum Hardware and Software Requirements**

Component	Minimum Software Release
Cisco 1000 Series Connected Grid Routers	Cisco CG-OS Release 5.2(1)CG1(2)
Cisco Connected Grid Device Manager	CGD Manager release 1.0.12.105
Cisco ASR 1002 Aggregation Services Router (Cisco ASR) serving as a head-end router	Cisco IOS-XE 15.1(3)S
Cisco 3945 Integrated Services Router (Cisco ISR) serving as a Registration Authority	Cisco IOS 15.1(2)T2.1

## Installation Notes

This section addresses the following topics:

- [Determining the Software Version, page 7](#)
- [Upgrading to a New Software Release, page 7](#)
- [Erasing the Configuration File, page 11](#)

## Determining the Software Version

To identify the software version operating on the Cisco CG-OS router, enter the following command.

Command	Purpose
<b>show version</b>	Displays the software version installed on the Cisco CG-OS router.

## Upgrading to a New Software Release

You can upgrade the software on the Cisco CG-OS router by employing the **install all** command. Listed below are the two possible approaches when downloading images using the **install all** command. You must select one of the following approaches:

- Download the images (kickstart and system image) from a remote server into the volatile memory of the Cisco CG-OS router by employing the **install all** command to specify the path to the remote server and the protocol. After the download, the software installation begins *automatically*.
- Download the images (kickstart and system image) from a local server directly into the bootflash of the Cisco CG-OS router, and then *manually* enter the **install all** command to initiate the software upgrade.

The following table provides detailed command syntax for the **install all** command.

Command	Purpose
<pre>install all [kickstart {bootflash:   ftp://server[/path]   scp://[username@]server[/path]   sftp://[username@]server[/path]   tftp://server[:port][/path]   volatile:} kickstart-filename] [system {bootflash:   ftp://server[/path]   scp://[username@]server[/path]   sftp://[username@]server[/path]   tftp://server[:port][/path]   volatile:} system-filename] [non-interactive]</pre>	<p>Specifies the software images being downloaded (kickstart and system images), the method used to download the images such as FTP, SCP, TFTP (remote server downloads only), and the destination of the images (bootflash or volatile) on the Cisco CG-OS router.</p> <ul style="list-style-type: none"> <li>Define <b>bootflash:</b> as the destination in the <b>install all</b> command when the download is from a local server.</li> <li>Define <b>volatile:</b> as the destination in the <b>install all</b> command when you are downloading the software from a remote server (such as Cisco.com or a remote server in your own network).</li> </ul> <p><b>kickstart bootflash:</b> <i>kickstart-file-name</i>—Identifies the file as a kickstart image and the file name of that image. Format of the kickstart filename is as follows: cg-os_kick.bin. File name is case sensitive.</p> <p><b>system bootflash:</b> <i>system-filename</i>—Specifies internal flash memory as the destination of the software images. Format of the bootflash filename is as follows: cg-os_sys.bin. File name is case sensitive.</p> <p><b>ftp:</b> Specifies File Transfer Protocol (FTP) as the transfer method for the software images (kickstart and system).</p> <p><b>scp:</b> Specifies Secure Copy Protocol (SCP) as the transfer method for the software images (kickstart and system).</p> <p><b>sftp:</b> Specifies Secure Shell FTP (SFTP) as the transfer method for the software images (kickstart and system).</p> <p><b>tftp:</b> Specifies Trivial FTP (TFTP) as the transfer method for the software images (kickstart and system).</p> <p><i>username@</i>—Specifies the username on the server. Username is case-sensitive.</p> <p><i>//path</i>—Defines the path to the server on which the software images reside.</p> <p><i>//server</i>—Defines the IPv4 address or name of the server on which the software images reside.</p> <p><b>[non-interactive]</b>—Eliminates the need for interaction or responses from an administrator during the process. Process proceeds to completion without requesting approval by the user.</p>



## EXAMPLES

This example shows how to download the software images from a remote FTP server onto the Cisco CG-OS router bootflash. After download, the software installation starts automatically on the Cisco CG-OS router.

```
cgr1000# install all kickstart ftp://10.10.1.1/cg-os_kick.bin
system ftp://10.10.1.1/cg-os_sys.bin
```

This example shows how to download the software images from a remote SCP server onto the Cisco CG-OS router bootflash. After download, the software installation starts automatically on the Cisco CG-OS router.

```
cgr1000# install all kickstart scp://adminuser@10.10.1.1/cg-os_kick.bin
system scp://adminuser@10.10.1.1/cg-os_sys.bin
```

This example shows how to copy the image from a remote SCP server onto the Cisco CG-OS router bootflash and then *manually* upgrade the software by using the **install all** command.

```
cgr1000# copy scp://adminuser@10.10.1.1/cg-os_kick.bin bootflash:
cgr1000# install all kickstart bootflash:cg-os_kick.bin system bootflash:cg-os_sys.bin
```

This example shows how to copy the image from a remote SCP server onto the Cisco CG-OS router bootflash without requiring any action or entry by the administrator. All actions proceed automatically.

```
cgr1000# copy scp://adminuser@10.10.1.1/cg-os_kick.bin bootflash:
cgr1000# install all kickstart bootflash:cg-os_kick.bin system bootflash:cg-os_sys.bin
non-interactive
```



### Note

An output similar to the one below displays during the install. The same output displays for local and remote installations.

```
Verifying image bootflash:///cgr1000-uk9-kickstart.5.2.1.CG1.0.277.SPA.bin for boot
variable "kickstart".
[#####] 100% -- SUCCESS

Verifying image bootflash:///cgr1000-uk9.5.2.1.CG1.0.277.SPA.bin for boot variable
"system".
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:///cgr1000-uk9.5.2.1.CG1.0.277.SPA.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG1.0.277.SPA.bin.
[#####] 100% -- SUCCESS

Extracting "bios" version from image bootflash:///cgr1000-uk9.5.2.1.CG1.0.277.SPA.bin.
[#####] 100% -- SUCCESS

Extracting "loader" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG1.0.277.SPA.bin.
[#####] 100% -- SUCCESS

Performing module support checks.
2012 Jan 3 00:12:23 Router %$ VDC-1 %$
[#####] 100% -- SUCCESS
```

Notifying services about system upgrade.

