The bridge to possible

Cisco Secure Connect

The bridge to possible

Overview

Cisco® Secure Connect is a unified, turnkey solution with a blueprint for SASE made easy. It converges SD-WAN and SSE to enable operational consistency across premises to cloud in one powerful Meraki® dashboard, streamlining management across networking and security. Designed to be simple, complete, and unified, Secure Connect powers hybrid work across branch and remote, delivering greater network resiliency and seamless user experiences, everywhere.

Q: What is SASE?

A: SASE (Secure Access Service Edge) is a key enabler of any organization's hybrid work strategy. SASE combines networking and security functions in the cloud with campus, branch, remote worker, and contractor (B2B) connectivity to deliver a secure, seamless user experience anywhere users work. But deploying SASE can be complicated. Connecting existing branch SD-WAN appliances and the myriad of user endpoints to a secure cloud-based fabric requires planning, integration, and configuration.

Key components under SASE are SD-WAN, including routing, and Security Service Edge (SSE), including Zero-Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), Secure Web Gateway (SWG), and remote access as a service.

Q: What is Zero-Trust Network Access (ZTNA)?

A: Zero-Trust Network Access (ZTNA) is a model that establishes trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application. Secure Connect ensures that users are validated based on identity, posture, and context before they connect to corporate applications. Users will only have access to the applications specified as a requirement to do their job.

Q: What is Secure Connect?

A: Secure Connect is a unified, turnkey SASE solution that radically simplifies the way companies can securely access applications and resources hosted anywhere – across multiple public and private clouds – from any location at any time. Easy to deploy, use, and manage through a unified cloud dashboard, it significantly reduces organizations' operational complexities to deliver greater agility, speed, and scalability.

Secure Connect securely connects users anywhere (in the branch or remote), to any application (in the private data center, public cloud, or SaaS) with a single subscription. The solution integrates client-based and clientless remote worker access, native Cisco Meraki™ SD-WAN connectivity, and comprehensive cloud-based security capabilities with ZTNA.

Secure Connect delivers these main components for a complete SASE solution:

- Remote worker connectivity with ZTNA and endpoint posture verification as part of our complete package.

- Unified SASE dashboard for management, configuration, troubleshooting, and visibility into both the SD-WAN and SSE components of SASE.
- Simple, seamless support for Meraki SD-WAN for secure branch connectivity.
- Cisco's best-in-class, cloud-based security powered by Cisco Umbrella® and, Cisco Secure Access, all configured and managed through a unified dashboard – the most comprehensive, powerful, and yet simple unified SASE solution in the market.

Q: What is the difference between Secure Connect and other similar solutions in the market?

A: Secure Connect offers customers a distinct advantage over other options in the market, due to these key differentiators:

- Secure Connect is a unified, turnkey solution for internet access, private access, and secure SD-WAN connectivity for both branch and remote workers. It is managed from a unified dashboard and consumed as a single subscription.
- Secure Connect is designed with modernized and future-ready architecture that unifies security and networking to enable a consistent experience across different technologies, with rich security, interconnectivity, and visibility.
- Secure Connect is built on proven Cisco components, with cloud security powered by Umbrella SIG.
- Secure Connect offers deep integrations with the Meraki SD-WAN, creating a unified SASE experience by extending the fabric to the cloud with just a few clicks, providing high reliability and a next-generation policy engine to centralize management across the organization, and distributing security policy enforcement optimizing the end-user experience.
- Secure Connect provides flexibility with use-case packages that allow customers to choose from two unique use cases:
  - The **Foundation package** includes Umbrella SIG capabilities, providing secure internet access connectivity for branch and roaming users; Secure Connect fabric interconnects, providing private application access for branch users; a unified dashboard, providing streamlined operations management visibility and control for security and network policies; and unified support, providing seamless support for your SASE needs. The Foundation package also includes ten free-trial (nonproduction) licenses for hosted remote access as a service, which provides private application access for remote users. This package is designed for users who only work in an office setting.
  - The **Complete package** includes production-level support, client-based remote-access-as-a-service capabilities and both client-based and clientless ZTNA capabilities, providing a zero-trust security model for users. This package is designed for hybrid users who not only work in the office but also work remotely.

Q: What problems and pain points does Secure Connect solve?

