Data Sheet

# Cisco Catalyst 9800-CL Wireless Controller for Cloud

## Built from the ground up for intent-based networking

# Contents


Product Overview 3

Features 6

Benefits 8

Specifications 10

Software Requirements 12

Licensing 12

Warranty 17

Cisco environmental sustainability 17

Ordering Information 18

Cisco Capital 18

Document History 18

## Product Overview


Built from the ground-up for the 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 the best-in-class wireless experience for your evolving and growing organization. The Cisco Catalyst 9800 Series Wireless Controllersare 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-CL is the next generation of enterprise-class wireless controllers for cloud, with seamless software updates for distributed branches and midsize campuses to large enterprises and service providers.

The Cisco Catalyst 9800-CLController 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** in planned and unplanned events.
- **Secure** air, devices, and users with the Cisco Catalyst 9800-CL. 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: runtime defenses, image signing and integrity verification.
- **Deploy anywhere** to enable wireless connectivity everywhere. Whether in a public or private cloud, the Cisco Catalyst 9800-CL best meets your organization's needs.
- Built on a modular operating system, the 9800-CL 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 Catalyst 9800-CL for Private Cloud

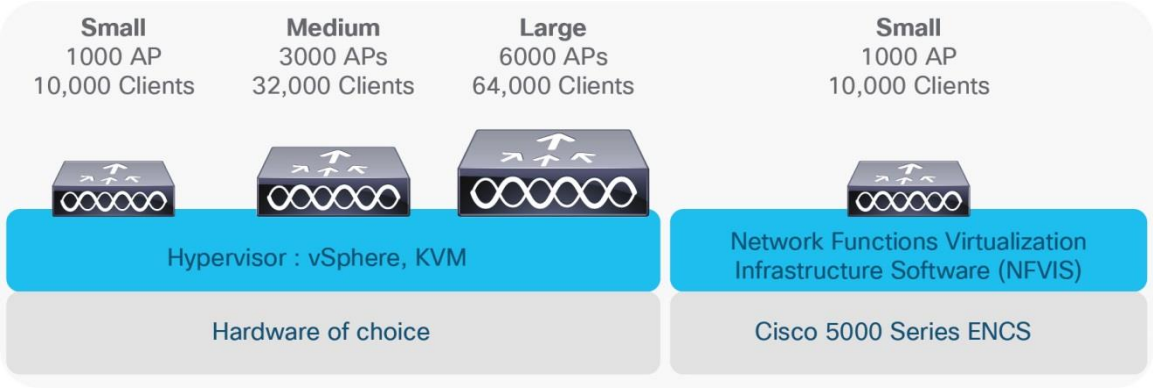


**Figure 1.**
Cisco Catalyst 9800-CL for private cloud

### Key highlights

- Multiple scale templates (small, medium, and large)
- VMware ESXi, KVM, and Cisco NFVIS (on ENCS) supported
- Supports centralized, Cisco FlexConnect®, and fabric (SD-Access) deployment
- Multiple scale options with a single deployment package to best meet your organization's needs.
  - **Small:** Designed for distributed branches and small campuses supporting up to 1000 Access Points (APs) and 10,000 clients
  - **Medium:** Designed for medium-sized campuses supporting up to 3000 APs and 32,000 clients
  - **Large:** Designed for large enterprises and service providers supporting up to 6000 APs and 64,000 clients
- Supports up to 1.5 Gbps of throughput in a centralized wireless deployment
- One deployment package for all the scale templates. Pick the deployment size when you instantiate the Virtual Machine (VM)
- An intuitive bootstrap wizard is available during the VM instantiation to boot the wireless controller with recommended parameters
- Optimize your branch by deploying the 9800-CL as a virtual machine on the Cisco 5000 Series Enterprise Network Compute System (ENCS) running Cisco NFVIS