[#####] 100% -- SUCCESS

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	none	

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version	Upg-Required
1	system	5.2(1)	5.2(1)	no
1	kickstart	5.2(1)	5.2(1)	no
1	bios	:		no
1	loader	1.2(2)	1.2(2)	no
1	fpga	2_0_0	2_4_0	yes

Do you want to continue with the installation (y/n)? [n] **y**

Install is in progress, please wait.

Performing runtime checks.

[#####] 100% -- SUCCESS

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom/fpga/modem firmware.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Install has been successful.

cgr1000#



#### Note

The Cisco CG-OS router reboots after a successful installation.

## Generating Software Images Using Incremental Image Files

The kickstart and system images are both available as incremental image files. Incremental image files contain only the differences between the previous software image and the new software image. An incremental software image can be combined with the previous software image to get the equivalent of the full version of the new software image, which can then be installed with the **install all** command, as described in the [Upgrading to a New Software Release](#) section.

For example, an incremental image file for CG3(1) contains only the differences between CG3(1) and the previous software release (that supports this feature), CG1(6). You can combine the CG3(1) incremental image file with the CG1(6) software image to get the equivalent of the full version of the CG3(1) software image. There are separate incremental image files for the kickstart and system images.

To generate software images using incremental patch files, you use the **image-patch** command in privileged EXEC mode. The following table provides detailed command syntax for the **image-patch** command.

Command	Purpose
<b>image-patch</b> <i>seed-image seed_img patch-file diff_img target-path target_url</i>	<p>Combines a specified seed image file with a specified incremental patch file, and copies the combined file to a specified target URL.</p> <p><b>seed-image</b>—Name of the image that you are upgrading from. There should be a copy of this image on the CGR bootflash.</p> <p><b>patch-file</b>—Name of the incremental patch file for image that you are upgrading to.</p> <p><b>target-path</b>—Location for the combined seed and patch file. The original seed and incremental patch files are left as-is.</p>

## Erasing the Configuration File

When you enter the **write erase** [**boot** | **debug** | **secrets**] command, it erases all of the persistent memory of the Cisco CG-OS router *except* for items noted in the table below.

Command	Purpose
<b>write erase</b> [ <b>boot</b>   <b>debug</b>   <b>secrets</b> ]	<p><b>boot</b>—Erases the configuration file (with the exception of the certificates, the private keys, the password encryption master key, and the cellular interface profile) from the persistent memory of the router. (CSCto56948)</p> <p><b>debug</b>—Erases only the debug configuration file from the persistent memory of the router.</p> <p><b>secrets</b>—Erases the certificates, private keys and the password encryption master key from persistent memory on the router.</p>

## Important Notes

### Battery Backup Unit

To prevent the battery backup unit (BBU) from discharging during transport or servicing of the Cisco CG-OS router, disable the BBU automatic discharge feature using the system software. Details on this procedure, please see the Installing Battery Backup chapter within the *Cisco 1240 Connected Grid Router Hardware Installation Guide*.

**Guidelines and Limitations**

Refer to the “Guidelines and Limitations” section of each chapter within the *Cisco Connected Grid Routers Software Configuration Guides* listed in [Table 2](#) and the highlighted Notes, Warnings, and Cautions throughout all Cisco CG-OS router documentation.

## Limitations and Restrictions

Cisco recommends that you review this section before you begin working with the router. These limitations might not be fixed, or do not have a workaround. Some features might not work as documented, and some features might be affected by recent changes to the switch module hardware or software.

- **CSCtw44740**

**Symptom:** In some cases, over the air service provisioning (OTASP) might not be successful or might time out.

**Workaround:** Re-attempt OTASP activation.

- **CSCty61792**

**Symptom:** The CGR 1000 fails certificate authentication.

**Conditions:** This issue can occur when authenticating the router using Simple Certificate Enrollment Protocol. If the enrollment profile refers to a Cisco IOS registration agent (RA), and the RA refers to a sub-certificate authority (SubCA) instead of a certificate authority (CA), the authentication fails.

**Workaround:** Authenticate to the SubCA over a terminal connection, or authenticate to the SubCA but do not use a Cisco IOS RA.

- **CSCud12701**

**Symptom:** IKEv2 handshake fails given IKEv2 can only accept messages of up to 2048 bytes.

**Conditions:** CGR 1000 was configured with IKEv2 for authentication by using RSA signatures and certificates. The IKEv2 authentication resulted in packets that were larger than 2048, which IKEv2 could not accept.

**Workaround:** There is no workaround.

# Caveats

This section addresses the open and resolved caveats in CG1 releases and provides information on how to use the Bug Toolkit to find further details on those caveats.

- [Open Caveats, page 13](#)
- [Resolved Caveats, page 22](#)
- [Accessing Bug Toolkit, page 29](#)

## Open Caveats

- **CSCto92724**

**Symptom:** The **show ip adjacency statistics** command displays inaccurate statistics. All packet and byte counts are displayed as 0. Entering the **clear ip adjacency statistics** command does not resolve this issue.

