

Cisco Virtual Office

Flexibility and Productivity for the Remote Workforce

Cisco Virtual Office Overview

Q. What is the Cisco® Virtual Office?

- A.** The Cisco Virtual Office solution provides secure, rich network services to workers at locations outside of the traditional corporate office, including teleworkers, full- and part-time home-office workers, mobile contractors, and executives. By providing extensible network services that include data, voice, video, and applications, the Cisco Virtual Office effectively creates a comprehensive office environment for employees, regardless of their location.

Q. What are the features of Cisco Virtual Office?

- A.** Cisco Virtual Office supports applications such as secure voice, video, and wireless solutions; secure IP Multicast; and IP services such as quality of service (QoS), Network Address Translation (NAT), and split tunneling.

Q. What components are included and required to deploy Cisco Virtual Office?

- A.** For a home office, all you need is a router, an IP phone, and an Internet connection (for example, DSL or cable modem connectivity from your home). The router and IP phone are included as part of the Cisco Virtual Office solution.

For the corporate headquarters, a Cisco IOS® Software-based router is required for VPN aggregation. In addition, management servers for policy configuration; configuration deployment; and identity authentication, authorization, and access control are required.

Q. How does Cisco Virtual Office work?

- A.** For a home office, you just need to plug the router into your Internet access device. The router automatically receives the appropriate configuration that is required based on the services that you need. Your corporate IP phone automatically registers with the Cisco Unified Communications Manager, assuming its MAC address was registered for you.

For the corporate headquarters, Cisco Virtual Office uses Cisco IOS Software at the remote site to manage a digital certificate infrastructure and for VPN concentration. All of these devices are managed from a single user interface with a Cisco management tool.

To provision a new home office, you first fill out a request form. Cisco Security Manager is configured with all the security policies ready to deploy. Your user profile and the device are created on the back-end Cisco Secure Access Control Server (ACS), the authentication, authorization, and accounting (AAA) server. After you receive the Cisco Virtual Office home router and connect it to the Internet, type a URL in a browser (for example, <https://join-my-company-cvo.company.com>) to authenticate your one-time password (OTP) AAA credentials (or whatever authentication policy is defined by company policies). This process triggers router configuration.

Q. What types of network services are available with Cisco Virtual Office?

- A.** Cisco Virtual Office supports many secure services, including wireless, voice, video, and even TelePresence. These services are essential for enhancing the communication and collaboration capabilities for Cisco Virtual Office, allowing you to take advantage of tools such as Cisco IP/TV, Cisco Unified MeetingPlace® conferencing, WebEx® technology, dual-mode phones, and more.

Q. Who can benefit from Cisco Virtual Office?

- A.** Cisco Virtual Office is applicable to all industries (financial, healthcare, government, retail, education, biotechnology, and more). It is targeted toward commercial, enterprise, and service provider networks. It can be beneficial to organizations in terms of productivity, business resilience, and reduced costs, as well as to end users in terms of offering time flexibility and a rich, office-caliber experience without the need to travel to the corporate office.

The solution is appropriate for employees who need consistent access to content at home or at work, as well as full-time telecommuters who require the same IP telephony and data connectivity as at the corporate site. It is also appropriate for small branch deployments where network services are expected but onsite technical support and IT staff are not available.

Q. How would an enterprise benefit from Cisco Virtual Office?

- A.** Cisco Virtual Office provides many benefits across different groups within enterprises:

- For end users:
 - Work schedule flexibility, better work-life balance
 - Helps control costs by reducing commuting hours, saving on gas and vehicle mileage, insurance costs
 - Improves collaboration capabilities while working from SOHO locations
 - Allows spouses and children to access Internet without introducing additional security risks to corporate policy
 - Minimal set up and maintenance requirements (zero-touch deployment)
- For IT organizations:
 - Extends real-time services such as voice, wireless, video, and data to remote locations with no IT staff
 - Mitigates risks in split tunneling scenarios, permitting personal Internet access to be combined on the same device
 - Simplified IT management and maintenance for greater consistency for policy configuration at the remote site
- For Business Decision Makers:
 - Improved productivity at remote site locations
 - Reduced operation costs
 - Improved business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
 - Enables Green best practices

Q. How secure is Cisco Virtual Office?

- A.** Cisco Virtual Office provides layered secure identity, meaning that the different layers of connections have secure authentication mechanisms—and a two-factor authentication form is highly recommended. Family or guests are allowed to connect to the Internet over the remote Cisco Virtual Office router; you can use the 802.1x standard or a Layer 3 web authentication mechanism to securely segment access over separate VLANs.

