

Cisco Remote Workforce Network Solutions

Common questions

Q: What are the Cisco® Remote Workforce Network solutions?

A: The Cisco Remote Workforce Network solutions are fundamental to the next level of workspaces and to future business resiliency. They extend enterprise network connectivity to remote workforces at home and micro-offices at scale. Going beyond traditional VPN connectivity, the Remote Workforce Network solutions extend corporate SSID and Authentication, Authorization, and Accounting (AAA) services to home offices, providing a seamless corporate experience to remote employees and IT administrations.

With these solutions, remote workers have the same level of security, performance, and policies and ultimately the same experience as they have in a corporate office. IT administrators can provision, manage, and deploy consistent

policies across all distributed home and micro-offices remotely and securely via a centralized orchestration tool.

There are two enterprise-ready Cisco Remote Workforce Network solutions—one with Cisco wireless access points and the other with a Cisco routing solution.

Q: What are the benefits of the Remote Workforce Network solutions?

A: Cisco Remote Workforce Network solutions enable remote employee and IT administrators with:

- **Orchestration:** A centralized location for provisioning new remote locations, deploying enterprise-class identity-based policy, and managing all distributed workforces
- **Onboarding:** A zero-touch process for launching network devices, including personal devices

- **Experience:** Seamless corporate-level security and application experiences for remote workspaces

Q: What differentiates Cisco solutions from those available from competitors?

A: In addition to seamless onboarding, Cisco solutions extend advanced enterprise features such as Cisco Umbrella®, Application Visibility and Control (AVC)/Quality of Service (QoS), Cisco TrustSec®, and secure Direct Internet Access (DIA) for Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) applications with the ability to manage personal SSIDs for personal Wi-Fi devices.

Q: Can remote workers create their own personal SSID in these solutions?

A: Yes. A personal SSID can be created by remote workers.

Q: Is a Smart Account required for these solutions?

A: Automatic onboarding of wireless access points and Cisco Integrated Services Routers (ISRs) requires Cisco cloud Plug and Play (PnP) Connect, which can be accessed only through a Smart Account. Without Cisco PnP Connect, a network administrator would need to manually stage the access points before shipping them to the end users.

Wireless option

Q: What are the key benefits and features of these wireless solutions?

- Expansion of corporate network connectivity and identity-based policies to the home
- Zero-touch and identity-based onboarding of wired and wireless devices (including personal devices)
- Cisco CleanAir® and advanced Radio Resource Management (RRM) technologies for spectrum management and RF visibility
- Centralized provisioning and management and cloud security
- Seamless application experience via optimized data path and QoS

Q: How is this solution different from the Cisco OfficeExtend Access Point (OEAP) wireless solutions?

A: There are several differences:

OEAP doesn't have any central orchestration, so the IT administrator has to configure the access points manually before sending them to users.

With the Remote Workforce Wireless solution, users can get the device directly from the manufacturer (bypassing IT), plug it in, and be ready to go after only a couple of minutes. It uses the PnP Connect cloud to get all the designated configurations and download them to the device automatically.

The existing OEAP solution does not support DIA (split tunneling) for cloud applications.

The new solutions support DIA (split tunneling), where policy can be defined for traffic to be tunneled from a wireless controller or switch locally to the internet.

With regard to security, OEAP does not offer Umbrella security and TrustSec. It also can't apply QoS policies to video or audio traffic. This new solution offers the same security policies and application experience that a user would have at a campus or branch location.

Q: What is the advantage of the Cisco Catalyst™ 9105 Series Wi-Fi 6 access points for a remote workforce?

- A: Cisco CleanAir and RRM technologies for Catalyst Wi-Fi 6 access points, including the Catalyst 9105 Series, are Spectrum Intelligence solutions designed to proactively manage the challenges of a shared wireless spectrum. They identify the source, location, and scope of RF interference and can proactively guard against it.

Q: How do you deploy the Remote Workforce Wireless solution?