**Conditions:** This issue can occur when the system is passing data.

**Workaround:** There is no workaround for this issue.

- **CSCto95431**

**Symptom:** The Cisco Secure ACS Max Sessions feature, which determines the maximum number of simultaneous connections to the CGR 1000 router per user or per group, fails to prompt valid users to log in when configured for 1 or 2 maximum sessions.

**Conditions:** The issue occurs when the maximum number of simultaneous sessions is set to 1 or 2. When the maximum simultaneous sessions is set to 3 or more, this feature works as expected and the router supports up to 64 simultaneous sessions.

**Workaround:** Configure the Cisco Secure ACS Max Sessions feature on the router for 3 or more maximum simultaneous connections.

For more information about the Cisco Secure ACS Max Sessions feature, see:  
[http://www.cisco.com/en/US/products/sw/secursw/ps2086/products\\_user\\_guide\\_chapter09186a0080205a6e.html](http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a0080205a6e.html)

- **CSCtr21995**

**Symptom:** The **tacacs-server host test** command does not display related messages.

**Conditions:** This issue occurs when using any of the command keywords: {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}

**Workaround:** Enter the **test aaa** configuration mode command to display related messages. See the *Cisco 1000 Series Connected Grid Router Security Software Configuration Guide* for more information about this command: [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)

- **CSCtr22041**

**Symptom:** The **radius-server host test** configuration command does not display related messages.

**Conditions:** This issue occurs when using any of the command keywords: {**idle-time minutes** | **password password** [**idle-time minutes**] | **username name** [**password password** [**idle-time minutes**]]}

**Workaround:** Use the **test aaa** configuration command for similar results. See the *Cisco 1000 Series Connected Grid Router Security Software Configuration Guide* for more information about this command: [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs)

- **CSCts11031**

**Symptom:** DHCP debug commands are not supported for DHCPv4 devices. These debug commands include the following: **debug dhcp all**, **debug dhcp errors**, **debug dhcp mts-errors**, **debug dhcp mts-events**, **debug dhcp pkt-events**, **debug dhcp pss-errors**, and **debug dhcp pss-events**.

**Conditions:** This issue occurs under all conditions.

**Workaround:** Use the **show logging log** command to gather general information for DHCP4 devices.

- **CSCtt18599**

**Symptom:** After entering the **logging level facility severity-level** configuration command, no log files are displayed.

**Conditions:** This issue occurs under all conditions

**Workaround:** Use the **logging logfile** configuration command to configure a log file name, then use the **show logging** command to display that log file.

- **CSCtt27515**

**Symptom:** When the CGR 1000 ports Ethernet 2/1 and Ethernet 2/4 are connected to a SmartBit test device, the router displays the following message, and then the ping times out:

```
switch %$ VDC-1 %$ %ARP-2-DUP_SCRIP: rap [3453] Source address of packet received from
0000.0000.1010 on Ethernet2/1 is duplicate of local, 10.100.10.1
```

**Conditions:** This issue occurs when traffic is sent over the affected ports.

**Workaround:** Use MAC addresses instead of IP addresses for the destination and source address configuration.

- **CSCtu31015**

**Symptom:** Entering the **show accounting log last-index** command causes all AAA processes on the CGR 1000 to end.

**Conditions:** This issue occurs in all conditions, when the command is entered.

**Workaround:** Avoid using the **show accounting log last-index** command.

- **CSCtu34138**

**Symptom:** When the CGR 1000 router is configured with a Generic Router Encapsulation (GRE) tunnel for IPv6, the tunnel receiving end indicates an invalid link-layer address (LA) when it receives an RA.

**Conditions:** This issue occurs when a GRE tunnel on the router sends IPv6 data.

**Workaround:** There is no workaround for this issue.

- **CSCtu41227**

**Symptom:** The CGR 1000 Router Ethernet interfaces stop detecting Ethernet traffic when both IPv4 and IPv6 is sent over the interface.

**Conditions:** This issue occurs when both IPv6 and IPv4 Ethernet packets are sent to a router Ethernet interface that is configured with both an IPv4 address and an IPv6 address.

**Workaround:** There is no workaround for this issue.

- **CSCtv01443**

**Symptom:** The the router no longer pings over the Ethernet interfaces, and the ARP entry indicates incomplete.

**Conditions:** This issue occurs when the router is reloaded or power cycled several times.

**Workaround:** Try reloading or power cycling the router.

- **CSCtw44774**

**Symptom:** The CGR 1000 shuts down after consecutive reloads.

**Conditions:** This issue occurs when the router is consecutively reloaded 84 times.

**Workaround:** Avoid reloading the router consecutive times.

- **CSCtw50574**

**Symptom:** You cannot use the ip address interface configuration command to configure a static IP address on a router interface that has DHCP enabled.

**Conditions:** This issue occurs on interfaces with DHCP enabled.

**Workaround:** Use the **no ip address dhcp interface** configuration command to disable DHCP on the interface, then configure a static IP address on the interface.

- **CSCtw59629**

**Symptom:** The CGR 1000 displays NTP syslog errors when there is no NTP configuration on the router.

**Conditions:** This issue can occur when an NTP configuration exists on the router, and is then removed, and the router is reloaded.

**Workaround:** There is no workaround for this issue.

- **CSCtw64974**

**Symptom:** When there are two or more servers on the same local area network (LAN), devices on the LAN may not be assigned an IP address from any of the DHCP servers.

**Condition:** This issue occurs intermittently when there are two or more DHCP servers on the same LAN.

**Workaround:** There is no workaround for this issue.

- **CSCtw66798**

**Symptom:** The **show environment power** command does not display data from the CGR 1000 AC power supply. Instead the command display includes the following error:

```
Failed to read data from power supply unit!
```

**Conditions:** This issue occurs when the router is being supplied with power from the Battery Backup Unit (BBU).

**Workaround:** There is no workaround for this issue.

- **CSCtw70336**

**Symptom:** The QoS policy does not effectively prioritize high-priority traffic, and the router might drop high-priority traffic.