A: Secure Connect helps customers who want to:

- Unify the networking and security components of SASE into one solution for simplified, operational efficiency and a better end-user experience.
- Adopt a hybrid work model where the same employee works both from home and in the office.
- Implement a network transformation project to secure branch users optimally.
- Support lean IT and who are challenged to minimize audits and risk across remote and corporate (site) users.

- Increase the efficiency of a single network and security team, leaning on network-led SASE decisions.
- Minimize capital and operation deployment time in delivering remote access to users.
- Improve the network's security posture and resiliency with end-to-end control and visibility for policy and security across SD-WAN and the cloud.

Q: What are the key differentiators between Secure Connect and competing SASE aaS offers?

A: Our key differentiation is delivering a turnkey, unified SASE solution inclusive of SD-WAN operations and security policies through a single interface that converges and streamlines the management of networking and security on one platform. Other vendors in the market that offer both SD-WAN and SSE solutions are struggling to deliver a unified platform that accelerates the time to value of SASE outcomes by creating a streamlined interface and a SASE fabric that automatically adds SASE value as new components are expanded.

Other key differentiators:

- This is a unified solution for internet access, private access, and secure SD-WAN connectivity for both branch and remote workers managed from a unified dashboard and consumed as a single subscription.
- The solution provides a modernized and future-ready architecture that unifies security and networking to enable a consistent experience across different technologies, with rich security, interconnectivity, and visibility.
- The solution is built on proven, industry-leading Cisco components that secure 100 percent of the Fortune 100, and on our global experience connecting and securing users around the world.

Q: What does the new Secure Connect Foundation package mean for existing Cisco SIG/Meraki/ SD-WAN connector customers?

A: For customers who are looking to expand their Umbrella SIG contract and expand into Secure Connect Foundation due to the enhanced value proposition, please contact your sales rep to discuss transition options.

Technical

Q: In which regions does Secure Connect have data centers? What services are available where?

A: You can find the latest view of geolocations of available data centers and services here: https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Pre-configuration_Checklist/Data_Centers.

Q: How many sites and users are supported through Secure Connect?

A: Secure Connect can support up to 5000 sites and 50,000 users.

Q: What is the difference between Secure Connect and the Cisco Umbrella Meraki SD-WAN Connector?

A: The Cisco Umbrella Meraki SD-WAN Connector is for secure internet access from the branch site. It extends the Meraki SD-WAN fabric all the way to the Umbrella cloud. The connector can be enabled once a customer has Meraki SD-WAN and Umbrella SIG. There is a 250 Mbps limitation to each deployed connector, and a limitation to the number of connectors a customer can deploy. Outside of Secure Connect, the two solutions (Meraki SD-WAN and Umbrella SIG) are managed through two separate dashboards.

Secure Connect focuses on delivering a unified SASE experience that centralizes management of security and networking in the Meraki dashboard. It enables secure internet access with enhanced performance and additional

use cases such as remote access; ZTNA; interconnections between users, sites, and applications; and unified technical support.

Customers can choose the SASE use cases they want to adopt through Secure Connect Complete, or can simply choose the secure internet access use case through Secure Connect Foundation. A unified SASE experience is gained in both cases.

Q: What does the new Secure Connect Foundation package mean for existing Cisco SIG/Meraki/ SD-WAN connector customers?

A: Most customers using the existing integration between Meraki's MX and Umbrella SIG will be able to get a no-cost upgrade to the new Foundation license. Any customer who purchased SIG not as part of an Enterprise Agreement (EA), and without any add-ons (reserve IP, RBI, or multi-organization), should be able to have the upgrade. Customers with add-ons and/or under an EA will be able to get the upgrade in future. If you are interested in upgrading your solution, please contact your Cisco sales representative.

Q: What user device endpoints are required for remote users to connect (laptops, cellphones, etc.)?

A: Endpoint software is available for Microsoft Windows 7, 8, 10, and 11, MacOS 10.8 and later, and Linux, as well as mobile versions for Apple iOS, Android, and Google Chrome OS.

Q: We already have Cisco SD-WAN, powered by Meraki. How do we add Secure Connect?

