



The bridge to possible

[Data sheet](#)
Cisco Public

Cisco Catalyst 9800-40 Wireless Controller

Built from the ground up for intent-based
networking

Contents

Product overview	3
Features	4
Details	5
Benefits	11
Specifications	13
Software requirements	17
Licensing	17
Warranty	19
Cisco environmental sustainability	19
Ordering information	20
Cisco Capital	20

Product overview



Figure 1.
Cisco Catalyst 9800-40 Wireless Controller

Built from the ground-up for intent-based networking and Cisco DNA, Cisco® Catalyst® 9800 Series Wireless Controllers are Cisco IOS® XE based and integrate the RF excellence of Cisco Aironet® access points, creating a best-in-class wireless experience for your evolving and growing organization. The 9800 Series is built on an open and programmable architecture with built-in security, streaming telemetry, and rich analytics.

The Cisco Catalyst 9800 Series Wireless Controllers are built on the three pillars of network excellence— always on, secure, and deployed anywhere—which strengthen the network by providing the best wireless experience without compromise, while saving time and money.

The Cisco Catalyst 9800-40 is a fixed wireless controller with seamless software updates for midsize and large enterprises. It is feature rich and enterprise ready to power your business-critical operations and transform end-customer experiences:

- High availability and seamless software updates, enabled by hot and cold patching, keep your clients and services **always** on during planned and unplanned events.
- **Secure** air, devices, and users with the Cisco Catalyst 9800-40. Wireless infrastructure becomes the strongest first line of defense with Cisco Encrypted Traffic Analytics (ETA) and Software-Defined Access (SD-Access). The controller comes with built-in security: Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity.
- Built on a modular operating system, the 9800-40 features open and programmable APIs that enable **automation** of day-0 to day-N network operations. Model-driven streaming telemetry provides deep insights into the **health of your network and clients**.
- Cisco User Defined Network, a feature available in Cisco DNA Center, allows IT to give end users control of their very own wireless network partition on a shared network. End users can then remotely and securely deploy their devices on this network. Perfect for university dormitories or extended hospital stays, Cisco User Defined Network grants both device security and control, allowing each user to choose who can connect to their network. (Available second half of calendar year 2020.)
- The Wi-Fi 6 readiness dashboard is a new dashboard in the Assurance menu of Cisco DNA Center. It will look through the inventory of all devices on the network and verify device, software, and client compatibility with the new Wi-Fi 6 standard. After upgrading, advanced wireless analytics will indicate performance and capacity gains as a result of the Wi-Fi 6 deployment. This is an incredible tool that will help your team define where and how the wireless network should be upgraded. It will also give you insights into the access point distribution by protocol (802.11 ac/n/abg), wireless airtime efficiency by protocol, and granular performance metrics.
- With Cisco In Service Software Upgrade (ISSU), network downtime during a software update or upgrade is a thing of the past. ISSU is a complete image upgrade and update while the network is

still running. The software image—or patch—is pushed onto the wireless controller while traffic forwarding continues uninterrupted. All access point and client sessions are retained during the upgrade process. With just a click, your network automatically upgrades to the newest software.

Features

Table 1. Key features

Metric	Value
Maximum number of access points	Up to 2000
Maximum number of clients	32,000
Maximum throughput	Up to 40 Gbps
Maximum WLANs	4096
Maximum VLANs	4096
Maximum site tags	2000
Maximum Flex® APs per site	100
Maximum policy tags	2000
Maximum RF tags	2000
Maximum RF profiles	4000
Maximum policy profiles	1000
Maximum Flex profiles	2000
Interfaces	4x 10G/1x 1G SFP+/SFP
Power supply	AC power with optional redundant AC power
Maximum power consumption	381W
Deployment modes	Centralized, Cisco FlexConnect®, and Fabric Wireless (SD-Access)
Form factor	1RU
License	Smart License enabled
Operating system	Cisco IOS XE
Management	Cisco DNA Center, Cisco Prime® Infrastructure, integrated WebUI, and third party (open standards APIs)*

Metric	Value
Interoperability	AireOS-based controllers*
Policy engine	Cisco Identity Services Engine (ISE)*
Location platform	Cisco Connected Mobile Experiences (CMX), Cisco DNA Spaces*
Access points	Aironet 802.11ac Wave 1 and Wave 2 access points, Cisco Catalyst 9100 802.11ax access points

*For information on compatibility: [Compatibility Guide](#)

Always on

Seamless software updates enable faster resolution of critical issues, introduction of new access points with zero downtime, and flexible software upgrades. Stateful switchover (SSO) with 1:1 active standby and N+1 redundancy keeps your network, services, and clients always on, even in unplanned events.

Secure

Secure air, devices, and users with the Cisco Catalyst 9800-40 Wireless Controller. Wireless infrastructure becomes the strongest first line of defense with ETA and SD-Access. The controller comes with built-in security: Secure Boot, runtime defenses, image signing, integrity verification, and hardware authenticity.

Open and programmable

The controller is built on the Cisco IOS XE operating system, which offers a rich set of open standards-based programmable APIs and model-driven telemetry that provide an easy way to automate day-0 to day-N network operations.