**Conditions:** The issue occurs on all interface types when there is congestion on the interface, and different queues are classified at ingress and prioritized to different levels

**Workaround:** There is no workaround for this issue.

- **CSCtw73191**

**Symptom:** The QoS statistics displayed for a virtual tunnel interface are correct, but the QoS statistics displayed for the corresponding physical interface are incorrect.

**Conditions:** This issue occurs when two QoS policies are configured on the CGR 1000, and one of the policies is assigned to a virtual tunnel interface and the other is assigned to the corresponding physical interface.

**Workaround:** There is no workaround for this issue.

- **CSCtw78760**

**Symptom:** The CGR 1000 **show environment power** command displays **0** for the current AC amperage value, even when the amperage value is actually higher.

**Conditions:** This issue occurs intermittently.

**Workaround:** There is no workaround for this issue.

- **CSCtw79027**

**Symptom:** When two or more IMIX data streams are configured with different priorities and are sent in both directions over the 3G interface, the data stream set to default priority is given a higher priority than data streams configured with a higher priority.

**Conditions:** This issue occurs when no QoS priorities are applied on either the egress or ingress, and there is data congestion on the interface.

**Workaround:** There is no workaround for this issue.

- **CSCtw79047**

**Symptom:** The IP ARP table that is displayed when you enter the **show ip arp** command shows the state INCOMPLETE in the MAC address column.

**Conditions:** This issue can occur when the Ethernet cable is removed from an Ethernet port that is actively transferring data.

**Workaround:** Stop the traffic flow and rediscover ARP.

- **CSCtw84640**

**Symptom:** Entering the **show led** command on the CGR 1000 displays LED status that references ports Ethernet 2/7 and Ethernet 2/8, each with a displayed status of Off. These ports do not exist on the router.

**Conditions:** This issue occurs in all conditions, when you enter the **show led** command.

**Workaround:** There is no workaround for this issue.



- **CSCtw85052**

**Symptom:** When the **ip http secure-port** command is used on the CGR 1000 to configure the port value between 6553 and 99999, a network connection to the CG Device Manager cannot be established.

**Conditions:** This issue occurs in all conditions.

**Workaround:** Do not set a value greater than 65535 with the **ip http secure-port** command.

- **CSCtw85126**

**Symptom:** The **show version** command does not display EPLD versions for modules installed in the CGR 1000.

**Conditions:** This issue occurs under all conditions.

**Workaround:** There is no workaround for this issue.

- **CSCtw87364**

**Symptom:** The output for the **show ip interface brief** command is incorrect for the link state and the admin state. These value for these fields should be either UP or DOWN, however the output displays the following message:

```
link-state TRUE or FALSE admin-state TRUE or FALSE
```

**Conditions:** This issue occurs after entering the **show ip interface brief** command.

**Workaround:** There is no workaround for this issue.

- **CSCtw87639**

**Symptom:** The CGR 1000 software incorrectly displays the software name as “Cisco Nexus Operating System (NX-OS) Software” and displays the software version number as 5.2(1).

**Conditions:** This issue occurs in various instances in the router command-line interface.

**Workaround:** There is no workaround for this issue.

- **CSCtw87711**

**Symptom:** The term “switch” is used in the CGR 1000 CLI. The CGR is a router.

**Conditions:** The term is used in various places in the CLI.

**Workaround:** There is no workaround for this issue.

- **CSCtw91033**

**Symptom:** When two Ethernet interfaces on the CGR 1000 are configured for DHCP addressing with the **ip address dhcp** command, one of the interfaces is assigned an IP address through DHCP but the other is not. Entering the **no ip address dhcp** command on the interface with the assigned IP address does not result in a DHCP address being assigned to the second interface.

**Conditions:** This issue occurs when two Ethernet interfaces are configured for DHCP addressing.

**Workaround:** Enter the **no ip address dhcp** command on the interface that did not receive the IP address, then enter the **ip address dhcp** command.

- **CSCtw95689**

**Symptom:** The **shut** and **no shut** commands have no effect on the cellular interface on the CG 3G module installed in the CGR 1000.

**Conditions:** This issue occurs when the module is reloaded multiple times and the commands **shut** and **no shut** are entered several times for the module’s cellular interface.

**Workaround:** Reload the CGR 1000.

- **CSCtx04493**

**Symptom:** The CGR 1000 displays a message that contains this warning:

```
WARNING: This sap has exceeded its pre-set buffer limit.
```

**Conditions:** This message can occur intermittently when the router has IPSec, OSPFv3, and OSPF configured with two tunnel interfaces.

**Workaround:** There is no workaround for this issue.

- **CSCtx04502**

**Symptom:** Entering the **show clock** command in boot mode on the CGR 1000 displays the following error message:

```
/isanboot/bin/vshboot: symbol lookup error: /isanboot/lib/libsyscli_boot.so: undefined
symbol: mts_bind
```

**Conditions:** This issue occurs in boot mode.

**Workaround:** There is no workaround for this issue.

- **CSCtx06803**

**Symptom:** The image upgrade table does not display any data for the CG WPAN (RF) module in the **Running-Version(pri:alt)** column or the **New-Version** column.

**Conditions:** This issue occurs intermittently when using the **install all** command to upgrade the software for the module.