A: Deployment of Cisco SD-WAN powered by Meraki within Secure Connect is simple and quick. In fact, once you subscribe to this offer, connecting your existing SD-WAN to the Secure Connect fabric is just a few clicks away.

There are different types of connections available to Secure Connect, based on region. Learn more on how to connect sites to Secure Connect here: https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco__Secure_Connect_Now-_Sites.

Depending on the data center, some or all of Secure Connect's capabilities are available. You can learn more about the available capabilities per data center here: https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Pre-configuration_Checklist/Data_Centers.

Q: Does Secure Connect support split tunneling/traffic steering?

A: Yes, traffic steering is supported for both Meraki SD-WAN networks and remote workers. For remote access, traffic steering in Secure Connect behaves exactly as it does with remote access on Adaptive Security Appliances (ASAs). Tunnel modes include tunnel all traffic, steer inside, and steer outside the tunnel.

Q: Does Secure Connect integrate and work with Cisco SecureX™? If so, how?

A: Secure Connect integrates with Cisco SecureX for security monitoring and controls. Proxy and DNS events are recorded and discoverable, giving users insights into events ranging from malicious file analysis to blocked malicious domains, as well as into the traffic allowed to benign destinations.

Secure login to Secure Connect from Cisco SecureX is also available; learn about how to set up SecureX login here: https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Onboarding/Cisco__Secure_Connect_-_Secure_X_Integration.

Q: Does Secure Connect have troubleshooting tools?

A: Yes, the new generative AI Assistant is offered to further simplify reporting and troubleshooting of the Secure Connect environment.

The bridge to possible

Zero-Trust Network Access (ZTNA)

Q: What ZTNA capabilities are included with Secure Connect?

Secure Connect clientless ZTNA use cases include secure connectivity from unmanaged devices of remote workers or B2B contractors to private applications. End users can securely access applications using only their browser through clientless ZTNA, where Cisco supplies certificates and domain names for quick admin configs, making setup a snap.

Alternatively, IT administrators can get similar outcomes with a client (Cisco Secure Client, formerly Cisco AnyConnect®) installed on the users' device, enabling granular access between users and applications with posture checks.

Secure Connect Client ZTNA offers a feature-rich solution powered by Cisco Secure Access, providing a seamless end-user experience that connects users to private applications using any port and any protocol. Client ZTNA has QUIC support with MASQUE proxy. Access is instant and "just works," delivering better remote worker experiences and stronger security. Administrators can reduce the attack surface, enforce least privilege controls, enable posture validation, and eliminate security gaps in a distributed environment.

Q: Which protocols are supported for clientless ZTNA?

A: Currently, HTTP and HTTPS are supported for the clientless ZTNA solution.

Q: Can we bring our own MFA for clientless ZTNA?

A: The Secure Connect ZTNA capability supports all MFA solutions that are used as part of a customer's SAML authentication. Customers can bring their own MFA.

Q: What posture capabilities are supported by Secure Connect?

A: For our client-based remote access as a service capabilities, the machine certificate, OS (operating system), firewall, disk encryption, and anti-malware for each endpoint are checked. The posture policy verdict is either "block" or "allow"; "quarantine" is not supported.

For our clientless ZTNA solution, the IT administrator can create posture profiles based on OS type and version, browser type and version, and geolocation.

Q: Is it possible to do the posture through our own Cisco ISE infrastructure? If yes, how?

A: Posture checking through Cisco ISE is not supported.

Cisco Catalyst SD-WAN integration

Q: What is the scope of the Cisco Catalyst® SD-WAN (Viptela®) integration?

A: Cisco Catalyst SD-WAN customers will be able to enjoy the key use cases that Secure Connect offers as a turnkey SASE solution. This includes:

- Securing branches and corporate locations to public and private applications.
- Securely connecting remote workers to private and public applications, including:
  - Client connectivity with zero-trust outcomes, enabling identity-based policies to private applications.
  - Clientless, browser-based connectivity.

The first stage of the integration will focus on connectivity between Cisco Catalyst SD-WAN devices and Secure Connect. It will continue leveraging the automation in place between SIG and Cisco Catalyst SD-WAN, and will add private access to it, with dynamic routing for an easy set up.

Q: How is this different from the existing integration between Cisco Umbrella SIG and Viptela?

