Miercom

An Independent Assessment:

Simplified Wi-Fi Deployment Using
Cisco Embedded Wireless Controller

CISCO

DR200420E

June 2020

Miercom

www.miercom.com

Contents

1 - Executive Summary

Miercom tested the Cisco Embedded Wireless Controller (EWC) – combining the most advanced controller – the Cisco Catalyst 9800 Series Wireless Controllers – with the latest Wi-Fi 6 access points – the Cisco Catalyst 9100 Access Points – creating a best-in-class wireless experience for your evolving and growing organization. This Cisco EWC is the successor of Mobility Express, the First Embedded Wireless Controller Solution Miercom tested in Sep 2018. This time, Cisco returns with a much more powerful and vastly improved second generation solution. The Cisco EWC solution is one of the easiest wireless products to deploy that we've encountered to date. Featuring a new mobile wireless application for management, and a straightforward built-in WebUI, a full enterprise class feature set, the deployability of the Cisco 9100 APs with EWC from small businesses to large distributed enterprises clearly exceeded our expectations. The solution poses an excellent value as EWC is all inclusive with the purchase of the new Cisco Catalyst 9100 APs and has upward scalability for investment protection for installations requiring more than 100 APs and/or 2,000 concurrent clients. Cisco EWC can easily scale up to 100 APs and 2,000 wireless clients per instance, while accommodating small to medium sized businesses or distributed enterprises with one or many distributed sites.

Key Findings and Observations:

- **Integrated Wireless Controller** – EWC integrates a Wireless controller directly on all the latest Catalyst 9100 APs requiring no other physical controller hardware or software making this solution an excellent value, and very efficient for small to medium sites or branch deployments.
- **Simplified Setup -** Cisco's EWC on the AP, over-the-air provisioning can use the Cisco Catalyst Wireless mobile app, or the built-in WebUI for quick and effective setup. We accomplished a straight out-of-box setup within 10 minutes! For multisite deployments Cisco DNA center Plug n Play option can be utilized as well.
- **Advanced Enterprise Features** - Cisco's EWC is a game changer. Other vendors' products with built in all-in-one controller have nowhere near the feature set and enterprise capabilities found in Cisco's EWC.
- **Comprehensive Wi-Fi Security** - Advanced Wireless Intrusion Prevention (aWIPs), Multi Pre-Shared key (mPSK) and Identity Pre-Shared-Key (iPSK for IoT and BYOD), coupled with advanced telemetry and Assurance – Insights afford Cisco's wireless solution to be a clear choice for small and mid-size businesses. EWC fully supports the latest WPA3 Security Standard.
- **Best in Class Security** – Cisco Catalyst 9100 with EWC and Cisco Umbrella achieved better security efficacy for malware, phishing and ransomware than all other WiFi security solutions we have evaluated to date.
- **Enterprise Management** – Optionally, Cisco's EWC fully integrates with Cisco Digital Network Architecture Center (Cisco DNA Center) enterprise automation and management systems to enable deployment, provisioning, monitoring, and troubleshooting for distributed enterprises.
- **Investment Protection** – Cisco's EWC allows for cost effective migration to a standalone controller solution for customers requiring more than 100 APs

Having evaluated the features, security efficacy, ease of deployment of Cisco's Embedded Wireless Controller, we found this solution superior in use for single and multi-site enterprise-grade Wi-Fi networks. Minimal technical expertise is required to reap the rewards included in this robust enterprise WiFi solution. We are proud to present the **Miercom Performance Verified** certification to Cisco's for the Embedded Wireless Controller solution.

Robert Smithers, CEO

Miercom

2 - Simplicity in Deployment and Manageability

We installed the Cisco Catalyst 9100 APs with EWC trying both the Mobile App as well as the WebUI. We found both to be simple and effective to use. It depends on the administrators' preference which path they are most comfortable for the initial setup of the Embedded Wireless Controller (on same or separate APs). In our review, this setup process took less than 10 minutes for either method.

2.1 Configuring Cisco Embedded Wireless Controller via WebUI

We were able to configure the DUT and conduct all initial setup for the Embedded Wireless Controller on the Catalyst 9100 in 8 minutes, which was even better than the advertised 10-minute installation claims in Cisco literature.