**Workaround:** There is no workaround for this issue.

- **CSCtx15578**

**Symptom:** The RADIUS server crashes.

**Conditions:** This issue occurs intermittently when the server is receiving a high volume of authentication requests.

**Workaround:** There is no workaround for this issue.

- **CSCtx18250**

**Symptom:** A learned OSPF route is given preference over the same static route configured in the CGR 1000.

**Conditions:** This issue occurs when the same router is both a learned OSPF route and a configured route.

**Workaround:** To resolve this issue, remove the learned OSPF route from the router configuration. To prevent this issue from occurring, do not use OSPF on an interface for which you want to use static routes.

- **CSCtx22265**

**Symptom:** The CGR 1000 free memory decreases, which can be verified by viewing the output of the **show system resources** command.

**Conditions:** This issue might occur when the router has been operating for 10 days or longer.

**Workaround:** Reloading the router might resolve the issue.

- **CSCtx31096**

**Symptom:** The CGR 1000 console session hangs and then the following error message is displayed:

```
Process did not respond within the expected time frame, please try again.
```

**Conditions:** This issue occurs when you enter the show logging persistent command during a router console session.

**Workaround:** There is no workaround. The console session resumes after the error message is displayed.

- **CSCtx35868**

**Symptom:** The CGR 1000 displays the following syslog error:

```
2012 Jan 13 15:48:38 far_1_1 %NETSTACK-3-CPI_ERR: netstack [3979] Write to mbufsk
failed in pm_mbufsk_write with error 9, num-pkts 1, num-processed 0 fd -1
```

```
2012 Jan 13 15:48:44 far_1_1 Jan 13 15:48:44 %KERN-3-SYSTEM_MSG: [134526.000040]NETDEV
WATCHDOG: usb0 (sierra_net): transmit timed out - kernel
```

**Conditions:** This issue can occur when constant bidirectional traffic is sent over the CG 3G module interface over an IPSEC GRE tunnel for long durations.

**Workaround:** The router will recover by itself after the traffic load is reduced.

- **CSCtx52882**

**Symptom:** Enabling DHCP on an interface removes any IP address configured on the interface.

**Conditions:** This issue occurs when you enable DHCP on an interface that is already enabled for DHCP.

**Workaround:** Enter the **no ip address dhcp** command on the interface to disable DHCP addressing, then enter the **ip address dhcp** command to re-enable DHCP on the interface.

- **CSCtx58117**

**Symptom:** The IP routing table displayed with the **show ip route** command shows all IPv4 routes in a pending state.

**Conditions:** This issue occurs in all conditions for IPv4 routes only (not for IPv6 routes).

**Workaround:** There is no workaround for this issue.

- **CSCtx60322**

**Symptom:** The **class-map** configuration command does not support the **match-all** command option for access list and packet length matching combined.

**Conditions:** This issue occurs when using the **class-map match-all** option with access-list and packet length matching combined.

**Workaround:** Use the **class map match-all** option with either access-list or packet length matching, but not with both.

- **CSCtx68817**

**Symptom:** Entering the **show interface counters module x** command on any of the interfaces (3G, Ethernet) results in an error condition. The error message displayed is:

```
vsh: ../utils/if_index/lib/if_index_impl.c:2562: if_index_get_slot: Assertion `0'
failed.
```

**Conditions:** This issue occurs when using the **show interface counters module** command on the affected module interfaces.

**Workaround:** Avoid using this command on the affected module interfaces.

- **CSCtx68856, CSCtx68893**

**Symptom:** Entering the **show interface counters module x** command on the 3G, WiMAX, and Ethernet interfaces results in the following error condition:

```
vsh: ../utils/if_index/lib/if_index_impl.c:2562: if_index_get_slot: Assertion `0'
failed.
```

**Conditions:** This issue occurs when using the **show interface counters module** command on the affected module interfaces.

**Workaround:** Avoid using this command on the affected module interfaces.

- **CSCtx74312**

**Symptom:** The output for the **show system internal mts buffers details** command displays reduced memory for the CGR 1000.

**Conditions:** This issue can occur after continued use of the **ping6** command.

**Workaround:** Avoid continued use of the **ping6** command.

- **CSCtx90382**

**Symptom:** A static route to a subnet cannot be removed from the CGR 1000 with the **no ip static-route** command until after the router is rebooted.

**Conditions:** This issue occurs when the **ip static-route** command is used to configure a static route to a subnet.

**Workaround:** To prevent this issue, avoid configuring static routes to subnets. To resolve this issue remove the static router after rebooting the router.

- **CSCtx95796**

**Symptom:** The CGR 1000 displays the private key password in clear text in the accounting logs and on external AAA (TACACS+) servers.

**Conditions:** This issue occurs when manually importing a PKCS #12 formatted certificate that has already been copied to the CGR bootflash with the command **crypto ca import trustpoint\_name pkcs12 bootflash: <PKCS #12 certificate filename> <private key password>**.

The private key password is displayed when AAA (TACACS+) config-commands and command authorization, and accounting are enabled.

**Workaround:** There is no workaround for this issue.

- **CSCTy01882**

**Symptom:** A tunnel interface is configured with **no keepalive** by default.

**Conditions:** This issue occurs on all tunnel interfaces.

**Workaround:** Use the **keepalive** interface configuration command to enable keepalive on the tunnel interface.

- **CSCty02541**

**Symptom:** The CGR 1000 Path MTU Discovery feature is not able determine the maximum transmission unit (MTU) size on the network path between hosts.

**Conditions:** This issue occurs when an intermediate node on the network (between the hosts) experiences a change in MTU size.

**Workaround:** There is no workaround for this issue.

- **CSCty07645**

**Symptom:** The CGR 1000 CLI displays the maximum supported value for the **air-sync server port** command to be 99999. The actual supported maximum value is 65535.