A: There are multiple differences between the Umbrella SIG/Catalyst SD-WAN integration and Secure Connect:

In terms of use cases, Cisco Umbrella SIG offers secure internet access to branch users and roaming (SWG) support for remote users. This use case is also a part of Secure Connect. Further, we add client-based remote access that enables identity-based access to private applications and secure internet access for all ports and protocols through Secure Connect, and clientless access to HTTP/HTTPS applications.

Secure Connect with Cisco Catalyst SD-WAN gives a unified management and policy control for integration of private applications or resources behind the Viptela service hub. Further, this enables interconnect capability where remote access users can securely access Cisco Catalyst SD-WAN resources integrating with Secure Connect.

Q: Which dashboard is used for management for Cisco Catalyst SD-WAN (Viptela)?

A: Secure Connect is managed through the Meraki dashboard, with some cross-launches into the Cisco Umbrella dashboard for specific tasks. The Meraki and Umbrella dashboards are tightly coupled, with single sign-on and RBAC synchronized between the two for a seamless experience. Any configuration for Cisco SD-WAN (Including tunnel setup, BGP configuration, etc.) is still being done through Cisco vManage.

Q: Is the Cisco Catalyst SD-WAN integration supported by both Secure Connect Foundation package and Complete package?

A: Yes, for a mixed organization; for example, if a customer has Cisco Meraki and Catalyst SD-WAN, or if a customer needs both secure internet access and secure private access.

If the use case is only Cisco Catalyst SD-WAN for secure internet access, leveraging the SIG integration might provide a better experience to customers.

Support

Q: What is the Secure Connect trouble-shooting support model?

A: Secure Connect includes 24/7 trouble-shooting support. It provides a single point of contact for all parts of the solution, across networking and security, and will be the point of contact for customers when they have an issue with Secure Connect. Customers can reach out through a direct phone number and through the dashboard. To learn more go to: https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Troubleshooting_Guides/How_to_Contact_Cisco___Secure_Connect_Support.

Q: How does Secure Connect support onboarding services?

A: Enhanced and premium support SKUs are available for seamless onboarding services. Please contact your Cisco sales representative if you are interested.

Pricing and packaging

Q: What package options are available for Secure Connect?

A: Secure Connect is offered in two packages that make it easy for customers to choose the right level of protection and coverage for their organizational needs: Secure Connect Foundation and Secure Connect Complete.

Secure Connect Foundation package

The Secure Connect Foundation package includes Umbrella SIG capabilities, which provide secure internet access connectivity for branch and roaming users; Secure Connect fabric interconnect, which provide private application access for branch users; a unified dashboard, which provides streamlined operations management visibility and control for security and network policies; and unified support, provides seamless support for your SASE needs. The Foundation package also includes ten free-trial (nonproduction) licenses for hosted remote access as a service, which provides private application access for remote users.

Table 1. Secure Connect Foundation package

Functionality	Secure Connect Foundation package	
	Essentials	Advantage
Security		
Secure web gateway	✓	✓
URL filtering	✓	✓
Secure malware analytics	✓	✓
Sandbox submissions	500	Unlimited
Cloud-access security broker	✓	✓
Cloud malware detection	For up to 2 applications	Unlimited
DNS-layer security	✓	✓
L3 cloud-delivered firewall	✓	✓
L4 cloud-delivered firewall	✓	✓
L7 cloud-delivered firewall		✓
IPS firewall		✓
Unified SASE		
Unified security policy	✓	✓
24x7 unified support	✓	✓

The bridge to possible

Functionality	Secure Connect Foundation package	
	Essentials	Advantage
Unified dashboard	✓	✓
Turnkey experience	✓	✓
Fabric interconnect (CNHE: cloud native head end)	✓	✓
Remote access		
Client-based access	10 free users*	10 free users*
Clientless browser-based access		
Granular user, application-based access policy	*	*
SAML authentication	*	*
Posture and contextual access control	*	*
Reporting	*	*

* Six-month trial-only nonproduction licenses

Secure Connect Complete package

The Secure Connect Complete packages includes production-level support, client-based remote-access-as-a-service capabilities, and clientless/client ZTNA capabilities, which provide a zero-trust security model for users.

