

Cisco Wireless Release 8.4

PB738891

Overview

We are pleased to announce the immediate availability of Cisco Wireless Release 8.4 for Cisco® wireless access points and wireless LAN controllers.

Digitization continues to accelerate, impacting companies of all sizes and creating the potential for an estimated \$18 trillion of new value¹. With Cisco's new [Cisco Digital Network Architecture \(Cisco DNA\)](#) companies can take full advantage of the digital transformation. With the proliferation of digital devices and IoT, the risks to the network and consequence of data breaches are increasing. From 2013 to 2016 the cost of the average data breach increased by 29%².

New features in the 8.4 release will help customers to lower risk, meet compliance goals more easily, and reduce the operational effort to implement segmentation. For example, companies can easily enhance the security of their wireless environment and protect any device on the network with Cisco Umbrella WLAN. Based on the 8.4 integration with Cisco Umbrella WLAN it has never been easier to access this security enhancement. Additionally, the TrustSec feature available in 8.4 enables Software-Defined Segmentation when used along with ISE. A recent Forrester study found with TrustSec that policy changes are 98% faster and the opex required to make those policy changes is 80% lower³.

Primary Features in Release 8.4

- **Cisco Umbrella WLAN:** [Cisco Umbrella \(OpenDNS\) integration with wireless](#)
- **TrustSec:** TrustSec Software-Defined Segmentation, enables controls to be defined simply by using endpoint roles, instead of using IP addresses
- **ISE enhancement:** Smart default configuration for ISE in Wireless controllers
- **IPv6 support on Wave 2 APs:** All 802.11ac Wave 1 Access Points will provides native IPv6 functionality
- **IPv6 EoGRE Support for Flexconnect Mode Access Points:** IPv6 EoGRE Support on Flexconnect Mode APs allows the ability to establish an IPv6 EoGRE tunnel directly from an AP in Flexconnect mode
- **Ethernet over GRE (EoGRE) support for Wave 2 Access Points:** Ethernet over GRE support for Wave 2 Access Points
- **Cisco Mobility Express:** increased scale up to maximum 100 access points
- **Mesh on AP1560:** Support for mesh/bridging networks with AP1560

¹ <http://www.idc.com/getdoc.jsp?containerId=US40526216>

² "2016 Cost of Data Breach Study: Global Analysis" by IBM and Ponemon Institute LLC

³ <https://www.cisco.com/c/dam/en/us/products/collateral/security/secure-access-control-system/tei-of-cisco-trustsec.pdf>

Platform Support

Cisco Wireless Release 8.4 is supported on the following platforms:

- Cisco Aironet access points running the Control and Provisioning of Wireless Access Points (CAPWAP) protocol
- Lightweight access points: 1600, 1700, 1810 OEAP, 1810W, 1815I, 1815W, 1830, 1850, 2600, 2700, 2800, 3500, 3600, 3700, 3800, 700, 700W, 802, 803, and ASA5506W-AP702
- Outdoor and industrial access points: 1550 (128 MB versions), 1530, 1560, 1570, and IW3700
- Modules: AIR-RM3010L-x-K9= and AIR-RM3000M=
- Cisco 2504 Series Wireless LAN Controllers
- Cisco 5500 (5508 and 5520) Series Wireless LAN Controllers
- Cisco Catalyst® 6500 Series Wireless Services Module 2 (WiSM2)
- Cisco Flex 7500 Series Wireless Controllers
- Cisco 8500 (8510 and 8540) Series Wireless Controllers
- Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Virtual Wireless Controller (vWLC): VMware ESXi, HyperV, and KVM
- Cisco Mobility Express
- Cisco Mobility Services Engine (MSE)
- Cisco Virtual Mobility Services Engine (vMSE): VMware ESXi and KVM

Management support for Release 8.4 will be delivered as part of the Cisco Prime™ Infrastructure Release 3.1.5 and APIC-EM release 1.4

Recommended Release for Production Deployments

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

- Releases 8.0 and 8.3 are the next MD release trains (a release in this train will be qualified as MD).
- Release 7.4 is the current MD release train, and 7.4.140.0 is the latest recommended release.

Early Deployment (ED) releases: These software releases provide new features and new hardware platform support as well as bug fixes.

- Release 8.2 is recommended for customers with 802.11ac deployments. Customers are advised to upgrade to Release 8.2.151.0 to take advantage of multiple software fixes in the release.
- Customers with earlier ED release versions of 7.2, 7.3, 7.5 or 7.6 should upgrade to 8.0.140.0.