**Conditions:** This issue occurs in all conditions.

**Workaround:** Do not enter a value greater than 65535 with the **air-sync server port** command.

- **CSCty14312**

**Symptom:** The CGR 1000 does not respond with an echo reply to link- local echo requests.

**Conditions:** This issue occurs when the router receives a link-local request for the first time. The router does send an echo reply to subsequent link-local echo requests.

- **CSCty19932**

**Symptom:** Entering the CLI **install all** command fails to install the required software for the Connected Grid WPAN module. The same issue occurs when entering the **install all** command from CG Device Manager.

**Conditions:** This issue occurs when the software image is downloaded using CG NMS software.

**Workaround:** Do not download the software image with CG NMS software. Use another file transfer method.

- **CSCty81424**

**Symptom:** The CGR 1240 router does not support SFP model GLC-FE-100FX-RGD.

**Conditions:** This issue occurs under all conditions.

**Workaround:** Use one of the following supported SFP models: GLC-FE-100LX-RGD, GLC-SX-MM-RGD, GLC-LX-SM-RGD, GLC-ZX-SM-RGD.

## Resolved Caveats

This section summarizes the resolved caveats of CG1 releases.

- [Caveats Resolved in Cisco CG-OS Release CG1\(6\)](#), page 22
- [Caveats Resolved in Cisco CG-OS Release CG1\(5\)](#), page 22
- [Caveats Resolved in Cisco CG-OS Release CG1\(4\)](#), page 23
- [Caveats Resolved in Cisco CG-OS Release CG1\(3d\)](#), page 23
- [Caveats Resolved in Cisco CG-OS Release 5.2\(1\)CG1\(3c\)](#), page 24
- [Caveats Resolved in Cisco CG-OS Release 5.2\(1\)CG1\(3b\)](#), page 25
- [Caveats Resolved in Cisco CG-OS Release 5.2\(1\)CG1\(2\)](#), page 26

### Caveats Resolved in Cisco CG-OS Release CG1(6)

- **CSCtx55382:**

**Symptom:** Cisco CG-NMS lost connectivity to CGR 1000.

**Conditions:** Two trust points were active in the CGR 1000 network. Each trust point was mapped to a different Certificate Authority (CA) server. JVM manager was mishandling the trust point certificate.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(6)

- **CSCtz47793:** On rare occasions, the CGR 1000 sent the registration request before the Connected Grid Device Manager (CGDM) initialized.

**Conditions:** The CGR 1000 sent a registration request to CG-NMS before the CGR CGDM Jetty server was bound to the port and was listening for requests. When CG-NMS responded quickly to the registration request, the connection that CG-NMS tried to establish to the CGR CGDM service was rejected. This issue appeared in the CG-NMS log as "java.net.ConnectException".

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(6)

### Caveats Resolved in Cisco CG-OS Release CG1(5)

- **CSCtz86343**

**Symptom:** Communication between a Cisco ASR and Cisco CGR 1000 stopped after a meter power outage, when the ASR mistakenly forwarded packets using an older SPI over its IPSec connection to a Cisco CGR 1000.

**Conditions:** Two SPIs were defined for the IPSec connection between the ASR and CGR 1000.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(5).

- **CSCub22538**

**Symptom:** Excessive memory leaks in the software due to call home notifications could result in a reload of the CGR 1000.

**Conditions:** Each time the CGR 1000 sent a call home notification, a memory leak occurred. The frequency of the periodic inventory notifications also affected the amount of the memory loss.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(5).

- **CSCuc64503**

**Symptom:** A number of CGR 1000s in a network reloaded multiple times within a day over the period of a week without the action being initiated by any personnel.

**Conditions:** Routers that reloaded were connected to specific 3G network vendors.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(5).

- **CSCuc91336**

**Symptom:** The dialer retry timer always reset after the 3G module reloaded.

**Conditions:** This issue occurred when the 3G module reloaded.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(5).

- **CSCuc94606**

**Symptom:** In some cases, the system clock on the CGR 1000, would change to an older system clock after a system reboot. The modified clock setting could be several days old. This affected any applications dependent on the system clock.

**Conditions:** A reboot of the CGR 1000 reset the system clock to a previous date.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(5).

## Caveats Resolved in Cisco CG-OS Release CG1(4)

- **CSCtz90193**

**Symptom:** CDMA Simple IP configuration failed.

**Conditions:** This issue occurred during Verizon CDMA certification testing.

**Workaround:** This issue is resolved in Cisco CG-OS Release CG1(4).

## Caveats Resolved in Cisco CG-OS Release CG1(3d)

- **CSCtx90505**

**Symptom:** A CGR 1240 operating with a completely drained BBU with firmware version 2082 might display incorrect information when the user enters the **show env power** command after booting up with CG-OS software CG1(3c) or earlier release.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCtz20900**

**Symptom:** A netstack process failed when the 3G cellular module reloads and the user enters the **shutdown** and **no shutdown** commands on the cellular interface. Uplink and traffic was 5Mbps.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCtz84988**

**Symptom:** When the RSSI was weak (for more than five minutes), a cellular link could take longer than five minutes to reconnect.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCtz87086**

**Symptom:** In cases that the CGR had more than 1,000 endpoints operating in its network for an extended period, the jvm\_mgr core might crash within the CG-NMS managing the CGR.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCua94395**

**Symptom:** The Backhaul Manager might not be able to reset or redial a data connection for the 3G cellular module by using the **shutdown** and **no shutdown** commands.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCub04025**

**Symptom:** System returns "IP address 0" when it receives packet data protocol (PDP) activation from the modem. Issue occurs when user toggles between different GSM bands.