A: Please refer to the deployment guide.

Q: What access point and controller models are supported for the Remote Workforce Wireless solution?

A: Table 1. Wireless models supported by the Remote Workforce Wireless solution:

Type of wireless device	Models
Wi-Fi 5 access points	Aironet [®] 1815t, ¹ 1840, ¹ 1815w, ² 1815i, ² and the 2800, ² 3800, ² and 4800 ² Series
Wi-Fi 6 access points	Catalyst 9115, ¹ 9105 ¹ , 9120, ² and 9130 ² Series
Wireless controllers ²	3504, 5520, 8540, 9800-L, 9800-40, 9800-80, and 9800-CL (private cloud)

¹Discounted models within bundle.

²Bring your own hardware.

Q: Can wired clients be connected to a home access point?

A: Yes, wired clients such as desktops, IP phones, etc. can be onboarded with secure 802.1X authentication. Also, the LAN ports of certain wireless access point and ISR models support Power Over Ethernet (PoE).

Routing option

Q: What is the Cisco Remote Workforce Routing solution?

A: The Remote Workforce Routing solution extends a uniform enterprise SD-WAN to the home and remote workforce. Extensive

cloud integration delivers a consistent and optimal application experience. A cloud-delivered Secure Access Service Edge (SASE) architecture provides unified security and compliance. Centralized management automates the deployment, configuration, and troubleshooting in an agile and scalable manner. The Cisco Remote Workforce Routing solution consists of the following flexible hardware and software solutions:

- Cisco 1131 ISR: The ability to connect users reliably and securely across multicloud, branch, data center, and the hybrid workforce has become a critical success factor for any organization. The Cisco 1131 ISR is the next iteration of ISRs optimized for distributed

small branches and the remote workforce, with built-in Wi-Fi 6 and 5G support for enhanced SD-WAN connectivity.

- Cisco SD-WAN Remote Access (SD-WAN RA): Integrates remote-access functionality into the SD-WAN fabric, thereby delivering all the benefits of Cisco SD-WAN to the remote workforce. Remote workers can simply leverage existing remote-access clients (including Cisco AnyConnect[®], Windows, Apple OS native clients, and hardware-based routers such as the Catalyst Wireless Gateway) to access the nearest Cisco SD-WAN edge device, regardless of their location and devices.

- Cisco Catalyst Wireless Gateway CG113 Series: Simple-to-deploy wireless router designed to empower the remote workforce to collaborate like never before. Flexible Wi-Fi 6 and cellular failover deliver a consistent application experience with enterprise Wi-Fi connectivity and security extended to the remote workforce. A centralized dashboard automates deployment and management in an agile manner. A small and silent form factor accelerates the transition to the hybrid workforce where and when it is needed. The Catalyst Wireless Gateway can either be used as a standalone wireless home router or integrated with Cisco SD-WAN RA.

Q: What are the key benefits and features of the routing solution?

A: The routing solutions offers:

- A consistent and optimized application experience with seamless connectivity to cloud and SaaS applications
- Automated deployment, configuration, and management of hybrid work routing solutions with Cisco vManage
- An integrated cloud-delivered SASE architecture for unified security policy and compliance across the hybrid workforce

- Scalable hardware or software endpoint options that accelerate the transition to hybrid work where and when it is needed, in a simple and agile manner
- The ability to leverage existing branch infrastructure, thereby lowering the Total Cost of Ownership (TCO) while extending enterprise-grade SD-WAN in a flexible and distributed manner
- End-to-end micro- and macro-segmentation
- A highly scalable and distributed architecture, eliminating single points of failure in the network

Q: What is Cisco SD-WAN Remote Access (Cisco SD-WAN RA)?