## Cisco Catalyst 9800-CL for Public Cloud

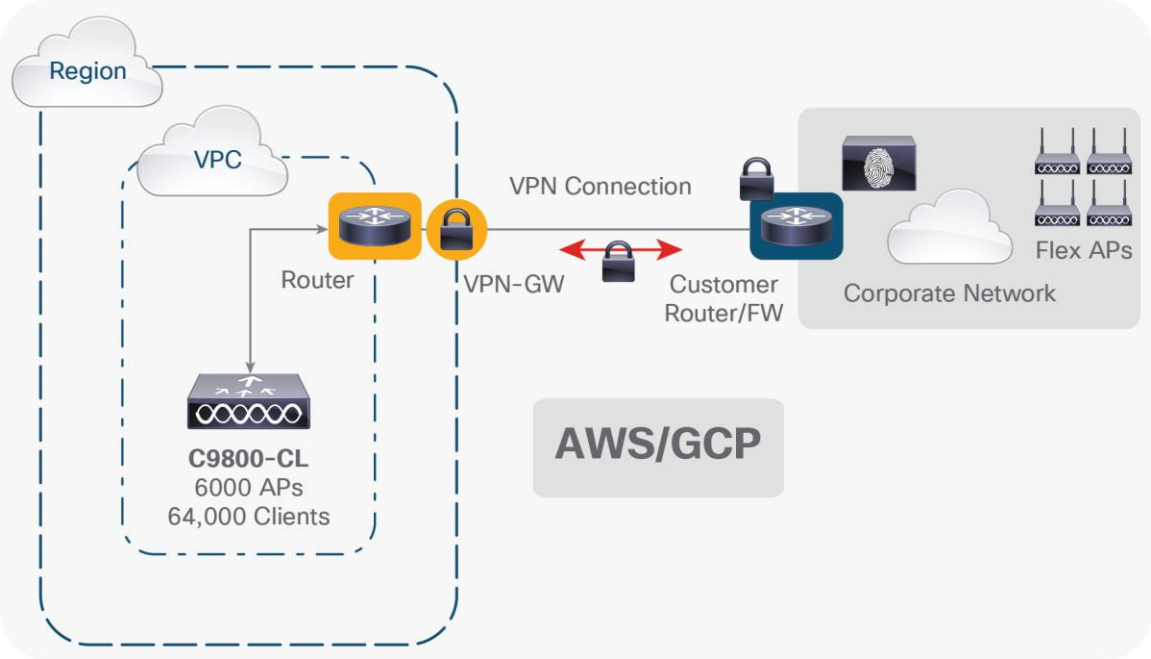


**Figure 2.**
Cisco Catalyst 9800-CL for public cloud

### Key highlights

- Cisco Catalyst 9800-CL is available as an IaaS solution in the Amazon Web Services(AWS) and Google Cloud (GCP) Marketplaces
- Supported only with managed VPN
- Cisco FlexConnect central authentication and local switching
- Available on AWS GovCloud
- Supports up to 6000 access points and 64,000 clients.
- The 9800-CL should be instantiated within a Virtual Private Cloud (VPC).
- A VPN tunnel has to be established from the customer site to AWS/GCP to enable communication between the Cisco access point and 9800-CL wireless controller.
- Deploy a wireless controller instance in AWS using cloud-formation templates provided by Cisco (recommended) or by manually using the EC2 console.
- Deploy a wireless controller in GCP using the guided workflow in the marketplace

## Features

**Table 1.** Key features

| Metric | Value |
|---|---|
| **Maximum number of access points** | Up to 6000 |
| **Maximum number of clients** | 64,000 |
| **Maximum throughput** | Up to 1.5 Gbps |
| **Maximum WLANs** | 4096 |
| **Maximum VLANs** | 4096 |
| **Deployment modes** | Centralized, Cisco FlexConnect, and Fabric Wireless (SD-Access) |
| **License** | Smart License enabled |
| **Operating system** | Cisco IOS XE Software |
| **Management** | Cisco DNA Center 1.2.8, Cisco Prime® Infrastructure 3.5, integrated WebUI, and third party (open standards APIs) |
| **Interoperability** | AireOS-based controllers with 8.8 MR2, 8.5 MR4, and 8.5 MR3 special |
| **Policy engine** | Cisco Identity Services Engine (ISE) 2.2, 2.3, and 2.4 |
| **Cisco Connected Mobile Experiences (CMX)** | CMX 10.5.1 |
| **Access points** | Aironet 802.11ac Wave 1 and Wave 2 access points |