Details



Physical dimensions

Table 2. Physical dimensions

Dimension	Value
Width	17.3 inches (43.94 cm)
Depth	19.5 inches (49.53 cm)
Height	1.72 inches (4.37 cm)
Weight	22.8 lb (10.34 kg)

Front panel



Figure 2.
Front panel

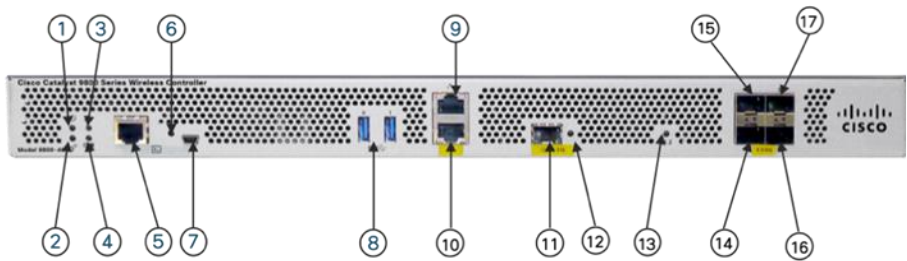


Figure 3.
Front panel components

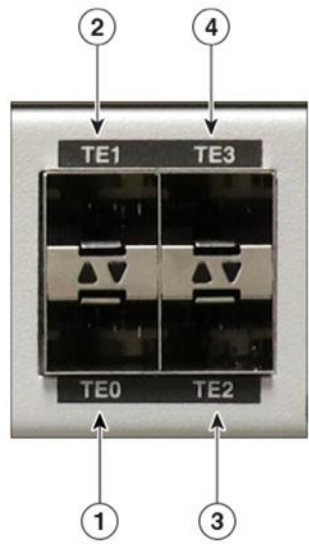


Figure 4.
10G/1G ports

Table 3. Descriptions of front panel components

Label	Component
1	PWR: Power LED
2	SYS: System LED
3	ALM: Alarm LED
4	HA: High-availability LED

Label	Component
5	CON: RJ-45 compatible console port
6	EN: USB console-enabled LED
7	CON: Mini USB console port
8	USB ports 0 and 1
9	SP: RJ-45 10/100/1000 management Ethernet port
10	RP: RJ-45 10/100/1000 redundancy Ethernet port
11	RP: 1 GE SFP port (the only SFPs supported on the RP port are GLC-SX-MMD and GLC-LH-SMD)
12	LINK: RJ-45 connector LED
13	SSD: SSD activity LED
14	TE0: 1 GE SFP/10 GE SFP+ port 0
15	TE1: 1 GE SFP/10 GE SFP+ port 1
16	TE2: 1 GE SFP/10 GE SFP+ port 2
17	TE3: 1 GE SFP/10 GE SFP+ port 3

Ports

Table 4. Ports and their purpose

Port	Purpose
1x RJ-45 console port	Console port for out-of-band management
1x USB 3.0 console port	Console port for out-of-band management
2x USB 3.0 ports	USB 3.0 ports for plugging in external memory
1x RJ-45 management port	Management port used for out-of-band management. Also known as service port
1x RJ-45 redundancy port	Redundancy port used for SSO
1x SFP Gigabit Ethernet redundancy port	Redundancy port used for SSO <ul style="list-style-type: none"> Redundancy port used for SSO; works with Cisco supported SFPs (GLC-LH-SMD and GLC-SX-MMD) for RP port

Port	Purpose
4x 10G/1G SFP+ or SFP ports	Ports used for sending and receiving traffic between access points and controller, northbound traffic, in-band management traffic, and wireless client traffic. Must be connected to the switch

Front panel LEDs

Table 5. Front panel LEDs

LED	Color	Function
Power	Green	Green if all power rails are within spec
System status	Green	On: IOS has boot complete Blinking: IOS boot in progress
	Amber	On: System crash Blinking: Secure boot failure Off: ROMMON boot
High Availability	Green	On: HA active Blinking: HA standby hot
	Amber	Slow blink: Booted with HA standby cold Fast blink: HA maintenance
Alarm	Green	On: ROMMON boot complete Blinking: System upgrade in progress
	Amber	On: ROMMON boot and SYSTEM bootup Blinking: Temperature err and secure boot failure
USB console	Green	When LED is lit, USB Console is enabled (RJ-45 console is disabled)
SSD activity	Green	Indicates active use of the hard disk SSD memory devices in the unit
Network link	Green	Solid green indicates link
		Flashing green indicates activity

Rear panel

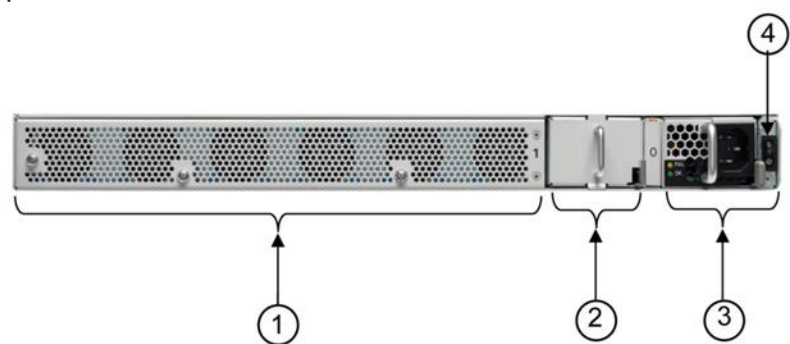


Figure 5.
Rear panel

Table 6. Descriptions of rear panel components

Label	Component
1	Fans
2	Optional redundant power supply (PEM 1)
3	Power supply (PEM 0)
4	Power/standby switch