We used the mywifi.cisco.com URL for accessing EWC-AP and then worked through the WebUI. Deployment was simple using DHCP, there was no need for static IP address management, but full options were available to meet any customer environment. We found the WebUI to be very straightforward and were surprised everything simply just worked, even without requiring a reboot of the AP after the Day 0 configuration and setup.
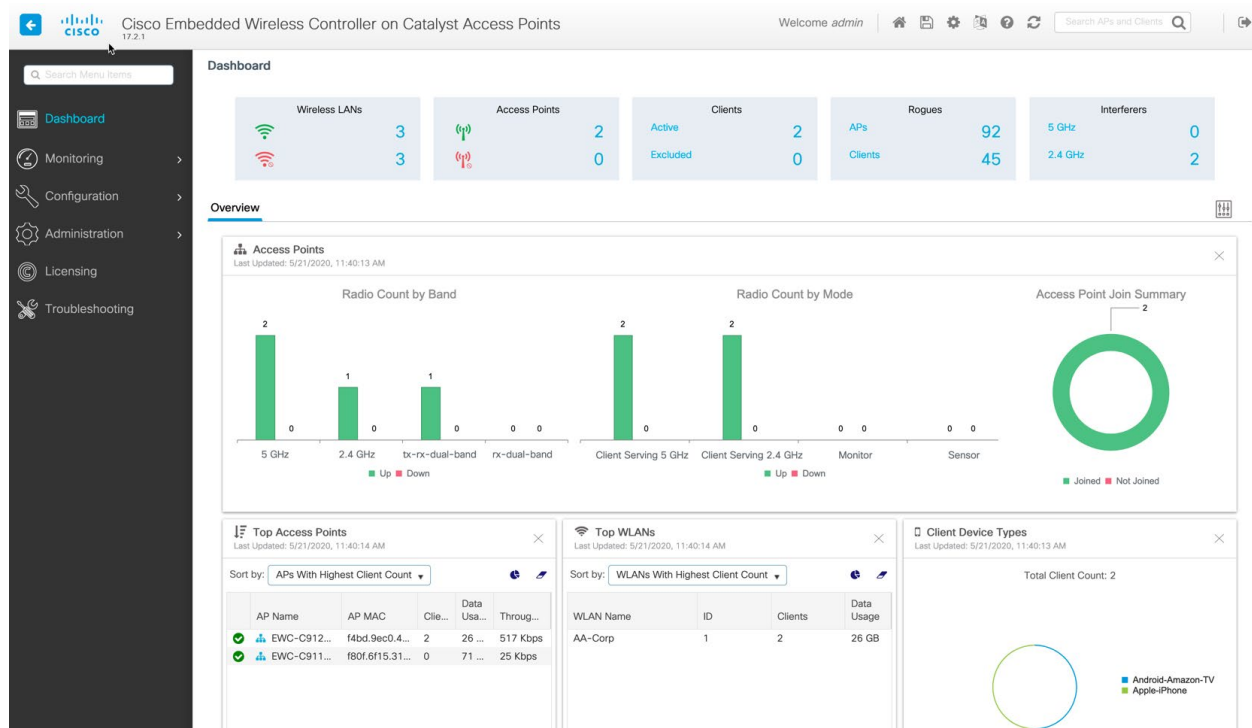
Cisco EWC WebUI offers full management visibility and control through this very straightforward interface. We found the layout and design very intuitive with smartly laid out default widgets of commonly needed statistics.   These are completely configurable to customers' liking.