### 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-CL. Wireless infrastructure becomes the strongest first line of defense with ETA and SD-Access. The controllers come with built-in security: runtime defenses, image signing and integrity verification.

### Deploy anywhere

Whether in a public or private cloud, the Cisco Catalyst 9800-CL wireless controllers can be deployed anywhere for wireless everywhere. The 9800-CL meets the needs of your branch and campus network deployments.

### Open and programmable

The controllers are 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.

## Key Specifications

**Table 2.** Key specifications

| Metric | Private cloud | | | Public Cloud | | |
|---|---|---|---|---|---|---|
| | Small | Medium | Large | Small | Medium | Large |
| Deployment modes supported | Centralized, Cisco FlexConnect, Fabric(SD-Access) | Centralized, Cisco FlexConnect, Fabric (SD-Access) | Centralized, Cisco FlexConnect, Fabric (SD-Access) | Cisco FlexConnect (local switching only) | Cisco FlexConnect (local switching only) | Cisco FlexConnect (local switching only) |
| vCPUs Required | 4 | 6 | 10 | 4 | 6 | 10 |
| RAM required (GB) | 8 | 16 | 32 | 8 | 16 | 32 |
| Hypervisors and cloud providers supported | ESXi 6.0/6.5, KVM, NFVIS | ESXi 6.0/6.5, KVM, NFVIS | ESXi 6.0/6.5, KVM, NFVIS | AWS, GCP | AWS, GCP | AWS, GCP |
| Maximum number of access points | 1000 | 3000 | 6000 | 1000 | 3000 | 6000 |
| Maximum number of clients | 10,000 | 32,000 | 64,000 | 10,000 | 32,000 | 64,000 |
| Maximum throughput | 1.5 Gbps | 1.5 Gbps | 1.5 Gbps | (All traffic will be locally switched) | (All traffic will be locally switched) | (All traffic will be locally switched) |
| Maximum WLANs | 4096 | 4096 | 4096 | 4096 | 4096 | 4096 |
| Maximum VLANs | 4096 | 4096 | 4096 | 4096 | 4096 | 4096 |
| Maximum site tags | 1000 | 3000 | 6000 | 1000 | 3000 | 6000 |
| Maximum APs per site | 100 | 100 | 100 | 100 | 100 | 100 |
| Maximum policy tags | 1000 | 3000 | 6000 | 1000 | 3000 | 6000 |
| Maximum RF tags | 1000 | 3000 | 6000 | 1000 | 3000 | 6000 |
| Maximum RF profiles | 2000 | 6000 | 12,000 | 2000 | 6000 | 12,000 |
| Maximum policy profiles | 1000 | 1000 | 1000 | 1000 | 1000 | 1000 |
| Maximum Flex profiles | 1000 | 3000 | 6000 | 1000 | 3000 | 6000 |
| vNIC adapters | **ESXi:** VXNET3, E1000E, E1000<br>**KVM:** VIRTIO | **ESXi:** VXNET3, E1000E, E1000<br>**KVM:** VIRTIO | **ESXi:** VXNET3, E1000E, E1000<br>**KVM:** VIRTIO | – | – | - |
| Virtual switch | **ESXi:** vSwitch<br>**KVM:** OVS Linux Bridge(brctl) | **ESXi:** vSwitch<br>**KVM:** OVS Linux Bridge(brctl) | **ESXi:** vSwitch<br>**KVM:** OVS Linux Bridge(brctl) | – | – | – |