Rear panel LEDs

Table 7. Power LEDs

Green LED	Amber LED	Power supply status
Off	Off	No AC power to all power supplies
Off	On	Power supply failure (includes over voltage, over current, over temperature, and fan failure)
Off	1 Hz blinking	Power supply warning events in which the power supply continues to operate (high temperature, high power, and slow fan)
1 Hz blinking	Off	AC present, 12VSB on (power supply off)
On	Off	Power supply on and OK

Power

The 9800-40 controller supports an optional redundant AC power supply.

The AC input ranges are as follows:

- Worldwide ranging AC input range (90 to 264 VAC)

The power entry modules (PEMs) provide redundant power to the system, and the 9800-40 can operate continuously with only a single PEM installed. The PEMs are hot-swappable, and replacement of a single PEM can be made without power interruption to the system. All external connections to the PEMs are made from the rear panel of the chassis, and they are removed or inserted from the rear. The main power switch for the unit is located directly next to the PEMs on the rear of the chassis.

SFPs supported

The four data ports can operate in either 10G or 1G mode.

Note: 10/100-Mbps operation is not supported.

Table 8. SFPs supported

Type	Modules supported
Small Form-Factor Pluggable (SFP)	GLC-BX-D
	GLC-BX-U
	GLC-LH-SMD
	GLC-SX-MMD
	GLC-ZX-SMD
	GLC-TE
Enhanced SFP (SFP+)	SFP-10G-SR
	SFP-10G-SR-S
	SFP-10G-SR-X
	SFP-10G-LR
	SFP-10G-LRM
	SFP-10G-LR-X
	SFP-10G-ER
	SFP-10G-ZR
	SFP-H10GB-ACU7M

Type	Modules supported
	SFP-H10GB-ACU10M
	DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41

Benefits

Cisco IOS XE opens a completely new paradigm in network configuration, operation, and monitoring through network automation. Cisco's automation solution is open, standards-based, and extensible across the entire lifecycle of a network device. The various mechanisms that bring about network automation are outlined below, based on a device lifecycle.

- **Automated device provisioning:** This is the ability to automate the process of upgrading software images and installing configuration files on Cisco access points when they are being deployed in the network for the first time. Cisco provides turnkey solutions such as Plug and Play (PnP) that enable an effortless and automated deployment.
- **API-driven configuration:** Modern wireless controllers such as the Cisco Catalyst 9800-40 Wireless Controller support a wide range of automation features and provide robust open APIs over Network Configuration Protocol (NETCONF) using YANG data models for external tools, both off-the-shelf and custom built, to automatically provision network resources.
- **Granular visibility:** Model-driven telemetry provides a mechanism to stream data from a wireless controller to a destination. The data to be streamed is driven through subscription to a data set in a YANG model. The subscribed data set is streamed out to the destination at configured intervals. Additionally, Cisco IOS XE enables the push model, which provides near-real-time monitoring of the network, leading to quick detection and rectification of failures.
- **Seamless software upgrades and patching:** To enhance OS resilience, Cisco IOS XE supports patching, which provides fixes for critical bugs and security vulnerabilities between regular maintenance releases. This support allows customers to add patches without having to wait for the next maintenance release.

Always on

- **High availability:** Stateful switchover with a 1:1 active standby and N+1 redundancy keeps your network, services, and clients always on, even in unplanned events.
- **Software Maintenance Upgrades (SMUs) with hot and cold patching:** Patching allows for a patch to be installed as a bug fix without bringing down the entire network and eliminates the need to requalify an entire software image. The SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. SMUs allow you to address the network issue quickly while reducing the time and scope of the testing required. The Cisco IOS XE platform internally validates the SMU compatibility and does not allow you to install incompatible SMUs. All SMUs are integrated into the subsequent Cisco IOS XE Software maintenance releases.
- **Intelligent rolling access point upgrades and seamless multisite upgrades:** The Cisco Catalyst 9800-40 Wireless Controller comes equipped with intelligent rolling access point upgrades to simplify network operations. Multisite upgrades can now be done in stages, and access points can be upgraded intelligently without restarting the entire network.

Security

- **Encrypted Traffic Analytics (ETA):** ETA is a unique capability for identifying malware in encrypted traffic coming from the access layer. Since more and more traffic is being encrypted, the visibility this feature provides related to threat detection is critical for keeping your network secure at different layers.
- **Trustworthy systems:** Cisco Trust Anchor Technologies provide a highly secure foundation for Cisco products. With the Cisco Catalyst 9800-40, these trustworthy systems help assure hardware and software authenticity for supply chain trust and strong mitigation against man-in-the-middle attacks on software and firmware. Trust Anchor capabilities include:
 - **Image signing:** Cryptographically signed images provide assurance that the firmware, BIOS, and other software are authentic and unmodified. As the system boots, its software signatures are checked for integrity.
 - **Secure Boot:** Cisco Secure Boot technology anchors the boot sequence chain of trust to immutable hardware, mitigating threats against a system's foundational state and the software that is to be loaded, regardless of a user's privilege level. It provides layered protection against the persistence of illicitly modified firmware.
 - **Cisco Trust Anchor module:** A tamper-resistant, strong cryptographic, single-chip solution uniquely identifies the product so that its origin can be confirmed to Cisco, providing assurance that the product is genuine.

