Release Notes for Cisco Catalyst Wireless Gateways, Cisco IOS CG Release 17.11.x

First Published: 2023-04-19

Last Modified: 2023-05-08

Release Notes for Cisco Catalyst Wireless Gateways, Cisco IOS CG Release 17.11.x

Read Me First

Related References

- *Hardware Installation Guide for Cisco Catalyst Wireless Gateways*
- *Cisco Catalyst Wireless Gateway Software Configuration Guide*
- *Cisco Catalyst Wireless Gateway Web-Based Interface*
- *Regulatory Compliance and Safety Information – Cisco Catalyst Wireless Gateways*

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

About Cisco Catalyst Wireless Gateways

Cisco Catalyst Wireless Gateway devices extend the enterprise network to remote workers. Connectivity is as follows:

- The Cisco Catalyst Wireless Gateway CG113-W6 accesses the internet using a wired WAN connection at a remote site.

- The Cisco Catalyst Wireless Gateway CG113-4GW6 accesses the internet using a wired WAN connection at a remote site or using a cellular link. The device supports two SIM cards: one active, and one on standby. If the wired WAN connection fails, the device fails over to the cellular link to ensure internet connectivity.

Cisco Catalyst Wireless Gateways provide numerous advantages to the remote worker, including the following:

- Hardware-based stable connectivity to an enterprise VPN

- Optimized network performance with Wi-Fi 6

- Cellular network connectivity, in supporting models, providing a cellular internet connection (with one active and one standby SIM) for uninterrupted internet connectivity

- Separate service set identifiers (SSIDs) for connecting work and personal devices

Managing Cisco Catalyst Wireless Gateways

Use Cisco vManage to configure and manage Cisco Catalyst Wireless Gateways. Cisco vManage provides a convenient workflow for configuring Wi-Fi, cellular, VPN, and other functionality. Cisco vManage also provides methods for monitoring device performance.

Cisco Catalyst Wireless Gateway Models

The Cisco Catalyst Wireless Gateways include the following models:

- Cisco Catalyst Wireless Gateway CG113-W6

  (Includes Wi-Fi connectivity)

- Cisco Catalyst Wireless Gateway CG113-4GW6

  (Includes Wi-Fi and cellular connectivity)

What's New for Cisco Catalyst Wireless Gateway Support in Cisco IOS CG Release 17.11.1a and Cisco vManage Release 20.11.1

Table 1: Cisco IOS CG Release 17.11.1a and Cisco vManage Release 20.11.1

Feature	Description
Support for Cisco SD-WAN Remote Access VPN	Cisco Catalyst Wireless Gateway devices support VPN connectivity with Cisco SD-WAN Remote Access servers. From this release, the default configuration of VPN connectivity is for a Cisco SD-WAN Remote Access headend, but a **Static Settings** option is available for configuring devices using Cisco IOS CG Releases 17.9.x or 17.10.x.

Feature	Description
Tunnel Redundancy	You can configure a secondary remote access server IP address or fully qualified domain name (FQDN), as a failover option in case the primary remote access server becomes unavailable.
Support for Additional Cipher Suites	You can configure the specific cipher suite to use for VPN encryption, if required by the VPN service. This is considered an advanced option and is available through the configuration group that you create for configuring Cisco Catalyst Wireless Gateway devices.
Support for Corporate Wired LAN	You can connect a corporate device, such as a corporate laptop, to a wired Ethernet connection on the Cisco Catalyst Wireless Gateway device.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) is a web-based tool providing access to the Cisco bug tracking system. If provides information about defects in Cisco products, including the status of a defect and affected releases.

Open Caveats in Cisco IOS CG Release 17.11.1a

The following table lists the open caveat(s) affecting Cisco Catalyst Wireless Gateway devices in Cisco IOS CG Release 17.11.1a:

Caveat	Description
CSCwb77115	When traffic exceeds maximum modem capacity, Cisco Catalyst Wireless Gateway may crash and reboot.

Open Caveats in Cisco vManage Release 20.11.1

In Cisco vManage Release 20.11.1, there are no open caveats that affect Cisco Catalyst Wireless Gateway devices.

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)