For encryption, Cisco Virtual Office uses IP Security (IPsec) with Triple Digital Encryption Standard (3DES) or Advanced Encryption Standard (AES).

Also, Cisco recommends using a public key infrastructure (PKI), which is usually installed at the beginning of the Cisco Virtual Office deployment, because PKI is a much better security solution than preshared keys and PKI is easy to manage with Cisco Virtual Office.

Q. What is the difference between using Cisco Virtual Office and using a software-based remote-access VPN?

- A.** Compared to a traditional VPN, Cisco Virtual Office provides faster access times because it implements a hardware VPN. It also provides increased security through the recommended 802.1x device authentication.

Q. How does Cisco Virtual Office compare to Linksys products or other home networking solutions?

- A.** Linksys is a teleworking solution for customers who wish to deploy and manage their home networking solution themselves. The user profile for this typically includes occasional day extenders that use VPN at home or even small businesses.

Cisco Virtual Office is a teleworking solution where another party is managing the solution, whether it is a central headquarters, a service provider or a channel partner. This means that Cisco Virtual Office can take advantage of advanced deployment and maintenance capabilities, such as the zero-touch capabilities, where security policy configurations can be pushed to the client. The user profile for this is typically a business employee that is leveraging their corporate network for services to do work from home, or small branches that require centralized management and support.

In many instances, it is even useful to use a Linksys device within a Cisco Virtual Office deployment. The Linksys device can be connected to a port on the Cisco router that is dedicated for non-corporate Internet traffic. The Linksys device would provide the ability to network any number home computers or devices.

Technical Details

Q. How many users does Cisco Virtual Office support?

- A.** Cisco Virtual Office is a scalable solution that can support many thousands of sites in one domain. You can replicate Cisco Virtual Office headends across multiple data centers. Typically, users are connected to small distributed data centers (depending on availability), or they can connect to high-concentration data centers that support many thousands of users. With this distributed environment, Cisco Virtual Office has virtually no limitations in terms of the number of sites it can support.

Q. How do I install Cisco Virtual Office?

- A.** The installation of Cisco Virtual Office involves two sides: the corporate and the end user. The corporate side consists of management servers and VPN headends, which can be deployed and configured by Cisco or one of our approved partners.

The end-user side is typically installed by the end user, following simple instructions. The end-user equipment consists of a router (Cisco 871, 881, or 1811 Integrated Services Router, etc.), and it is deployed using an administrator zero-touch deployment method. In simple terms, the end user invokes the configuration procedure by establishing a HTTPS connection to the provision server, and upon valid authentication, the Cisco Virtual Office end-user router is configured automatically.

Q. What services are available as part of the Cisco Virtual Office solution?

- A.** As part of the Cisco Virtual Office solution, we help you successfully deploy and integrate headend solution components and we guide you through automating the deployment and management of remote sites by providing support for planning, design, and implementation. We also help you reduce operating costs; keep devices working efficiently; and continually assess, tune, and evolve your Cisco Virtual Office to keep pace with changes in your business and evolving security threats through ongoing operational support and optimization.

Q. Does Cisco Virtual Office support private Internet use as well as corporate use?

- A.** Yes. Corporate and "family traffic" are separated by two different VLANs. Family or guest traffic is sent directly to the Internet. Corporate traffic is securely routed to a corporate data center. Depending on your company's information systems security policies, split tunneling is enabled for corporate users, so that Internet traffic is routed directly to the Internet.

Q. What do I need in order to use an IP phone? Does it have to be a Cisco phone?

- A.** Cisco IP phones are ready to use, but they need to be configured for your telephone number in the corporate Cisco Unified Communications Manager. Depending on how Cisco Virtual Office is deployed, the IP phone can be preconfigured from IT or added later on.

Power over Ethernet (PoE) is required in the Cisco 881 for the IP phone to draw power from the Ethernet connection. You can also use a power supply to power the IP phone.

You can connect Cisco IP phones to any LAN port in the Cisco Virtual Office router when you use 802.1x, or connect them to specific ports (F0 or F1) when you use web-auth proxy.

You can also use third-party phones, such as generic SIP phones. These phones will not be automatically detected, and will need to be connected to a port designated for voice-only traffic. Cisco routers also have support for SIP Application Layer Gateway code which allows non-Cisco SIP phones to sit behind the router and register with their SIP proxy server.