Flexible NetFlow

- **Flexible NetFlow (FNF):** Cisco IOS FNF is the next generation in flow visibility technology, allowing optimization of the network infrastructure, reducing operating costs, and improving capacity planning and security incident detection with increased flexibility and scalability.

Application visibility and control

- **Next-Generation Network-Based Application Recognition (NBAR2):** NBAR2 enables advanced application classification techniques, with up to 1400 predefined and well-known application signatures and up to 150 encrypted applications on the Cisco Catalyst 9800-40. Some of the most popular applications included are Skype, Office 365, Microsoft Lync, Cisco Webex®, and Facebook. Many others are already predefined and easy to configure. NBAR2 provides the network administrator with an important tool to identify, control, and monitor end-user application usage while helping ensure a quality user experience and securing the network from malicious attacks. It uses FNF to report application performance and activities within the network to any supported NetFlow collector, such as Cisco Prime, Stealthwatch®, or any compliant third-party tool.

Quality of service

- **Superior Quality of Service (QoS):** QoS technologies are tools and techniques for managing network resources and are considered the key enabling technologies for the transparent convergence of voice, video, and data networks. QoS on the Cisco Catalyst 9800-40 consists of classification of traffic based on packet data as well as application recognition and traffic control actions such as drop, marking and policing. A modular QoS command-line framework provides consistent platform-independent and flexible configuration behavior. The 9800-40 also supports policies at two levels of target: BSSID as well as client. Policy assignment can be granular down to the client level.

Smart operation

- **Bluetooth ready:** The Cisco Catalyst 9800-40 has hardware support to connect a Bluetooth dongle to the controller, enabling you to use this wireless interface as a management port. This port functions as an IP management interface and can be used for configuration and troubleshooting using WebUI or the Command-Line Interface (CLI), and to transfer images and configurations.
- **WebUI:** WebUI is an embedded GUI-based device-management tool that provides the ability to provision the device, simplify device deployment and manageability, and enhance the user experience. WebUI comes with the default image. There is no need to enable anything or install any license on the device. You can use WebUI to build a day-0 and day-1 configuration and from then on monitor and troubleshoot the device without having to know how to use the CLI.

Specifications

Table 9. Specifications

Item	Specification	
Wireless standards	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n , 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave1 and Wave2, 802.11ax	
Wired, switching, and routing standards	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, 802.1AX Link Aggregation	
Data standards	<ul style="list-style-type: none">• RFC 768 User Datagram Protocol (UDP)• RFC 791 IP• RFC 2460 IPv6• RFC 792 Internet Control Message Protocol (ICMP)• RFC 793 TCP• RFC 826 Address Resolution Protocol (ARP)• RFC 1122 Requirements for Internet Hosts• RFC 1519 Classless Interdomain Routing (CIDR)• RFC 1542 Bootstrap Protocol (BOOTP)• RFC 2131 Dynamic Host Configuration Protocol (DHCP)• RFC 5415 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol• RFC 5416 CAPWAP Binding for 802.11	
Security standards	<ul style="list-style-type: none">• Wi-Fi Protected Access (WPA)• IEEE 802.11i (WPA2, RSN)• Wi-Fi Protected Access 3 (WPA3)• RFC 1321 MD5 Message-Digest Algorithm• RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform• RFC 2104 HMAC: Keyed-Hashing for Message Authentication• RFC 2246 TLS Protocol Version 1.0• RFC 2401 Security Architecture for the Internet Protocol• RFC 2403 HMAC-MD5-96 within ESP and AH• RFC 2404 HMAC-SHA-1-96 within ESP and AH	

Item	Specification	
	<ul style="list-style-type: none"> • RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV • RFC 2407 Interpretation for Internet Security Association Key Management Protocol (ISAKMP) • RFC 2408 ISAKMP • RFC 2409 Internet Key Exchange (IKE) • RFC 2451 ESP CBC-Mode Cipher Algorithms • RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile • RFC 4347 Datagram Transport Layer Security (DTLS) • RFC 5246 TLS Protocol Version 1.2 	
Encryption standards	<ul style="list-style-type: none"> • Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits • Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP) • Data Encryption Standard (DES): DES-CBC, 3DES • Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit • DTLS: AES-CBC • IPsec: DES-CBC, 3DES, AES-CBC • 802.1AE MACsec encryption 	
Authentication, Authorization, and Accounting (AAA) standards	<ul style="list-style-type: none"> • IEEE 802.1X • RFC 2548 Microsoft Vendor-Specific RADIUS Attributes • RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)-TLS • RFC 2865 RADIUS Authentication • RFC 2866 RADIUS Accounting • RFC 2867 RADIUS Tunnel Accounting • RFC 2869 RADIUS Extensions • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 5176 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS Support for EAP • RFC 3580 IEEE 802.1X RADIUS Guidelines • RFC 3748 Extensible Authentication Protocol (EAP) • Web-based authentication • TACACS support for management users 	
Management standards	<ul style="list-style-type: none"> • Simple Network Management Protocol (SNMP) v1, v2c, v3 • RFC 854 Telnet • RFC 1155 Management Information for TCP/IP-based Internets • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 Trivial File Transfer Protocol (TFTP) • RFC 1643 Ethernet MIB • RFC 2030 Simple Network Time Protocol (SNTP) • RFC 2616 HTTP • RFC 2665 Ethernet-Like Interface Types MIB 	