| Metric | Private cloud | | | Public Cloud | | |
|---|---|---|---|---|---|---|
| **High availability** | SSO, N+1 | SSO, N+1 | SSO, N+1 | N+1 | N+1 | N+1 |
| **Cisco DNA support** | Automation, Assurance | Automation, Assurance | Automation, Assurance | – | – | – |
| **Guest anchor** | Yes | Yes | Yes | – | – | – |
| **Client IPv6 support** | Yes | Yes | Yes | Yes | Yes | Yes |
| **Infrastructure IPv6 support** | Yes | Yes | Yes | No | No | No |

## 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 the Cisco Catalyst 9800-CL Wireless Controller for Cloud 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-CL Wireless Controller for Cloud 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-CL, these trustworthy systems help assure 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.

### 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-CL. 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-CL consists of classification of traffic based on packet data as well as application recognition

and traffic control actions such as dropping, marking and policing. A modular QoS command-line framework provides consistent platform-independent and flexible configuration behavior. The 9800-CL 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

- **WebUI:** WebUI is an embedded GUI-based device-management tool that provides the ability to provision the device, simplifying device deployment and manageability and enhancing 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 3.** 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 Wave 1 and Wave 2 | |
| **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, IEEE 802.1AX Link Aggregation | |
| **Data standards** | • RFC 768 User Datagram Protocol (UDP)<br>• RFC 791 IP<br>• RFC 2460 IPv6<br>• RFC 792 Internet Control Message Protocol (ICMP)<br>• RFC 793 TCP<br>• RFC 826 Address Resolution Protocol (ARP)<br>• RFC 1122 Requirements for Internet Hosts<br>• RFC 1519 Classless Interdomain Routing (CIDR)<br>• RFC 1542 Bootstrap Protocol (BOOTP)<br>• RFC 2131 Dynamic Host Configuration Protocol (DHCP)<br>• RFC 5415 Control and Provisioning of Wireless Access Points (CAPWAP) Protocol<br>• RFC 5416 CAPWAP Binding for 802.11 | |

| Item | Specification | |
|---|---|---|
| Security standards | • Wi-Fi Protected Access (WPA)<br>• IEEE 802.11i (WPA2, RSN)<br>• RFC 1321 MD5 Message-Digest Algorithm<br>• RFC 1851 Encapsulating Security Payload (ESP) Triple DES (3DES) Transform<br>• RFC 2104 HMAC: Keyed-Hashing for Message Authentication<br>• RFC 2246 TLS Protocol Version 1.0<br>• RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile<br>• RFC 4347 Datagram Transport Layer Security (DTLS)<br>• RFC 5246 TLS Protocol Version 1.2 | |
| Encryption standards | • Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits<br>• Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP)<br>• Data Encryption Standard (DES): DES-CBC, 3DES<br>• Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit<br>• DTLS: AES-CBC<br>• IPsec: DES-CBC, 3DES, AES-CBC<br>• 802.1AE MACsec encryption | |
| Authentication, authorization, and accounting (AAA) standards | • IEEE 802.1X<br>• RFC 2548 Microsoft Vendor-Specific RADIUS Attributes<br>• RFC 2716 Point-to-Point Protocol (PPP) Extensible Authentication Protocol (EAP)-TLS<br>• RFC 2865 RADIUS Authentication<br>• RFC 2866 RADIUS Accounting<br>• RFC 2867 RADIUS Tunnel Accounting<br>• RFC 2869 RADIUS Extensions<br>• RFC 3576 Dynamic Authorization Extensions to RADIUS<br>• RFC 5176 Dynamic Authorization Extensions to RADIUS<br>• RFC 3579 RADIUS Support for EAP<br>• RFC 3580 IEEE 802.1X RADIUS Guidelines<br>• RFC 3748 Extensible Authentication Protocol (EAP)<br>• Web-based authentication<br>• TACACS support for management users | |
| Management standards | • Simple Network Management Protocol (SNMP) v1, v2c, v3<br>• RFC 854 Telnet<br>• RFC 1155 Management Information for TCP/IP-based Internets<br>• RFC 1156 MIB<br>• RFC 1157 SNMP<br>• RFC 1213 SNMP MIB II<br>• RFC 1350 Trivial File Transfer Protocol (TFTP)<br>• RFC 1643 Ethernet MIB<br>• RFC 2030 Simple Network Time Protocol (SNTP)<br>• RFC 2616 HTTP<br>• RFC 2665 Ethernet-Like Interface Types MIB<br>• RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions<br>• RFC 2819 Remote Monitoring (RMON) MIB<br>• RFC 2863 Interfaces Group MIB<br>• RFC 3164 Syslog | |