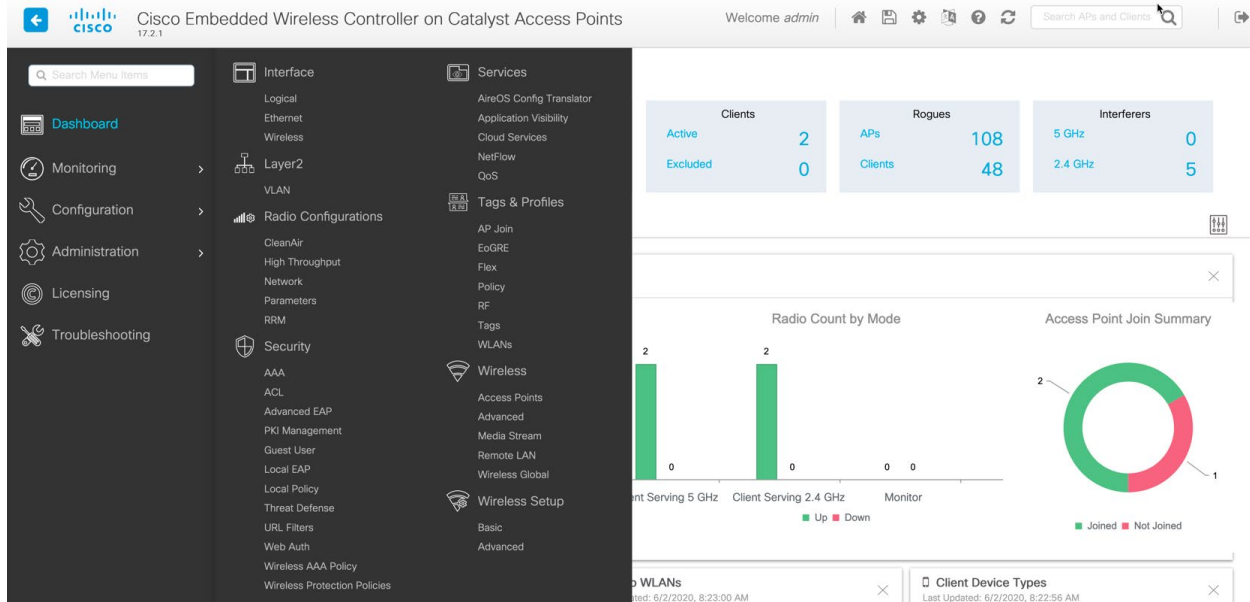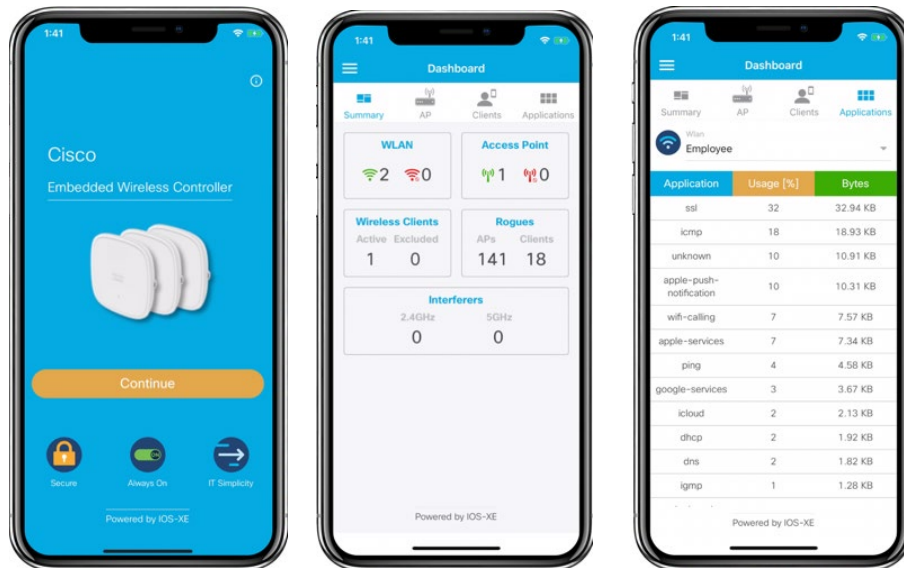
Cisco EWC WebUI offers excellent manageability through this very straightforward interface. We found the layout and design very intuitive with "nesting" and drill down access to settings for features on the toolbar left. Always having access to as little or as much as needed made navigating the Cisco WebUI a breeze. Offering a search option whichallows users to freely enter any keyword as needed for configuration, and eliminating the need to go over menus to find a specific feature. Cisco claims the same WebUI is used on dedicated Wireless Controller, Catalyst 9800. Supporting easy migratation to Catalyst 9800 for future larger, campus type deployment.