Item	Specification	
	<ul style="list-style-type: none"> • RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions • RFC 2819 Remote Monitoring (RMON) MIB • RFC 2863 Interfaces Group MIB • RFC 3164 Syslog • RFC 3414 User-Based Security Model (USM) for SNMPv3 • RFC 3418 MIB for SNMP • RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs • RFC 4741 Base NETCONF protocol • RFC 4742 NETCONF over SSH • RFC 6241 NETCONF • RFC 6242 NETCONF over SSH • RFC 5277 NETCONF event notifications • RFC 5717 Partial Lock Remote Procedure Call • RFC 6243 With-Defaults capability for NETCONF • RFC 6020 YANG • Cisco private MIBs 	
Management interfaces	<ul style="list-style-type: none"> • Web-based: HTTP/HTTPS • Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port • SNMP • NETCONF 	
Hard disk drives (HDD)	<ul style="list-style-type: none"> • SATA solid-state drive (SSD) • 240 GB of memory 	
Environmental conditions supported	<p>Operating temperature:</p> <ul style="list-style-type: none"> • Normal: 0° to 45° C (32° to 113° F) • Short term: 5° to 50° C (41° to 122° F) <p>Nonoperating temperature:</p> <ul style="list-style-type: none"> • -40° to 65° C (-104° to 149° F) <p>Operating humidity:</p> <ul style="list-style-type: none"> • Nominal: 5% to 85% noncondensing • Short term: 5% to 90% noncondensing <p>Nonoperating temperature humidity:</p> <ul style="list-style-type: none"> • 5% to 93% at 82° F (28° C) <p>Operating altitude:</p> <ul style="list-style-type: none"> • Appliance operating: 0 to 3000 m (0 to 10,000 ft) • Appliance nonoperating: 0 to 12,192 m (0 to 40,000 ft) <p>Electrical input:</p> <ul style="list-style-type: none"> • AC input frequency range: 47 to 63 Hz • AC input range: 90 to 264 VAC with AC PEM • 1100W AC with optional redundant power supply (hot-swappable) <p>Maximum power: 381W</p> <p>Heat dissipation: 1300 BTU/hr</p>	

Item	Specification	
	Sound power level measure: <ul style="list-style-type: none"> A-weighted sound power level is 74.1 LpAm(dBA) @ 27C nominal operation 	
Regulatory compliance	Safety: <ul style="list-style-type: none"> UL/CSA 60950-1 IEC/EN 60950-1 AS/NZS 60950.1 CAN/CSA-C22.2 No. 60950-1 	
	EMC – Emissions: <ul style="list-style-type: none"> FCC 47CFR15 AS/NZS CISPR 22 CISPR 22 EN55022/EN55032 (EMI-1) ICES-003 VCCI KN 32 (EMI-2) CNS-13438 	Class A
	EMC – Emissions: <ul style="list-style-type: none"> EN61000-3-2 Power Line Harmonics (EMI-3) EN61000-3-3 Voltage Changes, Fluctuations, and Flicker (EMI-3) 	
	EMC – Immunity: <ul style="list-style-type: none"> IEC/EN61000-4-2 Electrostatic Discharge Immunity IEC/EN61000-4-3 Radiated Immunity IEC/EN61000-4-4 EFT-B Immunity (AC Power Leads) IEC/EN61000-4-4 EFT-B Immunity (DC Power Leads) IEC/EN61000-4-4 EFT-B Immunity (Signal Leads) IEC/EN61000-4-5 Surge AC Port IEC/EN61000-4-5 Surge DC Port IEC/EN61000-4-5 Surge Signal Port IEC/EN61000-4-6 Immunity to Conducted Disturbances IEC/EN61000-4-8 Power Frequency Magnetic Field Immunity IEC/EN61000-4-11 Voltage Dips, Short Interruptions, and Voltage Variations K35 (EMI-2) 	
	EMC (ETSI/EN) <ul style="list-style-type: none"> EN 300 386 Telecommunications Network Equipment (EMC) (EMC-3) EN55022 Information Technology Equipment (Emissions) EN55024/CISPR 24 Information Technology Equipment (Immunity) EN50082-1/EN61000-6-1 Generic Immunity Standard (EMC-4) 	

Software requirements

The Cisco Catalyst 9800-40 runs on Cisco IOS XE Software version 16.10.1 or later. This software release includes all the features listed earlier in the Platform Benefits section.