Table 2. Secure Connect Complete package

Functionality	Secure Connect Complete package	
	Essentials	Advantage
Security		
Secure web gateway	✓	✓
URL filtering	✓	✓
Secure malware analytics	✓	✓
Sandbox submissions	500	Unlimited
Cloud-access security broker	✓	✓
Cloud malware detection	For up to 2 applications	Unlimited
DNS-layer security	✓	✓
L3 cloud-delivered firewall	✓	✓
L4 cloud-delivered firewall	✓	✓
L7 cloud-delivered firewall		✓
IPS firewall		✓

The bridge to possible

Functionality	Secure Connect Complete package	
	Essentials	Advantage
Unified SASE		
Unified security policy	✓	✓
24x7 unified support	✓	✓
Unified dashboard	✓	✓
Turnkey experience	✓	✓
Fabric interconnect (CNHE: cloud native head end)	✓	✓
Remote access		
Client-based access	✓	✓
Clientless browser-based access	For up to 10 applications	Unlimited
Granular user, application-based access policy	✓	✓
SAML authentication	✓	✓
Posture and contextual access control	✓	✓
Reporting	✓	✓

Q: Where is Secure Connect currently available?

A: This offer is available in certain geographic regions depending on the package offering, as follows:

The Foundation package is offered in all countries except for: China, Cuba, Iran, North Korea, Russia, Sudan, and Syria.

The Complete package is offered in all countries except for China, Cuba, Iran, North Korea, Russia, Sudan, and Syria.

Q: How do I purchase Secure Connect?

A: To purchase a Secure Connect subscription, contact your Cisco account manager or a Cisco partner.

Q: What is the pricing structure for Secure Connect?

A: Secure Connect is licensed on a subscription basis with two packages, each having two tiers, Essentials, and Advantage:

Secure Connect Foundation package: Focused on secure internet access for branch and roaming users.

- Essentials: Secure connectivity.
- Advantage: Data protection and advanced security.

Secure Connect Complete package: Focused on hybrid users that need secure internet access, ZTNA, and remote access as a service.

- Essentials: Secure connectivity.
- Advantage: Data protection and advanced security.

Subscriptions are available for standard-term lengths of 12, 36, and 60 months. Secure Connect is licensed per seat. A seat is defined as an internet-connected user who may have access to the service. Seat counts are independent of the number of devices or endpoints protected. Contact your Cisco account manager or a Cisco partner for pricing.

Q: Is Remote Browser Isolation (RBI) included in Secure Connect? How can we add on RBI?

A: Remote Browser Isolation (RBI) is not currently available in Secure Connect, nor can it be purchased a la carte for use with Secure Connect at this time. The following current Cisco Umbrella packages are not eligible to be replaced through a modified subscription with Secure Connect: Cisco Umbrella RBI, Cisco Umbrella through any Enterprise Agreement (EA), or Cisco Umbrella Premium support, or if there are more than 36 months remaining on an existing Cisco Umbrella subscription.

Q: Is reserved IP included in Secure Connect? How can we add reserved IP?

A: Reserved IP is available as an add-on service for Secure Connect Complete and Foundation.

Q: How many IPs can be ordered?

A: Two IPs are the minimum requirement, one as a primary and one as a failover.

Q: Why are data-center pairs important?

A: Data-center pairs for IPsec tunnels provide backup, or failover service, if one data center is unavailable. Customers can use data centers that are not paired but will have to manage failover manually.

Q: Which data centers support reserved IP?

A: Available data center list: https://docs.umbrella.com/umbrella-user-guide/docs/cisco-umbrella-data-centers.

The bridge to possible

Q: Does Reserved IP have Anycast support?

A: Currently, reserved IP does not support anycast; therefore, customers should use IPsec tunnels to connect their networks to Umbrella for reliable use of their reserved IP(s). For roaming computers, a client VPN should be used to forward web traffic to a network where an IPsec tunnel has been established to an Umbrella data center provisioned with a reserved IP.

Q: Are customers allowed to upgrade/move from the Secure Connect Foundation package to the Secure Connect Complete package?

A: Secure Connect Foundation Essentials customers can upgrade to a Complete Essentials or Advantage package. Secure Connect Foundation Advantage customers can only migrate to a Complete Advantage package.

C67-3064206-04 06/24