## 2.2 Simplified and Intuitive Deployment through Wireless Mobile App

Cisco

The Cisco Catalyst Wireless Mobile App for Android or Apple iOS is available on Google play (https://play.google.com/store/apps/details?id=com.cisco.catalystwireless) or the App Store (https://apps.apple.com/us/app/cisco-catalyst-wireless/id1498825806,)

 (we used iOS for the evaluation) and allows for easy deployment, monitoring and management as an alternative to the WebUI. There are Wizard-driven provisioning flows, and access to the comprehensive feature set was all there in the mobile app. We could not find anything missing in the mobile app that we wanted to do for configuration and management of the wireless system under test.

Cisco Catalyst Wireless mobile app offers excellent manageability through a very accessible straightforward interface. We found the layout and design very intuitive, very well-designed app allowing for inventory, configuration and deployment, monitoring.
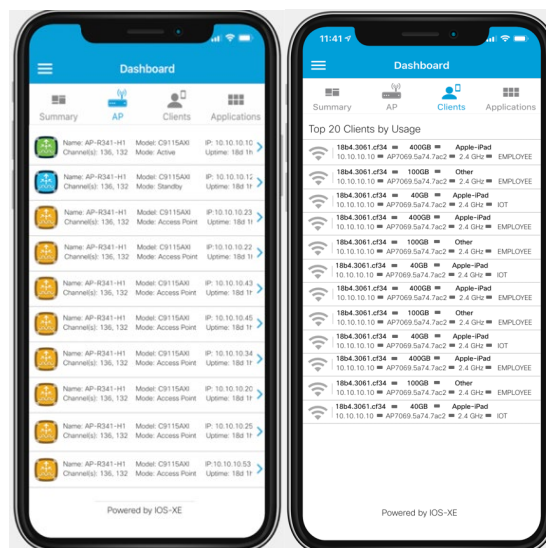
Cisco Catalyst Wireless mobile app has an intuitive dashboard to view the fleet of APs, Top Users / Clients, and other statistics for the wireless network. Simple and thorough visibility offers effective insight into device status and overall wireless network health. One of additional unique advantage is best practice configuration menu. Cisco EWC provide the best wireless configuration recommendation from the Mobile App or Web Interface so any level's of user can easily apply the best practice of Wireless configuration.

3 - Advanced Enterprise Features

In terms of Wi-Fi network operations, Cisco Embedded Wireless Controller exceeds expectations with a rich feature set as well as advanced unique features differentiating Cisco EWC from its competitors.

3.1 Embedded Wireless Controller– Enterprise Feature Set Validated

Partial list of Enterprise-ready feature set validated:

- o Best-in-class Cisco RF innovations like Flexible Radio Assignment (FRA), Cisco CleanAir, Cisco HDX (High Density Experience) and Spectrum Intelligence are all supported on Embedded Wireless Controller for a small site with a few clients or a site with many clients, a high-density environment
- o AAA Override on WLANs (SSIDs) – The Authentication, Authorization and Accounting override option of a VLAN, lets the administrator configure the wireless network for RADIUS authentication and apply VLAN, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on attributes from returned an AAA server
- o Application Visibility and Control – The ability to identify applications being accessed by clients and to apply controls to rate limit, drop or mark traffic on those applications
- o Guest Solutions – The ability of the product to offer and support a comprehensive suite of Guest WLAN options including Lobby Ambassador, Walled garden and Central Web authentication
- o Optimizations for Apple devices – With Cisco and Apple partnership, enterprise features such as roaming, prioritization of business app and iOS client analytics
- o mDNS Gateway –Required in K-12 deployments, allows mDNS services to be learned and offered to clients across multiple wired and wireless networks (included in release 17.3)
- o Controller Redundancy – There is always a standby controller, even if elected automatically incase the active controller is interrupted. Flexibility is present to designate preferred standby controllers
- o Cisco Umbrella integration with Embedded Wireless Controller allows blocking of malicious URLs, malware, ransomware and phishing exploits. Malicious domains are blocked even before a connection is made to preemptively stop threat
- o Programable interfaces with NETCONF/YANG for automation, configuration and monitoring.
- o Over the air threat detection and mitigation through advance rogues and wips capabilities

3.2 Embedded Wireless Controller– High Availability Failover

We observed failover from "Active" to a "Standby" AP running Embedded Wireless Controller. Active and standby controllers were running simultaneously on two Cisco Catalyst 9100 with EWC while both serving clients. Active Wi-Fi network traffic including a continuous ICMP (ping) sweep from clients connected through subordinate APs was unaffected. We monitored continuous uninterrupted traffic while the switchover occurred from primary to secondary controller. We were able to designate an AP as preferred active controller to steer recovery and healing of interrupted AP. ***We noted failover in less than 10 seconds with no interrupted network traffic observed***. After failover another access point in the network was elected to become a standby, providing further redundancy and healing.