Table 10. Minimum software requirements

Model	Description	Minimum software requirement
C9800-40-K9	Cisco Catalyst 9800-40 Wireless Controller	Cisco IOS XE Software Release 16.10.1

Licensing

No licenses are required to boot up a **Cisco Catalyst 9800 Series Wireless Controller**. However, in order to connect any access points to the **controller**, Cisco DNA software subscriptions are required. To be entitled to connecting to a 9800 Series controller, each access point requires a Cisco DNA subscription license.

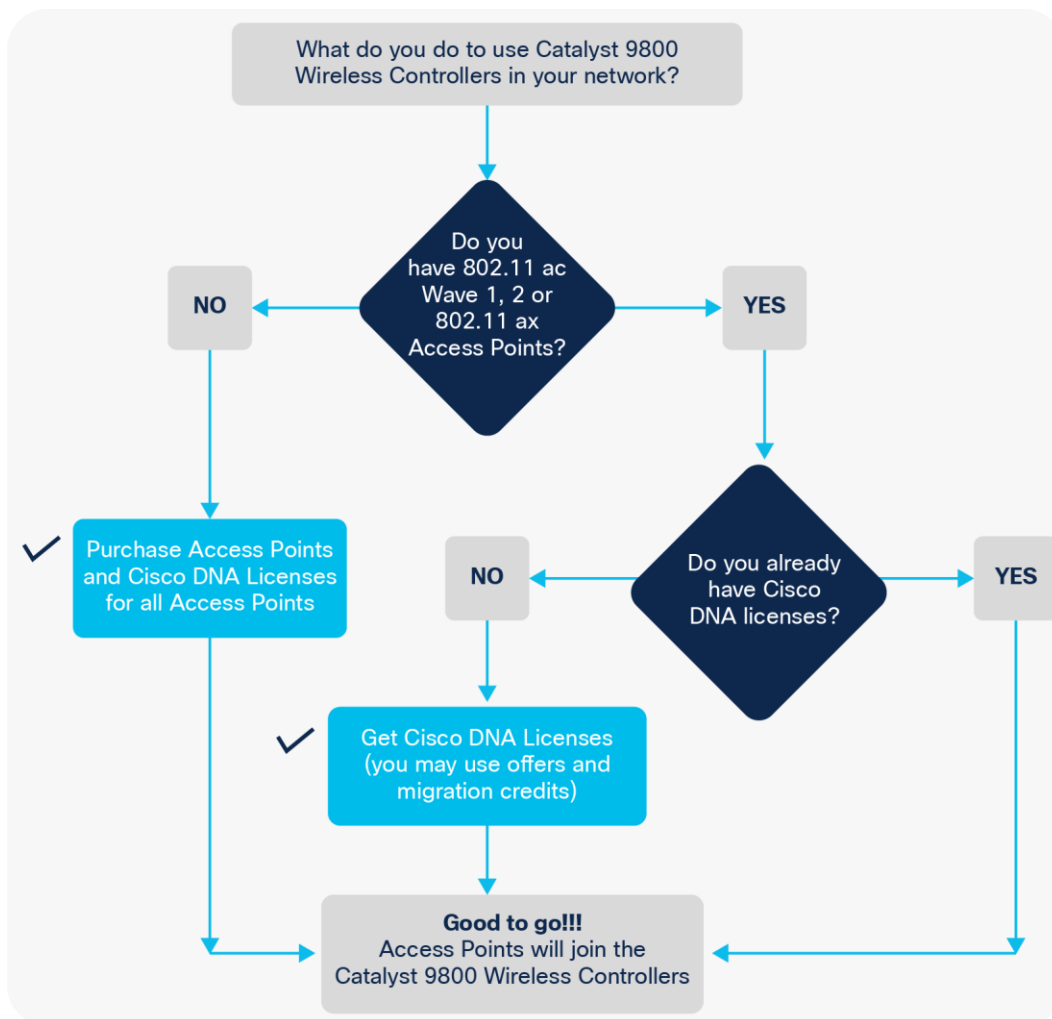


Figure 6. Determining license requirements for access points connecting to Cisco Catalyst 9800 Series Wireless Controllers

The access points connecting to the Cisco Catalyst 9800 Series have new and simplified software subscription packages.

They can support three tiers of Cisco DNA software: Cisco DNA Essentials, Cisco DNA Advantage and Cisco DNA Premier.

Cisco DNA software subscriptions provide Cisco innovations on the access point. They also include perpetual Network Essentials and Network Advantage licensing options, which cover wireless fundamentals such as 802.1X authentication, QoS and PnP; telemetry and visibility; and single sign-on, as well as security controls.

Cisco DNA subscription software has to be purchased for a 3-, 5-, or 7-year subscription term. Upon expiry of the subscription, the Cisco DNA features will expire, whereas the Network Essentials and Network Advantage features will remain.

For the full feature list of Cisco DNA Software, including the perpetual Network Essentials and Network Advantage, please see the feature matrix: https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrix-wireless.html?oid=porew018984.