**Workaround:** Issue the **shutdown** command followed by the **no shutdown** command or **reload** the module.

- **CSCub27668**

**Symptom:** The default timeout setting of 5 seconds for Simple Certificate Enrollment Protocol (SCEP) was not sufficient for running the protocol over a satellite link.

**Workaround:** The default timeout setting is now set to 25 seconds for the SCEP client on the CGR. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCub29574**

**Symptom:** The jettySSL times out on the CGR 1000 when communicating over a Satellite WAN link.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

## Caveats Resolved in Cisco CG-OS Release 5.2(1)CG1(3c)

- **CSCtz35817**

**Symptom:** If the CGR 1000 3G GSM interface does not connect to the cellular network on the initial attempt, the interface continues to attempt Packet Data Protocol (PDP) reactivation every 30 seconds.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3c) with the following behavior: The 3G GSM interface attempts PDP reactivation once per minute for 5 minutes. If these attempts are not successful, the interface attempts PDP reactivation four more times, at the following intervals: 10, 15, 30, and 60 minutes. If these attempts are not successful, the interface attempts activation once every 60 minutes until the connection is established.

- **CSCtz42307**

**Symptom:** In some cases, the **copy running startup** privileged EXEC command causes a file system error on the CGR 1000, and the router becomes unresponsive to CLI commands. The **copy running startup** command is used during Zero Touch Deployment (ZTD) after the CG-NMS pushes the configuration to the router. If the **copy running startup** command fails, the router does not complete ZTD and cannot communicate with the CG-NMS.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3c).

- **CSCtz42431**

**Symptom:** In some cases, during the Zero Touch Deployment (ZTD) process, the CGR 1000 does not successfully enroll using Simple Certificate Enrollment Protocol (SCEP). If this occurs, the ZTD process does not finish and the router cannot communicate with the CG-NMS.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3c).



## Caveats Resolved in Cisco CG-OS Release 5.2(1)CG1(3b)

- **CSCtx72509**

**Symptom:** The word SUPPLY is incorrectly spelled SUPPY in some CGR 1000 log messages, for example:

```
%PLATFORM-2-POWER_AC_TO_DC: Power Supply Transition Status Alert
```

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3b).

- **CSCtz13379**

**Symptom:** The 12 V DC power connector for powering external, third-party modules is disabled on the CGR 1000, and does not supply power to a module when connected.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3b).

- **CSCtz15031**

**Symptom:** The CGR 1000 DHCP client sends four syslog failure messages every three seconds when DHCP is enabled as part of Zero Touch configuration and the Ethernet port associated with the interface is not connected. The router DHCP clients attempts to configure the interface but fails because there is no Ethernet connection on the port.

**Workaround:** Ensure that the Ethernet port associated with Zero Touch configuration remains connected. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3b).

- **CSCtz16055**

**Symptom:** When AC power to the router is lost and then restored to the CGR 1000, the **show environment power command** indicates that the router power supply is not available by displaying a message like the following:

```
Power Supply Summary:
-----
Read PSU: Unable to choose port on I2C MUX
```

**Workaround:** Verify that power is being supplied to the router by checking the SYS LED to verify power is being supplied the router. For details, refer to the hardware installation guide at [www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs).

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3b).

- **CSCtz23964**

**Symptom:** When the CGR 1000 reboots after having established an IPSec tunnel with the peer device, the IPSec Security Associations (SA) on the peer device of a CGR 1000 IPSec tunnel are not correctly cleared.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3b).

- **CSCtz27313**

**Symptom:** The CGR 1000 can time out during registration, and can become isolated on the network, unable to communicate with the CG-NMS. This issue can occur in large-scale deployments if the router is rebooted or reloaded unexpectedly during registration. The copy running-config startup-config command does not copy the entire running configuration to the startup configuration, and when the router reboots, the configuration is incorrect.

**Workaround:** To resolve this issue, use the **http secure-server trustpoint tp-label** command to manually configure the router with the Trustpoint configured in CG Device Manager.

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3b).

## Caveats Resolved in Cisco CG-OS Release 5.2(1)CG1(2)

- **CSCtn91571**

**Symptom:** Packet size limits vary among service providers and can might cause ping packets to fail.

**Workaround:** Verify the packet size limits with your service provider before installing the Cisco CG-OS router. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCtr34492**

**Symptom:** In error, the Cisco CG-OS software allows the same RSA key-pair to be assigned to a certificate authority (CA) and registration authority (RA). The software provides no warning.

**Workaround:** Do not configure and assign the same RSA key-pair to the CA and RA. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2)

- **CSCto22974**

**Symptom:** At the loader prompt (loader >) of the kickstart image, the load command only accepts the first 89 characters when you cut-and-paste text.

**Workaround:** Type in the required text after the 89 character cut-and-paste limit is met. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2)

- **CSCto23106**

**Symptom:** The user cannot assign a custom value of allowed SSHv2 logins when using the **ssh login attempt <1-10>** command. Instead, the Cisco CG-OS router uses the default setting of 3.

**Workaround:** None. The Cisco CG-OS software uses the default setting. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto23263**

**Symptom:** Entering the **dir bootflash:kickstart** command at the loader prompt (loader >) does not display the sub-directories as expected. The following error message displays instead: *Error: drive bootflash:Kickstart not found*. Additionally, entering the **cd** command at the loader prompt does not access the sub-directories.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto35450**

**Symptom:** Special characters allowed by the Cisco CG-OS software (on your local Cisco CG-OS router) might not be supported on external AAA servers to which the router communicates.

The Cisco CG-OS software supports the following special characters:

- *username*—Supports the following special characters: ( \_ . + + \ - ) and can be a maximum of 28 alphanumeric characters. Username is case-sensitive.
- *password*—Supports all printable ASCII characters that are enclosed in quotation marks. Password is alphanumeric, case-sensitive, and limited to 64 characters.