| Item | Specification | |
|---|---|---|
| | • RFC 3414 User-Based Security Model (USM) for SNMPv3<br>• RFC 3418 MIB for SNMP<br>• RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs<br>• RFC 4741 Base NETCONF protocol<br>• RFC 4742 NETCONF over SSH<br>• RFC 6241 NETCONF<br>• RFC 6242 NETCONF over SSH<br>• RFC 5277 NETCONF event notifications<br>• RFC 5717 Partial Lock Remote Procedure Call<br>• RFC 6243 With-Defaults capability for NETCONF<br>• RFC 6020 YANG<br>• Cisco private MIBs | |
| **Management interfaces** | • Web-based: HTTP/HTTPS<br>• Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port<br>• SNMP<br>• NETCONF | |

## Software Requirements

The Cisco Catalyst 9800-CL Wireless Controller for Cloud 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 4.** Minimum software requirements

| Model | Description | Minimum software requirement |
|---|---|---|
| **C9800-CL-K9** | Cisco Catalyst 9800-CL Wireless Controller for Cloud | Cisco IOS XE Software Release 16.10.1 |

## Licensing

**The Cisco Catalyst 9800 Series Wireless Controllers require mandatory Smart Licensing**. This provides ease of use for Cisco DNA license management, consumption, and tracking.

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 licenses are required. Every access point connecting to Catalyst 9800 requires a Cisco DNA subscription license to be entitled to connect to the controller. See Figure 2.