Two modes of licensing are available:

- Smart Licensing (SL) simplifies and adds flexibility to licensing. It is:
 - Simple: Procure, deploy, and manage licenses easily. Devices self-register, removing the need for Product Activation Keys (PAKs).
 - Flexible: Pool license entitlements in a single account. Move licenses freely through the network, wherever you need them.
 - Smart: Manage your license deployments with real-time visibility into ownership and consumption.
- Specific License Reservation (SLR) is a feature used in highly secure networks. It provides a method for customers to deploy a software license on a device (product instance) without communicating usage information to Cisco. There is no communication with Cisco or a satellite. The licenses are reserved for every controller. It is node-based licensing.

Four levels of license are supported on the **Cisco Catalyst 9800 Series Wireless Controllers**. The controllers can be configured to function at any one of the four levels.

- Cisco DNA Essentials: At this level the Cisco DNA Essentials feature set will be supported.
- Cisco DNA Advantage: At this level the Cisco DNA Advantage feature set will be supported.
- NE: At this level the Network Essentials feature set will be supported.
- NA: At this level the Network Advantage feature set will be supported.

Cisco DNA Premier is a bundle with ISE licenses and Cisco DNA Spaces Extend. It is inclusive of Cisco DNA Advantage, so at this level the Cisco DNA Advantage feature set will be supported. For customers who purchase Cisco DNA Essentials, Network Essentials will be supported and will continue to function even after term expiration. And for customers who purchase Cisco DNA Advantage or Cisco DNA Premier, Network Advantage will be supported and will continue to function even after term expiration.

Initial bootup of the controller will be at the Cisco DNA Advantage level.

For questions, contact the Cisco Catalyst 9800 Series Wireless Controllers Licensing mailer group at [ask-catalyst 9800 licensing](#).

Managing licenses with Smart Accounts

Creating Smart Accounts by using the Cisco Smart Software Manager (SSM) enables you to order devices and licensing packages and also manage your software licenses from a centralized website. You can set up the Smart Account to receive daily email alerts and to be notified of expiring add-on licenses that you want to renew. A Smart Account is mandatory for the Cisco Catalyst 9800 Series. For more information on Smart Account refer to <https://www.cisco.com/go/smartaccounts>.

Warranty

Find warranty information on Cisco.com at the [Product Warranties](#) page.

Cisco 1-year limited hardware warranty terms

The following are terms applicable to your hardware warranty. Your embedded software is subject to the Cisco EULA (link available below) and/or any SEULA or specific software warranty terms for additional software products loaded on the device.

Duration of hardware warranty: One (1) year.

Replacement, repair, or refund procedure for hardware: Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the Return Materials Authorization (RMA) request. Actual delivery times may vary depending on customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's [Corporate Social Responsibility](#) (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Table 11. Links to sustainability information

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance
Sustainability inquiries	Contact: csr_inquiries@cisco.com

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Ordering information

Table 12. Ordering information

Type	Product ID	Description
Controller	C9800-40-K9	Cisco Catalyst 9800-40 Wireless Controller
	LIC-C9800-DTLS-K9	Cisco Catalyst 9800 Series Wireless Controller DTLS License
Accessories, spares	C9800-AC-750W R=	Cisco Catalyst 9800-40 750W AC Power Supply Reverse Air

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation and stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments.

[Learn more.](#)

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 <https://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/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)

ThunderIT for the REMC SAVE Contract

ThunderIT offers products and services for REMC SAVE contract customers at a discounted price in accordance to the REMC price list.

Overview for the REMC SAVE contract

REMC SAVE provides large volume contracts for a variety of educational resources, including furniture, school and office supplies, software and digital services, and technology.

The program saves time and money by providing bids compliant with the Michigan Revised School Code that also provides local school districts with the authority to purchase using REMC contracts. The legislation that established REMCs (Michigan Compiled Laws Act 451 Section 380.671), and State Board of Education Rules, enables REMCs to bid on behalf of local school districts and also provide local school districts with the authority to purchase using REMC contracts. All items and vendors are awarded through a sealed bid process by the REMC SAVE Bid Project and approved by the REMC Association.

REMC SAVE is provided as a project of the REMC Association of Michigan for all Michigan schools. REMC SAVE provides large-volume contracts for a variety of educational resources. By using REMC SAVE contracts, Michigan schools have saved more than \$1 billion since 1990. Every dollar saved through REMC SAVE today is one more dollar to invest in instruction tomorrow.

ThunderIT services the following REMC districts; REMC 1, REMC 2N, REMC 2C, REMC 2S, REMC 3, REMC 4, REMC 5, REMC 6, REMC 7, REMC 8, REMC 9, REMC 10, REMC 11, REMC 12W, REMC 12E, REMC 13, REMC 14W, REMC 14E, REMC 15, REMC 16, REMC 17, REMC 18S, REMC 18N, REMC 19W, REMC 19E, REMC 20, REMC 21, REMC 22

ThunderIT services the following REMC customers; AKIVA HEBREW DAY SCHOOL, BIRNEY MIDDLE SCHOOL, BUSSEY CTR-EARLY CHILDHOOD DEV, DEVRY UNIVERSITY - SOUTHFIELD – CENTRAL, HAMILTON ACADEMY CENTRAL OFFICE, LEONHARD ELEMENTARY SCHOOL, MCINTYRE ELEMENTARY SCHOOL, OAKLAND INTERNATIONAL ACADEMY

Other REMC contract holders include: Inacomp Technical Services Group, Sentinel Technologies, Software Services Group, Insight Direct USA, Information Systems Intelligence, Netech, Secant Technologies, CDW Logistics Inc (CDWG)

ThunderIT offers a variety of Solutions & Services to meet your every need

Digital Workplace

Transform your digital workplace and empower employees to drive your business forward. We deliver flexible, tailored, end-to-end solutions to keep your workforce engaged and productive. With an innovative approach centered around exceptional user experiences.