**Workaround:** When using an external AAA server in your configuration, ensure that you know any special character limitations for that server before defining the local username and password on the Cisco CG-OS router.

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2)

- **CSCto40955**

**Symptom:** In rare cases, the **show running-configuration** command display might not list details about the interfaces after the initial start or restart of the Cisco CG-OS router.

**Workaround:** Re-enter the command until the interface information displays. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto54222**

**Symptom:** Entering the **load bootflash:// system\_image** command at the router(boot)# prompt (kickstart prompt) does not load the Cisco CG-OS software image and reports the image or file as corrupted.

**Workaround:** To load the software image, enter the **load bootflash** command by using only one forward slash (/) rather than two (//) in the command as shown in the following commands:

```
loader> boot bootflash://kickstart_image
router(boot) # load bootflash:/system_image
```

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto54300**

**Symptom:** Entering the **show version image bootflash://system\_image** command at the router(boot)# prompt (kickstart prompt) reports a MD5 verification failure and image integrity failure.

**Workaround:** To correct the issue, enter only one forward slash (/) rather than two (//) after bootflash: as shown in the following command:

```
router(boot) # show version image bootflash:/system_image
```

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto56948**

**Symptom:** Entering the **write erase** command does not delete the cellular profile configured on the Cisco CG-OS router.

**Workaround:** To delete the cellular profile, enter the following command: **cellular slot\_number/port\_number gsm profile delete 1**.

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto91341**

**Symptom:** In some cases the Cisco CG-OS software allows assignment of both a network-operator and network-admin role (the default) for the local admin user account by entering the **username admin password password role network-operator** command.

By design, when two roles are defined for the local user admin account, the one with the least privileges replaces the other account rather than allow support for two roles. Entering the **show running-config command** can confirm the current settings.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto97289**

**Symptom:** When entering the **show core** command on the Cisco CG-OS router, the following displays: “Copy complete, now saving to disk (please wait)” after the relevant information displays. The term “disk” is meant to be a generic term that can refer to any relevant storage location for the data.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCto97525**

**Symptom:** The **show logging ip access-list cache** command does not display an output.

**Workaround:** Use the **show logging ip access-list status** command to access the information. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCtq11071**

**Symptom:** Removing a SIM card on the cellular module and placing it in another slot on that module or returning it to its original slot on the cellular module, requires a reset of the Cisco CG-OS Router. Enter the **reload** command to reset the router.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCtq33130**

**Symptom:** In some cases when there is high traffic on the cellular module, the **show modem cellular** command displays incomplete and/or inaccurate information for the module.

**Workaround:** None. Re-entering the command at periods of lower traffic might be successful. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCts06544**

**Symptom:** When moving a cellular interface from one slot to another in the Cisco CG-OS router, the IP route information associated with the first slot cannot be deleted or removed from the running configuration. The residual IP route information does not adversely affect the operation of the Cisco CG-OS router.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCtu39989**

**Symptom:** Log file does not survive a reload of the Cisco CG-OS router.

**Workaround:** Before reloading the Cisco CG-OS router, redirect the log file to persistent storage (such as bootflash) by using the **show logging > file** command.

Example:

```
router# show logging > bootflash:log-Jan32012.txt
```

This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCtw87426**

**Symptom:** In some cases, when the user manipulates the port speed, a mismatch of port speeds operating on the Cisco CG-OS router and the port on its peer might occur and cause one or both of the ports to shutdown.

Generally, when auto-negotiation is active on the ports no mismatches occur.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

- **CSCtx21964**

**Symptom:** The **poweroff module number** command is not supported in the Cisco CG-OS software.

**Workaround:** This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(2).

## Accessing Bug Toolkit

You can use the Bug Toolkit to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Toolkit lists both open and resolved caveats.

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use the Bug Toolkit, follow these steps:

- 
- Step 1** To access the Bug Toolkit, go to the following link:  
<http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>
- Step 2** Log in with your Cisco.com user ID and password.
- Step 3** To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field and click **Go**.
- Step 4** To look for information when you do not know the bug ID number, do the following:
- a. From the Select Product Category menu, choose **Routers**.
  - b. From the Select Products menu, choose **Cisco 1000 Series Connected Grid Routers**.
  - c. From the Software Version menu, choose the version number.
  - d. Under Advanced Options, choose either **Use default settings** or **Use custom settings**.
    - When you select **Use default settings**, the system searches for severity 1, 2, and 3 bugs, open and fixed bugs, and only those bugs containing bug details.
    - When you select **Use custom settings**, you can specify the severity and status parameters or search for keywords within the bug headline and description.
-

# Documentation Updates

## Changes

Release Notes for Cisco 1000 Series Connected Grid Routers have been restructured to contain information for all maintenance releases for a given software release within one Release Note. For example, the Release Notes for CG-OS CG1 include details on releases CG1(6), CG1(5), and so on. Previously, we had separate Release Notes for these iterative releases.

## Related Documentation

Find Cisco 1000 Series Connected Grid Routers product documentation at:

[www.cisco.com/go/cgr1000-docs](http://www.cisco.com/go/cgr1000-docs).

Find Connected Grid Modules for Cisco 1000 Series Connected Grid Routers documentation at:

[www.cisco.com/go/cg-modules](http://www.cisco.com/go/cg-modules)

For information on supporting systems referenced in this release note, see the following documentation on Cisco.com:

[Cisco ASR 1000 Series Aggregation Services Routers Configuration Guide](#)

[Cisco 3945 Series Integrated Services Router](#)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

No combinations are authorized or intended under this document.

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.

© 2013 Cisco Systems, Inc. All rights reserved.