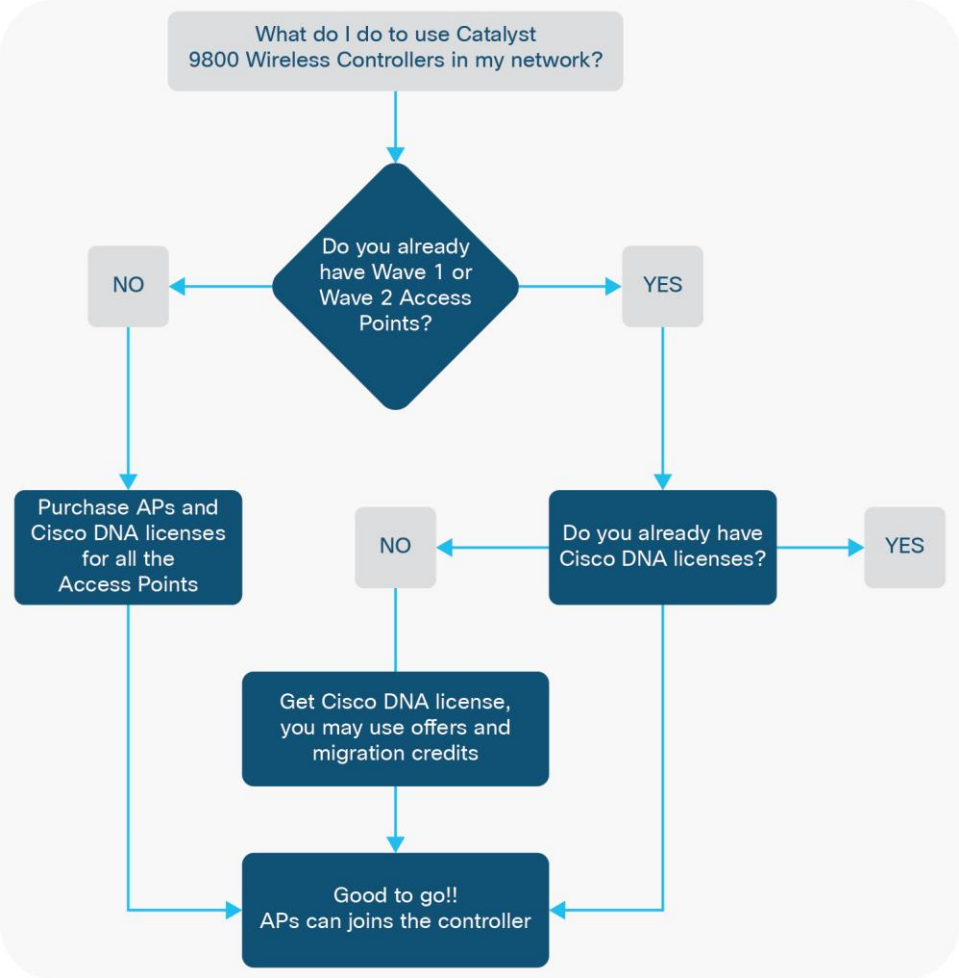


**Figure 3.**
The APs connecting to Catalyst 9800 has a new and simplified licensing package

They can support 3 types of Cisco DNA license: Cisco DNA Essentials, Cisco DNA Advantage and Cisco DNA Premier:

The Cisco DNA licenses provide Cisco innovations on the AP. The Cisco DNA license also includes the Network Essentials and Network Advantage licensing options whichcover wireless fundamentals such as 802.1x authentication, QoS, PnP etc, telemetry and visibility, SSO, as well as security controls. These Network essentials and Network advantage components are perpetual and is valid till the life of the AP. Cisco DNA subscription licenses have to be purchased for a 3-, 5-, or 7-year subscription term. However. upon expiry of Cisco DNA license, Cisco DNA features will expire, whereas network essentials and network advantage features will remain.

Here is a brief description of what each base and add-on package includes:

## Wireless Subscription Offer Structure

### Cisco DNA Essentials

Single SKU 3/5/7 Year Subscriptions

- Prime
- AP License
- Cisco DNA Essentials

Base Automation

### Cisco DNA Advantage

Enterprise Agreement Eligible

Single SKU 3/5/7 Year Subscriptions

- Prime
- AP License
- Cisco DNA Advantage

Automation and Assurance

### Cisco DNA Premier

Enterprise Agreement Eligible

Single SKU 3/5/7 Year Subscriptions

- CMX Base
- ISE Base + ISE Plus
- Prime
- AP License
- Cisco DNA Advantage

Automation, Assurance, SDA, Security and Location

Wave 2 APs and Cisco Catalyst 9800 Wireless Controllers with Cisco DNA licenses that include perpetual Network Essentials/Network Advantage

**Software Support Service (SWSS) included in all subscriptions**

## Catalyst 9800 Wireless Controller- Advantage vs. Essentials

C9800-40/C9800-80/C9800-CL

### Advantage

**Cisco DNA Advantage (Inclusive of Cisco DNA Essentials)** — 3,5,7 Year Terms

**Advanced Automation**
- SD-Access
- Location Plug and Play
- Automated ISE integration for guest
- Third Party API integration

**Enhanced Security & IoT**
- Encrypted Traffic Analytics
- Advanced WIPS*

**Policy Based Workflows**
- EasyQos configuration
- EasyQos monitoring
- Policy-based Automation

**Assurance and Analytics**
- Guided Remediation
- Apple iOS Insights
- Proactive issue Detection
  - Aironet Active Senor Tests
  - Intelligent capture
  - Client Location Heatmaps
  - Spectrum Analyzer
- Application performance (Packet Loss, Latency and Jitter)
- App 360, AP 360, Client 360 and WLC 360
- Custom Reports*