3.3 Hot Patch and Service Pack Installation Without Service Interruption

The second high availability test we conducted was to apply a hot patch update to the controller software on the AP. We proved this could be done without a major firmware upgrade, without a reboot and without any service interruption! ***We were impressed with the ability to selectively roll out these update or patches to the managed APs, 5%, 15%, 25%*** or "one Shot" to allow the administrator to roll out firmware patches selectively for uptime management. In our test we observed no traffic interruption, and no packet loss as this hot patch feature add was applied.
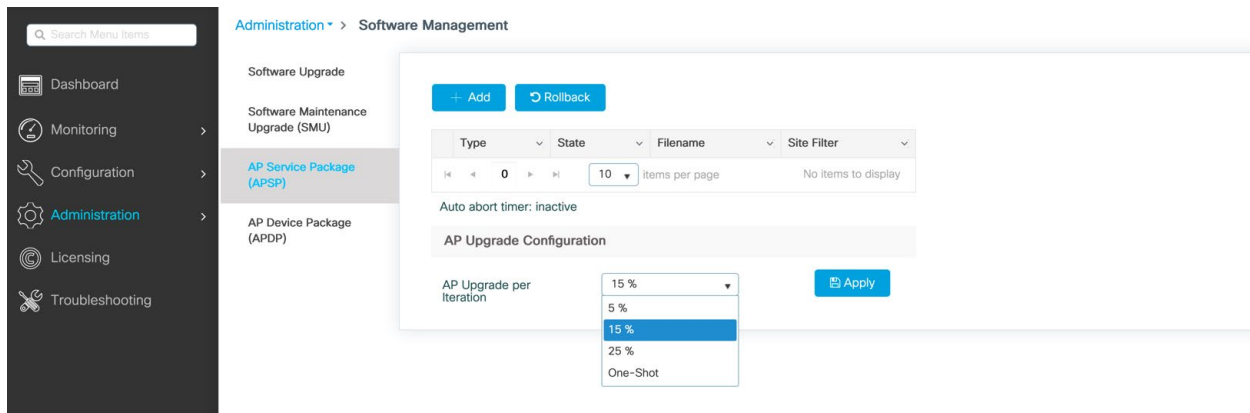
EWC features an incremental hot patch rollout to maximize network uptime. We were impressed with the ability to selectively roll out these update or patches to the managed APs, 5%, 15%, 25% or "one Shot" to allow the administrator to roll out firmware patches selectively for uptime management. In our test we observed no traffic interruption, and no packet loss as this hot patch for a customer requested feature add was applied.
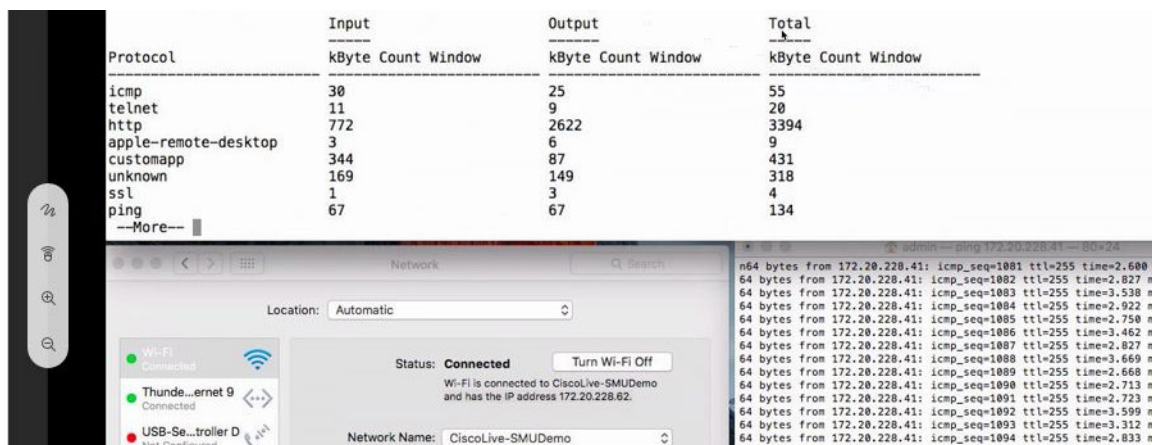
During the EWC feature upgrade evaluation we observed no traffic interruption, and zero packet loss as this hot patch was applied. A continuous ping sweep through the APs under test was observed uninhibited while this additional feature patch was applied to the AP.

4 - Security

4.1 Relative Security Assessment

We compared the Cisco security countermeasures to other leading WiFi vendors including HP/Aruba, Ruckus, Huawei and Ubiquity as to their abilities to thwart the latest and most lethal phishing, ransomware and other malware threats.

Cisco Catalyst 9100 with EWC and Cisco Umbrella achieved an amazing 97% detection rate, currently the highest in the industry at the time of this publishing for initial detection of malicious content including malware via malicious URLs, phishing attempts and ransomware. This is compared to the industry average of 73% of other vendors solutions evaluated. Further Cisco achieved a perfect 100% detection rate within the first day of learning the newly discovered threats. Cisco's implementation of DNS blocking and malicious URL detection was proven competitively superior to other product offerings we have tested.