Wireless Solutions Compatibility Matrix

The [Wireless Solutions Compatibility Matrix](#) provides detailed information on compatibility across releases for Cisco Prime Infrastructure and Mobility Services Engine (MSE).

New Access Point and Wireless Controller Features

Table 1 describes the new features in Cisco Wireless Release 8.4.

Table 1. New Access Point and WLC Features

Feature	Description	Benefit
Cisco Umbrella WLAN	Cisco Umbrella (OpenDNS) integration with wireless lan controller	Cisco Umbrella WLAN and WLC integration provides web classification and security for clients connecting to Cisco WLC. Key differentiators involve granular web classification and reporting by WLAN, User role and location. This feature will be supported on Cisco WLC 2504, 5508, 8510, 5520, 8540 and WiSM2.
Domain based ACL	Domain based ACL allows administrators to define an domain access control list (ACL) in order to allow or disallow traffic. This additional level of security has been added for wireless to allow user to blacklist or whitelist of a specific set of domains	Domain based ACL extends the ACL from Layer 3 IP to domain based ACL. This feature is support on WLC 8540 and 5520 only.
ISE enhancement	Smart default configuration for ISE in Wireless controllers	Simplified single click day 0 express smart default setup for ISE in the WLAN and WLC configurations.
TrustSec	TrustSec Software-Defined Segmentation, enables controls to be defined simply by using endpoint roles, instead of using IP addresses	<p>Network segmentation is essential for protecting critical business assets, but traditional segmentation approaches involve operational complexity and can be difficult to introduce to existing environments gracefully.</p> <p>By classifying systems using human-friendly logical groups, security rules can be defined using these groups, which are more flexible and much easier to manage than using IP address-based controls.</p> <p>IP addresses do not indicate the role of a system, the type of application a server hosts, the purpose of an IoT device or the threat-state of a system, but a TrustSec Security Group can denote any of these roles.</p> <p>Software-defined segmentation on Access Points and Wireless Controller is much easier to enable and manage than VLAN-based segmentation and can be used for use-cases such as:</p> <ul style="list-style-type: none"> • Restrict the lateral movement of threats with micro-segmentation • Provide rapid threat containment to isolate attacks • Enable scalable BYOD and mobility access controls • Reduce the scope of compliance for regulations such as PCI compliance • Control access to regulated applications in finance and healthcare organizations • Segment IoT devices • Simplify policy management to reduce demands on IT staff • Make firewalls and traffic monitoring tools aware of endpoint roles
Virtual Controller N+1 High Availability	High Availability with N + 1 solution now available on the virtual Wireless LAN Controller	Enhanced virtualization offering with N+1 High Availability. By introducing High Availability on the virtual controller an improved user experience can be delivered. Note please follow the implementation guidelines.
HyperV support for vWLC	Virtual Wireless LAN Controller now supported on the HyperV hypervisor	Support for virtual Wireless LAN Controller (vWLC) on the HyperV hypervisor. Cisco's vWLC is now supported on any x86 server with VMWare Hypervisor ESXi4.x, 5.x, and 6.x as well as KVM and HyperV.
Ethernet over GRE (EoGRE) support for Wave 2 Access Points	Ethernet over GRE support for Wave 2 Access Points	<p>Ethernet over GRE (EoGRE) is a aggregation solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host's traffic is terminated and subscriber sessions are initiated for the end host.</p> <p>This release allows Wave 2 Access Points the ability to establish EoGRE tunnels directly from a Flexconnect Mode access point.</p>
IPv6 EoGRE Support for Flexconnect Mode Access Points	IPv6 EoGRE Support on Flexconnect Mode APs allows the ability to establish an IPv6 EoGRE tunnel directly from an AP in Flexconnect mode	This release brings IPv6 EoGRE tunnel support, providing end to end IPv6 from the Access point to the EoGRE tunnel gateway.
IPv6 support on Wave 2 APs	All 802.11ac Wave 1 Access Points will provides native IPv6 functionality	As more and more networks move to IPv6, Cisco 802.11ac Wave 2 Access Points will support native IPv6 functionality.