**Element Management**
- Path Lifecycle Management

**Network Advantage (Inclusive of Network Essentials)** — Perpetual

**High Availability an Resiliency**
- ISSU, Process Restart
- Rolling AP Upgrades
- Patching (CLI)
- AP service pack/AP device pack

**Flexible Network Segmentation**
- VXLAN

### Essentials

**Cisco DNA Essentials** — 3,5,7 Year Terms

**Basic Automation**
- PnP Application
- Network Site Design and Device Provisioning

**Element Management**
- Software Image Management
- Discovery, Network Topology
- AVC

**Telemetry**
- Flexible Netflow

**Basic Assurance**
- Health dashboard (Network, Client and Application)
- AP Floormap and Coverage map
- Pre-defined Reports

**Base Security**
- Basic WIPS*

**Network Essentials** — Perpetual

**Essential Wireless Capabilities**
- 802.1x authentications, Guest access, device onboarding, Infra and client IPv6, ACLs, QoS, Videostream, Smart defaults, RRM, Spectrum intelligence, BLE, Zigbee, USB, TrustSec SXP, SSO, Dynamic QoS, Analytics, ADP, OpenDNS, IPSec, Rogue Management and Detection, Mobility

**Optimized RF**
- FRA, Client link, Clear Air Advanced
- NG-HDX, Predictive/Proactive RRM

**IoT Optimized**
- Identity PSK, Enhanced Device profilers

**DevOps Integration**
- PnP Agent
- NETCONF, RESTCONF*, gNMI*
- Yang Data Models
- GuestShell (On-Box Python)*

**Telemetry and Visibility**
- Model-driven Telemetry
- NETCONF dial-in, gRPC dial out*

**Federal Certifications***
- FIPS, CC, UCAPL, USGV6

- Cat 9800 controller **includes** the **Perpetual** Network Stack - **Network Essentials or Network Advantage**
- **Mandatory** to **attach Cisco DNA License for every AP joining the controller**
- Cisco DNA License **includes Wireless and Cisco DNA Center Features**

*Future

**Note:** It is not required to deploy Cisco DNA Center just to use one of the above packages.

The following table shows the features included in the Network Advantage and Network Essentials package.

**Table 5.** Features included in the Network Advantage and Network Essentials packages

| Features | Network Essentials | Network Advantage |
|---|---|---|
| **Essential capabilities**<br>• 802.1x authentications, Guest access, device onboarding, Infra and client IPv6, ACLs, QoS, Videostream, Smart defaults, RRM, Spectrum intelligence, BLE, Zigbee, USB, TrustSec SXP,SSO, Dynamic QoS, Analytics, ADP, OpenDNS, mDNS, IPSec, Rogue Management and Detection, Mobility | ✓ | ✓ |
| **Optimized RF**<br>• FRA, Client link, ClearAir Advanced,<br>• NG-HDX, Predictive/Proactive RRM | ✓ | ✓ |
| **Internet of Things (IoT) optimized**<br>Identity pre-shared keys (PSK), enhanced device profilers | ✓ | ✓ |
| **DevOPS integration**<br>• PnP Agent<br>• NETCONF, RESTCONF*, gNMI*<br>• Yang Data Models<br>• GuestShell (On-Box Python)* | ✓ | ✓ |
| **Federal Certifications**<br>Federal Information Processing Standards (FIPS), CC, UCAPL, USGV6 | ✓ | ✓ |
| **Telemetry and visibility**<br>• Model-driven Telemetry<br>• NETCONF dial-in, gRPC dial out* | ✓ | ✓ |
| **High availability and resiliency (advanced)**<br>• ISSU, Process Restart,<br>• Rolling AP Upgrades,<br>• Patching (CLI)<br>• AP service pack/AP device pack | ✗ | ✓ |
| **Flexible Network Segmentation**<br>• VXLAN | ✗ | ✓ |

The following table shows the features included in the Cisco DNA Advantage and Cisco DNA Essentials packages.