4.2 Cisco DNA Center

Cisco EWC is fully compatible with Cisco's DNA Center. Although EWC offers excellent management built in for day to day actions though the WebUI and the mobile application, customers seeking even more orchestration, scalability may wish to integrate with Cisco DNA Center.
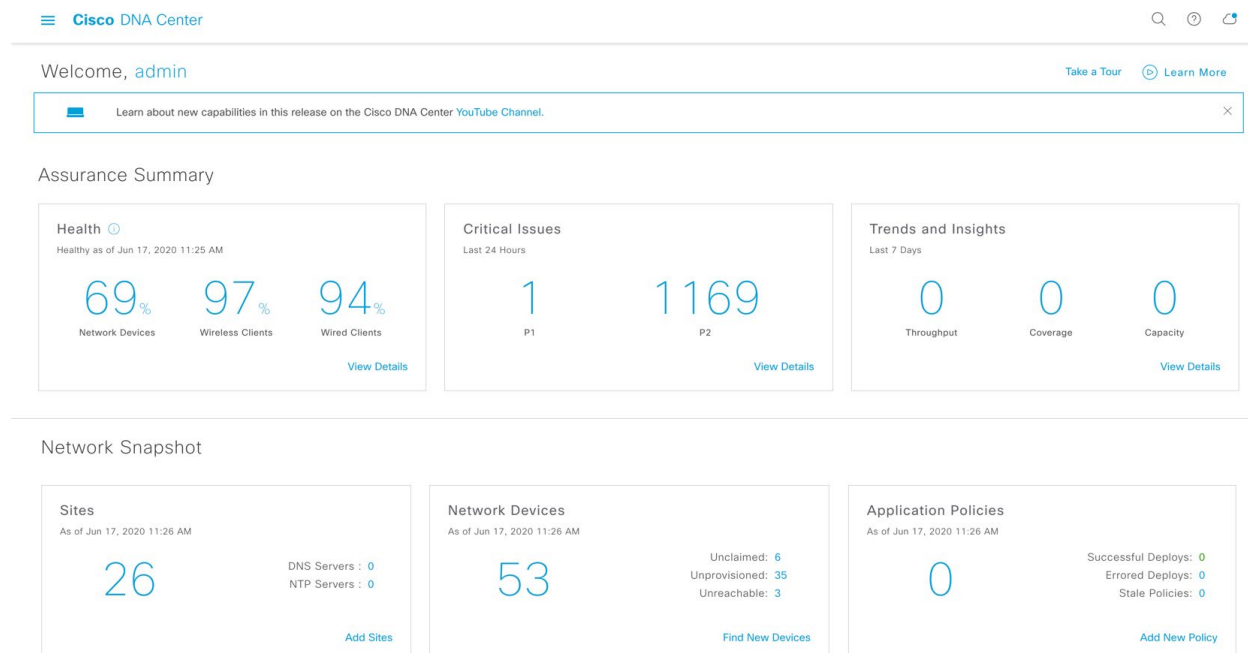
Cisco DNA Center is Cisco's latest management and orchestration solution and offers similar capabilities to the Cisco Prime Infrastructure. Cisco DNA Center is Cisco's long-term committment to overall network monitoring and management, along with other additional features like hierarchy-

