Release Notes for Cisco Ultra Reliable Wireless Backhaul on Catalyst IW Access Points, Release 17.14.1

First Published: 2024-04-15

What's New in Ultra-Reliable Wireless Backhaul on Catalyst IW Access Points, Release 17.14.1

The following new features are introduced in Unified Industrial Wireless (UIW) release 17.14.1:

- Dying Gasp functionality is implemented on Catalyst IW9165E. This allows the access point to send a message to the infrastructure when a loss of power occurs, and this message allows the network to stop sending traffic to the offline access point immediately.
- Support for High Availability with MPO.
- Support for 160 MHz channel bandwidth on Catalyst IW9165E.
- Support for Rx-SOP threshold functionality on Catalyst IW9167E.

This Release Note primarily provides information about the URWB mode of operation. For more details about Workgroup Bridge (WGB), check the Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.14.x.

Note Cisco recommends as best practice to upgrade the latest firmware version to use the Cisco URWB software features.

Software Matrix

The following table provides software matrix information:

Unified Industrial Wireless Software Release	Access Point Image Version Number	Supported Access Points
17.14.1	17.14.0.79	Catalyst IW9167E Heavy Duty Access Point Catalyst IW9165E Access Point Catalyst IW9165D Heavy Duty Access Point

Note The Cisco URWB feature is part of the Unified Industrial Wireless software image.

Supported Software and Hardware

The Catalyst IW9167E and IW9165 Access Point supports following software and hardware:

Access Point Model	Unified Industrial Wireless Image	Supported Hardware
Catalyst IW9165	ap1g6m-k9c1	IW9165E-x IW9165D-x
Catalyst IW9167E	ap1g6j-k9c1	IW9167EH-x

Note The Cisco URWB feature is part of the Unified Industrial Wireless software image.

Caveats

Caveats describe unexpected behaviour in Cisco releases in a product. Caveats that are listed as Open in a prior release is carried forward to the next release as either Open or Resolved.

Cisco Bug Search Tool

The Cisco Bug Search Tool allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input. To view the details of a caveat, click the corresponding identifier.

Open Caveats

To know more information about the open caveats, see Cisco Bug Search Tool for Open Caveats.

You can view the list of open caveats using the filter options in the tool.

Resolved Caveats

To know more information about the resolved caveats, see Cisco Bug Search Tool for Resolved Caveats.

You can view the list of resolved caveats using the filter options in the tool.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, refer to https://www.cisco.com/c/en/us/support/index.html

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.

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)