**Table 6.** Features included in the Cisco DNA Advantage and Cisco DNA Essentials packages

| Features | Cisco DNA Essentials | Cisco DNA Advantage/Premier |
|---|---|---|
| **Base Automation** | ✓ | ✓ |

| Features | Cisco DNA Essentials | Cisco DNA Advantage/Premier |
|---|---|---|
| Plug and Play, network site design and device provisioning | | |
| **Element management**<br>Image management, network topology and discovery, AVC | ✓ | ✓ |
| **Base Assurance**<br>Health dashboard (network, client, and application), AP floor map and coverage map, predefined reports | ✓ | ✓ |
| **Telemetry**<br>Flexible NetFlow | ✓ | ✓ |
| **Base security**<br>Basic wireless IPS | ✓ | ✓ |
| **Advanced Automation**<br>SD-Access<br>Location Plug and Play<br>Automated ISE integration for guest<br>3rd party API integration | ✗ | ✓ |
| **Assurance and Analytics**<br>Guided Remediation<br>Apple iOS Insights<br>Proactive issue Detection<br>Aironet Active Sensor Tests<br>Intelligent capture<br>Client Location Heatmaps<br>Spectrum Analyzer<br>Application performance (Packet Loss, Latency and Jitter)<br>App 360, AP 360, Client 360 and WLC 360<br>Custom Reports* | ✗ | ✓ |
| **Enhanced security and IoT**<br>Encrypted Traffic Analytics, Advanced WIPS | ✗ | ✓ |
| **Policy-based workflow**<br>EasyQoS configuration, EasyQoS monitoring, Policy based Automation | ✗ | ✓ |
| **Element Management**<br>Patch Lifecycle Management | ✗ | ✓ |

Two modes of licensing are available:

- SL: Smart Licensing 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 of ownership and consumption.
- SLR mode
  - 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 will be no communication with Cisco or a satellite. The licenses will be reserved for every controller. It will be 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 Essential: At this level the Cisco DNA Essentials features 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.
  - For customers who purchase Cisco Essentials, Network Essentials will be supported and will continue to function even after term expiration. And for customers who purchase Cisco DNA Advantage, 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 Advange level.

For questions, contact the Cisco Catalyst 9800 Series Wireless Controllers Licensing mailer group at ask-catalyst9800licensing.

## Managing licenses with smart accounts

Creating Smart Accounts by using the Cisco Smart Software Manager (CSSM) 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 Catalyst 9800 controller. 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.

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.

## 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:

| 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 |

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 7.** Ordering information

| Type | Product ID | Description |
|---|---|---|
| Controller | C9800-CL-K9 | Cisco Catalyst 9800-CL Wireless Controller for Cloud |
| | LIC-C9800-DTLS-K9 | Cisco Catalyst 9800 Series Wireless Controller DTLS license |

- Purchase the above SKU for software download and Cisco TAC support.
- The 9800-CL private cloud image for VMware ESXi, KVM, and **Cisco NFVIS on ENCS** can be downloaded from software.cisco.com.
- The 9800-CL public cloud image for AWS can be subscribed and deployed from the AWS Marketplace.
- The 9800-CL public cloud image for GCP can be subscribed and deployed from the GCP Marketplace.

## 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 help you 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.

## Document History

| New or revised topic | Described In | Date |
|---|---|---|
| Cosmetic changes to various tables were made | Table | November 15, 2018 |
| Updated images were included | Images | November 15, 2018 |
| Licensing information updated | Licensing | December xx, 2018 |

**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**.



Printed in USAs

C78-741546-03 10/19