Smart Spaces

We provide smart workspace solutions to help you deliver consistent network performance and give guests, employees and students an uninterrupted experience.

Secure Network Solutions

Our security solutions help protect your network and critical data from cybersecurity threats

Safe Environments

We believe that employee, student, and customer safety is paramount in any environment. That's why our solutions provide a cloud based platform to help you intuitively manage and monitor physical locations to ensure a safe experience for everyone.

Next Generation WiFi

Power new and improved user experiences with our managed wifi solutions, offering faster speeds for enhanced application experience and more capacity for high density indoor and outdoor environments.

Remote Work Solutions

With our remote work solutions, working away from the office is no big deal. Give employees a secure, optimized connection to your entire network from anywhere.

Hybrid Workforce

We provide a seamless hybrid workforce solution that embraces change and operational scale. Give your employees and customers unrivaled experiences with a cloud platform that unifies best-in-class technologies.

Free Network Evaluation & Demo

ThunderIT offers a FREE Network Evaluation and/or product Demo to help ensure you are well informed and confident when choosing the right Cisco Meraki solution for your needs. During our call we'll architect a custom built Cisco Meraki solution for your business or environment.

Migration & Deployment

ThunderIT offers Migration and Deployment Services for your Cisco Meraki solution. Our experienced team of IT Professionals can configure, deploy and support your products to meet your needs. Our custom solutions ensure maximum efficiency and provide a clear path for your business going forward.

Managed Security

ThunderIT offers the best and most cost-effective solution to lower your risk in a heightened threat environment. Our team of certified Cisco engineers are ready to ensure that your network is secure, and your firewall is optimally configured to defend your business.

Mobile device management (MDM) Services

Our Mobile Device Management (MDM) solution unifies management of thousands of endpoint devices in a secure cloud platform, driving your organization's mobility initiatives, while maintaining an environment of agility and security.

Support & Monitoring

ThunderIT offers network support and monitoring services that are designed to fit the needs of every customer.

FAQs for the REMC SAVE Contract

Q: Does REMC SAVE meet the legal requirement for competitive bidding? A: The legislation that established REMCs (Michigan Compiled Laws Act 451 Section 380.671), and State Board of Education Rules, enables REMCs to bid on behalf of local school districts and also provide local school districts with the authority to purchase using REMC contracts. All items are competitively bid by REMC SAVE and awarded by the REMC Association.

Q: Who can Use REMC SAVE contracts? A: The following agencies are eligible to purchase using REMC SAVE contracts: PreK-12 Public, Charter (PSA) and Non-Public Schools, Community Colleges, Universities and Colleges, Public Libraries, Museums, State, County, and Local Government Agencies, Educational Non-profit Organizations and Health Care Facilities. Personal purchases at awarded bid pricing are at the discretion of the vendors.

Q: What is REMC SAVE? A: REMC SAVE is a free service of the REMC Association for all Michigan schools. There are 3 staff of REMC SAVE, and they conduct all of the bids and maintain vendor contracts. You can ask your local REMC Center questions. Find your local REMC Center by scrolling down the REMC SAVE home screen to view the map for your region or look up by zip code.

Q: How do I provide feedback? A: Your local REMC SAVE contact will always listen to any feedback you wish to provide. If you have feedback about the product, scroll down the home screen at remcsave.org and click 'View All Vendors' and you can complete a vendor evaluation form.

Q: What if my company wishes to become an awarded vendor? A: Go to vendorcenter.remcbids.org and create an account by clicking Login or Register in the upper right corner. Follow the directions! The only requirement is that you need five Michigan K12 school references. Customers can send their vendor recommendations to their local REMC contact or email remcsave@remc.org

Q: How are the vendors and products selected? A: Products and Vendors are awarded through a competitive bid process. REMC SAVE staff analyzes all bids and make recommendations to the REMC SAVE Advisory Committee for award. Once the REMC SAVE Advisory Committee votes on the award recommendations, they are then voted on by the REMC Association Board of Directors for final award.

Q: Where do I send my order or contact an awarded vendor? To contact vendors, navigate to the vendor listing by scrolling down the home screen and click 'view all vendors,' or navigate to <https://www.remcsave.org/vendors>. Click on the vendor name to find their contact information.

Q: What do I need to include on my purchase order? Please make sure your purchase order is itemized and includes the REMC item number, the model number/name, the reseller product number (if available), the quantity of each item to be purchased, and the unit price. A quote may be attached, but the purchase order should still be itemized. Sometimes the item numbers for the warranties, accessories, and upgrades are located on the spec sheet, linked from the awarded item page – be sure to include on the Purchase Order.