based day-0 network design and provisioning capabilities (e.g. Automation, SD-Access) and Day-2 operational insight using Assurance module. With Cisco DNA Assurance for Embedded Wireless Controller, network administrators now have the same troubleshooting tools and capabilities available for EWC-based deployments. Network 360, Client 360, Device 360, Client Real Time Packet Capture and Analysis, Anomaly Detection and other capabilities are supported by Embedded Wireless Controller.
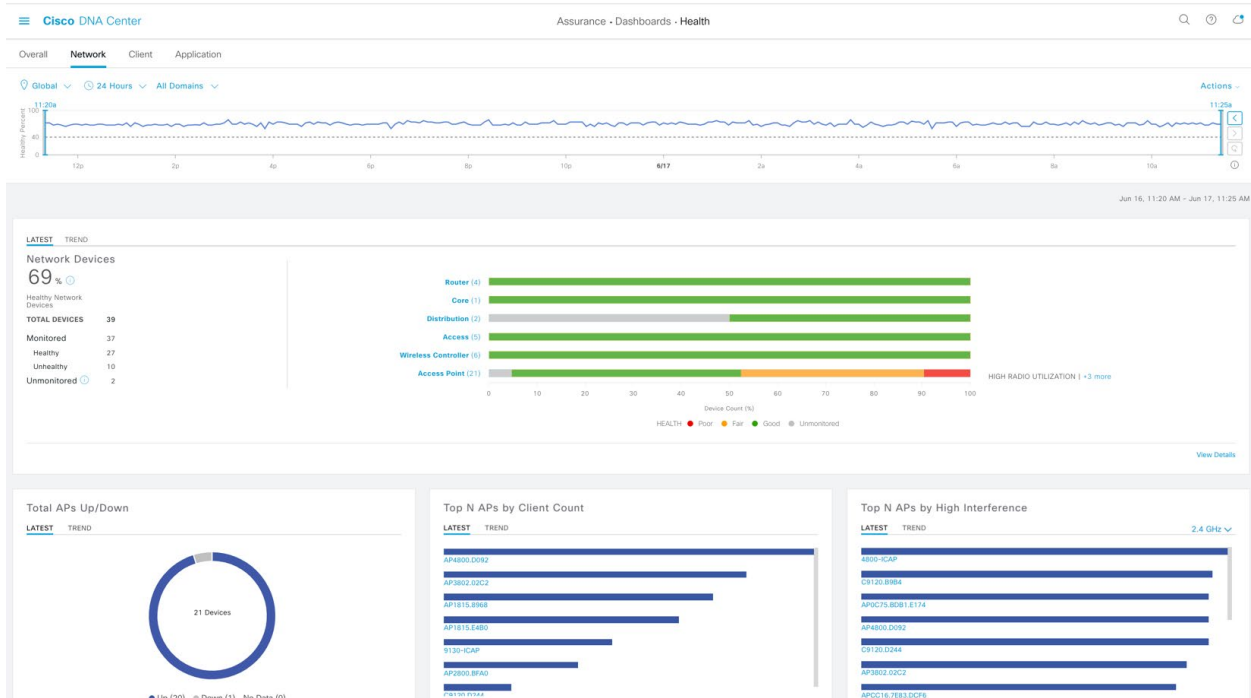
Cisco DNA Assurance automatically collects and organizes device, application and user data over a period of time. Data is correlated and analyzed to provide actionable insight that network managers can use to troubleshoot and improve performance. This helps administrators make smarter decisions before users are affected by service-impacting issues in the end-to-end wired and wireless network. All events are logged and accessible at any point in time for further analysis. Administrators can take real-time packet captures for a deeper dive while troubleshooting.

Cisco DNA Assurance addresses four main categories:

1. Health Monitoring – Is the network performing well for all users, devices and applications? Including dedicate Wi-Fi 6 Analytics Dashboard.

2. Fault Detection – What issues are being reported by the network and sensors?
3. Root-Cause Analysis – Issue Identification, Severity, and Patch Fix Verification
4. Sensor Tests – Over 15 synthetic tests using network sensors evaluate and benchmark performance
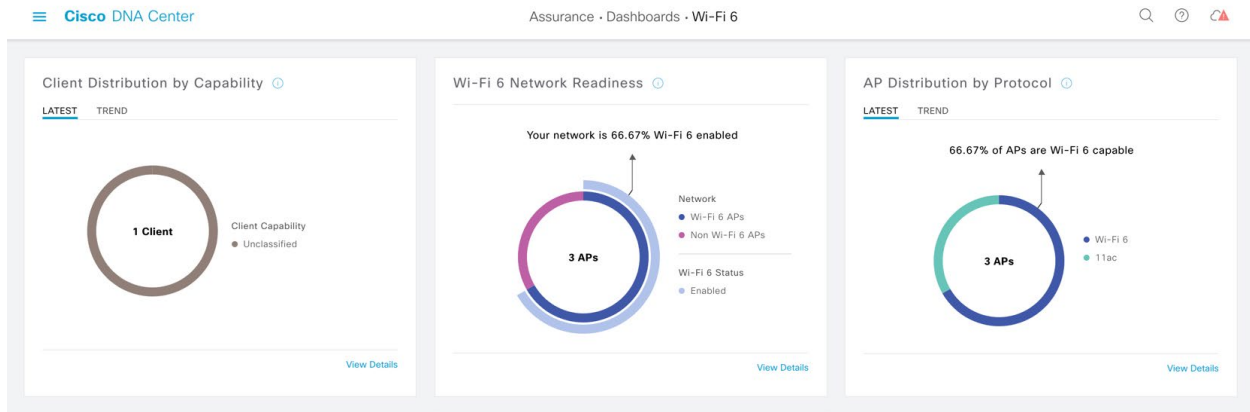
Cisco DNA Assurance also leverage client device ecosystem partnership from Apple and Samsung. It displays unique client-side analytics view from Cisco DNA Assurance screen from Apple iOS devices and Samsung S10 or newer Samsung Smartphones.