Q. Does Cisco Virtual Office support wireless?

- A.** Cisco Virtual Office supports wireless services such as wireless LANs (WLANs), wireless IP telephony (IPT), and unified wireless services. The Cisco 880 Series Integrated Services Routers have Lightweight Access Point Protocol (LWAPP) support, and soon will have control and provisioning of wireless access points (CAPWAP) support.

You can deploy Cisco Virtual Office for both corporate and family wireless, because the Cisco Virtual Office router supports multiple Service Set Identifiers (SSIDs). For the corporate wireless, policies are typically the same as in the corporate headquarters. For family wireless, Wireless Equivalent Privacy (WEP)-based SSIDs can typically be preconfigured. In the future, you will be able to have local login to a family wireless tool to change the personal wireless parameters.

The most common WPA-enterprise and WPA-personal methods are supported. Digital certificates (Extensible Authentication Protocol-Protected Extensible Authentication Protocol [EAP-PEAP] with Transport Layer Security [TLS]) are also supported.

Q. What is zero-touch deployment, and how does it apply to Cisco Virtual Office?

- A.** Traditionally, for client VPN routers, the IT staff preconfigures the VPN router first and then ships it to you for installation. This process is very "manpower-intensive." For Cisco Virtual Office, after the framework is in place at the central site, a ready-to-use router with a factory default configuration is securely provisioned automatically by the Cisco Virtual Office system. You just plug in the router to your Internet connection and follow the secure device provisioning steps sent by the IT administrator. Basically, you are asked to connect a PC to the router and type in the URL of the provisioning server. This URL uses Secure Sockets Layer (SSL; HTTPS) to make the connection secure. The provisioning server then asks you for the corporate credentials and username and password; if authentication is successful, the router is configured in 4 to 5 minutes.

Q. I want to be able to browse the Internet for my personal use, as well as access the corporate network. How does Cisco Virtual Office separate the two activities?

- A.** Split tunneling and two separate VLANs separate the two kinds of traffic. The corporate routes are pushed to the spokes through the routing protocol chosen for Dynamic Multipoint VPN (DMVPN); only traffic going to the corporate network is routed to the tunnel interface. The remaining traffic goes through the default gateway, which points to the Internet service provider (ISP).

In some cases, as your company's information systems security rules, split tunneling is disabled. In that case, when the corporate user is connected to the Cisco Virtual Office router, all traffic comes through the corporate data center, including Internet traffic.

Q. Do I need to use a VPN client after I have Cisco Virtual Office set up?

- A.** No. The wired and wireless connections are already encrypted through a hardware-based VPN. A VPN client is not required.

Q. How does Cisco Virtual Office prevent teleworker family members from accessing the corporate network?

- A.** The noncorporate PC gets an IP address from a local pool that does not have access to the VPN. Only PCs that pass 802.1x authentication (or web-auth proxy authentication) can access the corporate network. Before your machine gets access to the corporate network, you have to enter credentials and get access. Corporate users and family members are placed in separate VLANs based on their authentication.

Q. What are my options for voice-over-IP (VoIP) support?

- A.** Cisco Virtual Office supports physical VoIP phones, wireless VoIP phones (Skinny Client Control Protocol [SCCP] and Session Initiation Protocol [SIP]), and the Cisco IP Communicator for secure VoIP. You can also use dual-mode phones, such as the one available from Nokia, with Cisco Virtual Office.

Q. Does the Cisco Virtual Office solution support Apple Macintosh platforms?

- A.** Yes. Cisco Virtual Office is OS agnostic. The solution transparently passes traffic from the remote network back to the corporate network. Any OS or endpoint system that is supported in the corporate office is also supported as part of a Cisco Virtual Office deployment.

Q. What kind of video support does Cisco Virtual Office provide?

- A.** The Cisco Unified Video Advantage solution facilitates personal video telephony using a Cisco camera connected to Cisco IP phones.

Also, the Cisco Unified IP Phone 7985G, a "Tandberg"-like video IP phone, is supported with Cisco Virtual Office and the Cisco Unified Communications Manager.

When available, the personal Cisco TelePresence™ System 500 will be supported.

Q. What is the minimum bandwidth required at the telecommuter site for IP phone functions?

- A.** A minimum bandwidth of 250 kbps is required at the telecommuter site for voice and data functions. For video, voice, and data, you need 700 Kbps from your ISP.

Q. How scalable is the Cisco Virtual Office solution? How many users does it support?

- A.** The Cisco Virtual Office solution is highly scalable and there is virtually no maximum number of users. You just deploy more headends as the number of users increases.

