



Cisco Wireless Release 8.7

Product Bulletin

First Published: April 20, 2018

Overview

We are pleased to announce the immediate availability of Cisco® Wireless Release 8.7 for Cisco wireless access points and wireless controllers.

The Network. Intuitive. A platform that is constantly learning / adapting / protecting (security) and is built on Cisco Digital Network Architecture (DNA).

Building on Intent based networking infrastructure, 8.7 features support the following:

- **11ac Wave2 feature parity enhancements**
- **Assurance enhancements**
- **Increased Web Auth scale**
- **Mobility Express Features**
 - **DNA Centre support - WSA agent & enable DNA-C connectivity**
 - **Ability to update s/w during Day 0 using Network PnP**
 - **Support for SFTP software download transfer mode**
 - **Support for Optimal AP Join**
 - **Support for Bi-directional rate limit per client, BSSID and WLAN**
 - **Ability to limit clients per WLAN, per radio**
 - **Support for RLANs**
 - **Support for Passive Clients**
 - **802.1x supplicant support on AP with EAP-TLS and EAP-PEAP**
 - **Walled Garden, Radius NAC**
 - **DNS-based ACLs (Pre-auth ACL, IPv4 only)**
 - **Central Web Authentication**
 - **BYOD support**
 - **Ability to import EAP certificate**
 - **Ability to upload a new OID file**
 - **GUI Enhancements**

Platform Support

Cisco Wireless Release 8.7 is supported on the following platforms:

- Cisco Aironet access points running the Control and Provisioning of Wireless Access Points (CAPWAP) protocol
- Lightweight access points: 3700, 2700, 1700, 702, 702W, 1800 series, 2800 series, 3800 series
- Outdoor and industrial access points: Cisco Aironet 1530, 1540, 1560, and 1570 Series, and Cisco Industrial Wireless 3700 Series
- Modules: AIR-RM3010L-x-K9= and AIR-RM3000M= 3G Module
- Cisco 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller
- Cisco Virtual Wireless Controller (vWLC): VMware vSphere Hypervisor (ESXi) version 5.x or 6.x and KVM
- Cisco Mobility Express
- Cisco Connected Mobile Experiences (CMX)
- Cisco Virtual Mobility Services Engine (vMSE): VMware ESXi and KVM

Management support for Release 8.7 will be delivered as part of Cisco Prime® Infrastructure Release 3.4 and DNAC 1.2.

Recommended Release for Production Deployments

Maintenance Deployment (MD) releases: These long-lived software releases provide bug fixes and ongoing software maintenance.

- Releases 8.3 and 8.5 are the next MD release trains.
- Release 8.0 is the current MD release train, and 8.0.152.0 is the latest recommended release

For additional details, including on early deployment releases, refer to the [Guidelines for Cisco Wireless Software Release Migration Bulletin](#).

Wireless Solutions Compatibility Matrix

The [Wireless Solutions Compatibility Matrix](#) provides detailed information on compatibility across releases for Cisco Prime Infrastructure and Connected Mobile Experiences.

New Wireless Controller, Access Point, and Mobility Express Features

Table 1 New Wireless Controller, Access Point, and Mobility Express Features

Feature	Description	Benefits
---------	-------------	----------

Cisco WLC		
DNS-based ACL Filtering for BYOD	In this release, DNS-based ACL filtering is supported in FlexConnect and Fabric mode.	This gives the flexibility of matching traffic based on destination URL rather than IP addresses associated with the URL, which could change often.
Enhancement to HA Monitoring and Management	The monitoring and management of high availability standby WLC is enhanced to display the serial number and fan status of the standby WLC	Better visibility into the health of the Standby WLC
Encrypted Mobility Tunnel	A secure link called the encrypted mobility tunnel, which is based on mobility tunnel and encrypted using CAPWAP DTLS protocol, can be established between an anchor and a foreign Cisco WLC. The encrypted mobility tunnel feature is supported in high availability (HA) client SSO.	Enhances security by encrypting all WLAN traffic even as it transits between the Foreign and Anchor WLC
Enhancement to RxSOP Threshold Configuration	Prior to this release, if you configure RxSOP threshold on Cisco WLC CLI to a custom value, the Cisco WLC GUI would reflect the threshold value as 'AUTO'. In this release, an option is provided on Cisco WLC GUI to configure a custom RxSOP threshold value.	Allows the customer to tweak their High Density wireless network performance, without having to access the CLI.
Cisco Wave 2 AP		
802.1X Support for EAP-TLS and EAP-PEAP	In this release, 802.1X support is extended to EAP-TLS and PEAP methods along with EAP-FAST method in Cisco Wave 2 APs.	<p>Customers can now use multiple EAP types to authenticate the Access Point, rather than being limited to just EAP-FAST</p> <p>Prior to this release, EAP-FAST was the only supported 802.1X AP-switch port authentication method. EAP-TLS and PEAP methods are supported only in Cisco Wave 2 APs. Cisco Wave 1 APs support only EAP-FAST method</p>