Feature	Description	Benefit
Mesh support on the Cisco Aironet AP 1560 series	Mesh support on the Cisco Aironet AP 1560 series allows for Access points to wirelessly mesh over-the-air	Brings mesh support on the AP1560. This allows the access point the option to operate as a mesh mode Root Access Point (RAP) or mesh Access Point (MAP) to form a wireless backhaul network.
Air Time Fairness on 802.11ac Wave 1 Access Points in Mesh Mode	Air Time Fairness (ATF) on 802.11ac Wave 1 Access Points in Mesh Mode allows users to regulate radio resources for mesh networks	Traditional (wired) implementations of QOS regulate egress bandwidth. With wireless networking, the transmission medium is via radio waves that transmit data at varying rates. Instead of regulating egress bandwidth, it makes more sense to regulate the amount of airtime needed to transmit frames. Air Time Fairness (ATF) is a form of wireless QOS that regulates downlink airtime (as opposed to egress bandwidth) for specific SSIDs. The additional of ATF on Mesh, allows for users to implement this feature on mesh networks.
Cisco Aironet AP 1815W support	Cisco Aironet 1815w Access Point brings a full slate of Cisco high-performance functionality to multiple-dwelling-unit deployments	The Cisco® Aironet® 1815w Access Point offers a compact, wall plate-mountable access point, ideal for hospitality, cruise ships, residential halls, or other multiple-dwelling-unit deployments. Packing 802.11ac Wave 2 wireless standards support and Gigabit Ethernet wired connectivity into a sleek device, the 1815w is built to take full advantage of existing cabling infrastructure while blending into the visual footprint. This combination provides best-in-class performance while reducing total cost of ownership.
FlexConnect support for Wave 2 AP's for select features	<ul style="list-style-type: none"> • Proxy ARP • NAT/PAT • QoS override per client 	Proxy ARP – AP will act as an ARP Proxy to respond ARP requests on behalf of wireless clients. NAT/PAT – AP will support NAT/PAT for central DHCP. AAA QoS Override per Client – Clients will be able to assign QOS profile based on AAA.
Increased Mobility Express Scale	Increases the Mobility Express AP Scale to 100 APs	Cisco Mobility Express is a software-based controller function integrated on Cisco Wave 2 Access Points. It is a simplified, feature rich WiFi architecture with enterprise level WLAN capability streamlined for small to mid-sized wireless networks. The 8.4 Software release increases the Mobility Express scale from 25 APs per Mobility Express Controller to max 100 APs.
Mobility Express provisioning using Plug and Play (PnP)	PnP ability to configure Mobility Express controller using the APIC-EM	Helps preprovision Mobility Express controller from a central service (APIC-EM), even eliminating need for specific expertise on-site.
WeChat Support	Easy Wi-Fi Connectivity using the WeChat App	Support Wechat App for easy Wi-Fi connectivity by QR-code scanning to redirection or captive portal redirection.
LAG in Transition	Additional Configuration support for WLCs which are being converted to and from LAG mode	Cisco WLCs which support Link aggregation (LAG) goes into a LAG-in-Transition (LAT) mode during transition between LAG to non-LAG mode or vice versa. The transition is complete only when the WLC is rebooted. During the LAT mode, the user can make configuration or interface changes and also revert to the previous LAG mode. And when the WLC is rebooted, it can lead to configuration loss or system failure during reboot. This feature, prevents such incidents by restricting interface-related configuration changes when the WLC is in LAT state.
Guest User Management - Client Whitelisting	Simplified Guest Management	Locations like a university receives many guests with multiple devices (clients). It becomes eminent to protect the network from misuse or unauthorized access and allow legitimate clients to connect to the network. Registering or deregistering of clients is a tedious and time consuming task to perform on regular basis requiring a simpler solution. This feature addresses the need of whitelisting clients on a particular WLAN or SSID based on MAC address. For this purpose, the currently existing features will be reused - mac filtering option on WLAN, adding lobby admin user and reuse AAA DB to store the list of whitelisted clients on a WLAN. This feature administration is managed by two administrators: Global Administrator—creates a lobby admin user on the WLC and enables lobby administrator access on a WLAN. Lobby Administrator—adds or deletes the clients from a whitelist to manage the association to a WLAN or SSID through GUI interface only. Existing lobby administrators can also be used to configure the whitelists.

Cisco Prime Infrastructure 3.1.5

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 3.1.5 (PI 3.1 MR 5) allows basic monitoring and management of Cisco Wireless Release 8.4 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 <http://www.cisco.com/go/services>.

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



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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 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)