Q. Does Cisco Virtual Office provide QoS? How?

- A.** Hierarchical QoS provides shaping and Low Latency Queuing (LLQ), allowing for simultaneous use of voice and data services without compromising on the quality of either of them, and allowing for prioritization of real-time and latency-sensitive traffic such as voice and video.

Also, Network Based Application Recognition (NBAR) performs deep packet analysis to determine what protocol is used (SIP, SCCP, H.323, Skype, etc.). With NBAR combined with QoS, the Cisco Virtual Office router makes sure that gaming and peer-to-peer applications are not wrongly prioritized, because these types of applications often mask differentiated-services-code-point (DSCP) bits to gain network benefits.

Q. How do bandwidth-heavy applications affect Cisco Virtual Office voice quality?

- A.** Because of QoS guarantees provided by Cisco Virtual Office, external bandwidth-heavy applications do not cause degradation of the quality of voice in the application. Because NBAR recognizes voice traffic, it can guarantee that type of traffic a minimum amount of bandwidth, policy routing, and preferential treatment.

Q. Can I use my dual-mode phone with Cisco Virtual Office?

- A.** Yes. You can use dual-mode phones with the Cisco Virtual Office solution. Your dual-mode phone is assigned the same extension as the phone you use at the corporate site, and you can use it at home as well as at public hotspots.

Q. Can I have wireless access for family members?

- A.** Yes. Cisco Virtual Office allows family members to use the Internet wirelessly. Because the traffic is on separate VLANs, family members cannot access the corporate network.

Q. Can I connect third-party devices to the small office or home office (SOHO) router?

- A.** Yes. Cisco Virtual Office provides end-host support for PCs, Macs, laptops, UNIX, and Linux. You can also connect third-party phones to the teleworker router. When you use 802.1x or web-auth proxy, you need to bypass authentication for some devices, such as IP phones.

Q. I have my own router at home connected to the cable modem. Where does the Cisco Virtual Office router sit?

- A.** Your Cisco Virtual Office router should be connected directly to the modem that gives you access to the Internet. The family router should be connected to the Cisco Virtual Office router.

The other way around is also possible; you can connect the Cisco Virtual Office router to an intermediate router. We do not recommend this design, however, because Cisco Virtual Office cannot perform QoS in the family router, and family traffic can impair voice and video quality.

Q. Can I use a network printer with Cisco Virtual Office?

- A.** Yes. You can use a network printer with Cisco Virtual Office by connecting it to a nonsecure port on the router. However, you need to enable split tunneling, and your specific firewall rule needs to allow it.

Ordering**Q. How do I order Cisco Virtual Office?**

- A.** The ordering process for the Cisco Virtual Office is simple. To determine what you need for your remote sites, headend aggregation and management location(s), consult your Cisco representative. They can determine your specifications with the help of an ordering guide.

Q. How do I order Cisco Virtual Office services?

- A.** Cisco Virtual Office Planning, Design, and Implementation Service is a scoped service provided from the Worldwide Security Services Practice. You can order it through a Statement of Work using the appropriate theater-specific part number: AS-SEC-CNSLT (United States, Canada, and Europe), AS-SEC-CNSLT-A (Asia Pacific), or AS-SEC-CNSLT-L (Emerging Markets).

You can order Cisco Remote Management Services through subscription part numbers. More information is available at <http://cisco.com/go/ros>.

You can order Cisco Security Optimization Service through the Advanced Services Pricing Tool at http://wwwin-tools.cisco.com/CAIT/ASPT/load_opps.do.

Q. Which router platforms and which IP phone models are supported?

- A.** The supported router platforms include Cisco 870, 880, 1800, 1900 Series Integrated Services Routers for a teleworker scenario; Cisco 1800, 1900, 2800, and 2900 Series Integrated Services Routers for SOHO access; and Cisco 1800, 1900, 2800, 2900, 3800, and 3900 Series Integrated Services Routers for a site-to-site or branch-office deployment.

With regard to IP phone models, Cisco Virtual Office supports any Cisco wired phone and the Cisco Unified Wireless IP Phone 7920, the Cisco Unified IP Phone 7985G, and Cisco IP Communicator, using SCCP or SIP.

Typically, the same desktop IP phone is used at home as in the office. For example, the Cisco Unified IP Phone 7961G is a common office desktop IP phone as well as a Cisco Virtual Office IP phone.

For More Information

For more information about Cisco Virtual Office, visit <http://www.cisco.com/go/cvo> or contact your local Cisco account representative.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)