A: Cisco SD-WAN RA brings the ability to terminate remote-access users directly onto the nearest Cisco SD-WAN edge device (headend, branch, data center, or into the cloud). This integration of RA functionality into Cisco SD-WAN eliminates the need for separate Cisco SD-WAN and remote-access networks, as Cisco IOS® XE devices in the SD-WAN overlay network can function as remote-access headend devices. Remote workers can simply leverage existing remote-access clients (including Cisco AnyConnect, Windows, Apple OS native clients, and hardware-based routers such as the Catalyst Wireless Gateway) to access the SD-WAN, regardless of their location and devices.

SD-WAN RA effectively extends all the benefits of Cisco SD-WAN to the remote workforce without additional hardware investment, including optimal cloud integrations and visibility, all under a scalable SASE architecture.

SD-WAN RA provides the following advantages:

- Scalability: Enables large-scale distributed deployment across Cisco IOS XE SD-WAN devices within the SD-WAN fabric
- Improved user experience: Connects a remote worker to the closest SD-WAN-RA headend, decreasing latency and improving the overall user application experience
- Flexibility: Supports both Cisco and third-party software and hardware remote-access clients
- Security: Supports IKEv2/IPsec-based remote-access VPN. Full integration with Cisco Identity Services Engine (ISE) or any third-party AAA/RADIUS server for identity-based policy.
- Centralized management and monitoring: Eliminates the need to have multiple management consoles and unifies both SD-WAN and remote-access configuration and monitoring into a single highly visualized dashboard (Cisco vManage)

Q: What routers are available as part of this routing solution?

A: Table 2. Routers and features supported by the Remote Workforce Routing solution

Type of router and features	Model or description
Cisco SD-WAN Remote Access	Cisco SD-WAN RA enables Cisco IOS XE SD-WAN devices to provide remote-access headend functionality, managed through Cisco vManage. Available in Cisco IOS XE Release 17.6.1 and later.
Cisco Catalyst Wireless Gateway	CG113-W6x, CG113-4GW6x
Cisco ISR	C1131-8PWx, C1131X-8PWx

Q: Is this routing solution also available for non-SD-WAN deployments?

A: The Remote Workforce Routing solution has two deployment options:

- Cisco SD-WAN RA: Integrates the ability to terminate remote-access VPN tunnels directly onto the nearest SD-WAN edge device and delivers enterprise-grade SD-WAN benefits to the remote workforce. This solution supports flexible software-based endpoint clients (such as Cisco AnyConnect, Windows, or macOS-based native IKEv2 clients) and hardware-based endpoints (such as the Catalyst Wireless Gateway CG113 Series or Cisco IOS XE routers).

- Cisco Catalyst Wireless Gateway CG113 Series: Simple-to-deploy wireless router with Wi-Fi 6 and cellular failover. This solution extends enterprise Wi-Fi connectivity and security to the home user with plug-and-play zero-touch orchestration, configuration, and monitoring using a centralized dashboard (through Cisco vManage). This solution can be used in a standalone deployment or can be integrated with the SD-WAN RA solution.

Ordering questions

Q: How do I purchase the Cisco SD-WAN RA?

A: Please refer to the Cisco SD-WAN RA ordering guide. <https://salesconnect.cisco.com/#/content-detail/d80cd4fe-1537-4f6c-a7f6-3b95f2159d22>

Q: How do I purchase the Cisco Catalyst Wireless Gateway solution?

A: Please refer to the Cisco Catalyst Wireless Gateway CG113 Series ordering guide. <https://salesconnect.cisco.com/#/content-detail/609940aa-63e2-4484-ac60-fedb3650dfe1>

Q: Is a subscription available for those who already have compatible hardware at home?

A: Yes, you need to buy only the Remote Workforce Network licensing subscription if a remote worker has a supported wireless access point or router at home. For a corporate SSID extension at home, you'll still need to purchase the AIR-DNA-RW license subscription (available as part of the package).



Q: Which geographical regions are these solutions available for?

A: The offer is globally available, subject to country compliance certification of the supported routers and applicability of wireless bands in your geographies.

Q: Where can I go to learn more about these solutions?

A: For more information, go to Cisco.com/go/networkresiliency.