Among the insightful DNA Center tools is the AP performance view (by selecting "Wireless Dashboard" and then "Client Performance"). APs are graphically shown by operating frequency band, traffic, interference, RSSI and available capacity.

The same screen shows client density by AP and by frequency band and many other comprehensive data points.
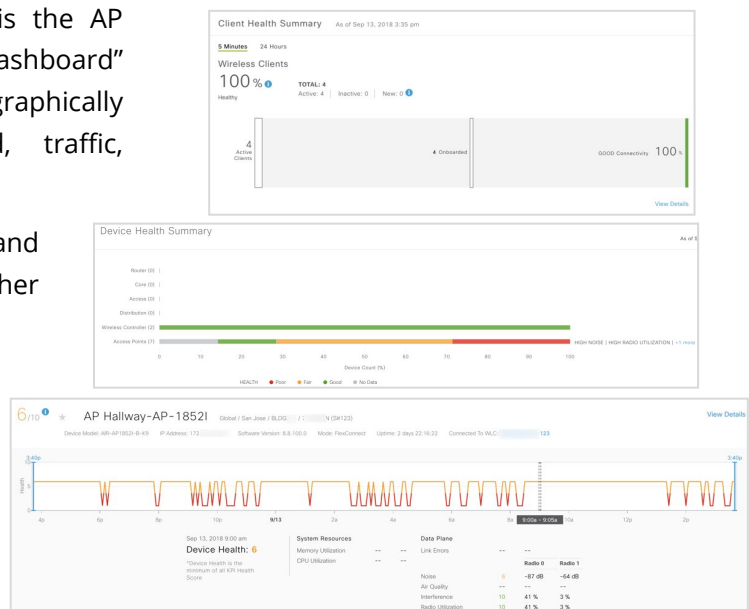
5 - Investment Protection and Future Proof

Cisco EWC by design in inherently scalable to grow with customer needs with complete investment protection. The Wi-Fi 6 based, Catalyst 9100 APs with EWC easily manage up to 100 APs and 2,000 user / client connections, while it can support up to 100 APs as subordinate APs, which is not only supporting same Wi-Fi 6 Catalyst 9100 series but also supports 802.11ac Wave-2. APs. To scale beyond that, dedicated premise or cloud-based controller options are available and the same APs can be utilized. Deployment rollout for upgrading for greater scalability can be done all at once or gradual roll out. The Catalyst 9100 with EWC is a scalable future proof investment for customers.

Embedded wireless controller WLAN deployment
Next-gen Wi-Fi designed for single or multi-site small to medium-sized enterprise
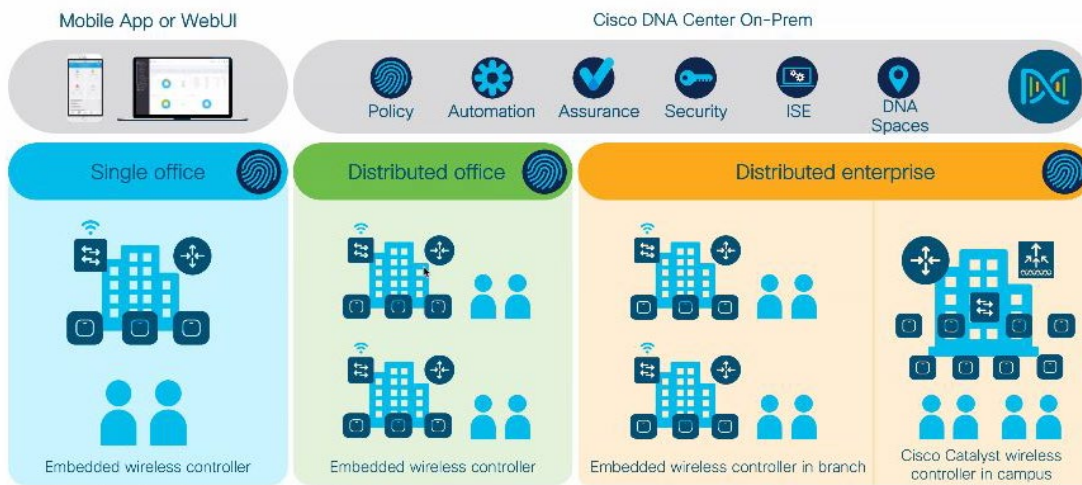
About "Miercom Performance Verified" Testing

This report was sponsored by Cisco Systems, Inc. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

About Miercom

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Cisco Systems, Inc. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.