AUX Ethernet Port Enabled on Cisco Wave 2 APs	All wave 2 access points with an Auxiliary Ethernet port shall support downlink connectivity on that port: AP1850, AP2800, AP3800 and also outdoor.	Downlink connectivity shall support RLAN functionality as it is implemented on wall plate access points.
Enable CleanAir, Disable BLE Detection by Default	Prior to this release, if CleanAir was enabled, by default, the BLE beacon was included in the list of interferences to be detected. In 8.7 and later releases, the functionality is changed wherein the BLE beacon is by default excluded from the list of interferences to be detected.	This change in functionality is made to eliminate unwanted off-channel scans to improve performance
Managing BLE Beacons in Cisco Wave 2 APs	BLE beacons are battery-powered, low-cost transmitters integrated with Cisco Wave 2 AP radios and can be used to transmit proximity-based, context-aware messages	This feature provides the ability to perform highly accurate indoor device positioning, app assisted wayfinding and other location related applications. This can also be used to perform proximity/zone-based messaging/advertising and device tagging.
NMSP by AP Groups with Subscription List from CMX	Support is added to send only the required Network Mobility Services Protocol (NMSP) data to CMX (both on premises and cloud based). The CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in Cisco WLC	This filtering helps increase CMX (on-prem and Cloud) scale and also reduces unwanted internet bandwidth charges when the customer is running CMX Cloud
Mobility Express		
Mobility Express Enhancements	DNA Centre support - WSA agent & enable DNA-C connectivity	This release brings Mobility Express to be part of the The Network. Intuitive. Mobility Express is Intent Based Networking ready and is fully integrated with Cisco DNA Center.
	Ability to update s/w during Day 0 using Network PnP	This feature brings makes it easier for Day0 controller configuration and software image download
	Support for SFTP software download transfer mode	This feature allows using SFTP transfer mode for software download resulting in faster and reliable download over slow WAN links

	Support for Optimal AP Join	Optimal AP Join will allow the ME network to provide the image without the need for using any external transfer mode when a new AP Joins an ME network. Currently, feature is supported on Aironet 2800, 3800 and 1560 AP families.
	Walled Garden support	Guest Splash Pages are configured to block Internet access until authentication is complete. However, certain domains must be added to the "Walled Garden" for allowed websites in order to complete the authentication. Wild cards are supported for domain names.
	Central Web Authentication	Central Web Authentication happens after the client fails MAC authentication on AAA. In CWA, the client is redirected to a web portal (ACL and Re-direct URL returned from AAA) where one can enter the username and password. After the credentials are validated by the AAA server, it sends a Change of Authorization (CoA) to the WLC. WLC sends back a COA-ACK to the AAA server and puts the client in run state.
	BYOD Support	Ability to on-board and secure non IT employee devices on the wireless network
	Support for Bi-directional rate limit per client, BSSID and WLAN	Allows customers to set upstream and downstream bandwidth for clients, BSSID and WLAN for efficient bandwidth usage.
	Ability to limit clients per WLAN, per radio	Allows customers to limit the number of clients per radio and WLAN

	Support for Passive Clients	Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. This feature enables the broadcast of ARP requests and the APs respond on behalf of the client.
	Support for RLAN	This feature now enables usage of wired ports along with 802.1X on 1815W with Mobility Express
	802.1x supplicant support on AP with EAP-TLS and EAP-PEAP	AP 802.1X supplicant feature supported in Cisco Wave 2 APs—In the 802.1X authentication scenario between an AP and a Cisco switch, the AP acts as an 802.1X supplicant and is authenticated by the switch using EAP-TLS, EAP-PEAP and EAP-FAST
	Ability to import EAP certificate Ability to upload a new OID file	Ability to add new OID signatures for device profiling
	GUI Enhancements	Allows customers to enable new and advanced features without the need for going to CLI

Note: Please consult the 8.7 Release notes for a detailed list of Wave1 AP features that are now supported in Wave2 APs

Cisco Prime Infrastructure 3.4

Cisco Prime Infrastructure is a network management platform that supports lifecycle management of the entire network infrastructure from one GUI. It provides network administrators with a “single-pane-of-glass” solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust GUIs make device deployments and operations simple and cost-effective.

Cisco Prime Infrastructure 3.4 allows basic monitoring and management of Cisco Wireless Release 8.7 with technology packs to enable new feature support.

Service and Support

Services from Cisco and our partners can help you assess, design, tune, and operate your wireless LAN to transparently integrate mobility services and take advantage of the systemwide capabilities of the Cisco Unified Wireless Network.

Our professional services help you align your interference management, performance, and security needs with your technical requirements to better use the self-healing, self-optimizing features built into the silicon-level intelligence of Cisco CleanAir® technology and the increased performance of the 802.11ac standard. These services can enhance deployment and operational efficiencies to reduce the cost and complexity of transitioning to new technologies.

Our Technical Support Services help you maintain network availability and reduce risk. Optimization services provide ongoing assistance with performance, secure access, and maintaining a strong foundation for business evolution and innovation.

For More Information

For more information about planning, building, and running services for Cisco CleanAir technology, Cisco 802.11ac, and the Cisco Unified Wireless Network, visit Cisco Technical Support Services or Cisco Professional Services at <https://www.cisco.com/go/services>.

For more information about Cisco wireless products, visit <https://www.cisco.com/go/wireless>.

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark

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. 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)

© 2018 Cisco Systems, Inc. All rights reserved.