

MASTER SERVICES AGREEMENT

SERVICE DESCRIPTION



SERVICE DESCRIPTION: CONNECTED BUSINESS SASE

DESCRIPTION

Connected Business SASE is a cloud-native security suite built on Cisco Secure Connect. Connected Business SASE provides security functions to support today's SD-WAN based networks, and comes in two versions:

- Foundation Essentials or Advantage – covering branch access (SIA)
- Complete Essentials or Advantage – covering branch access (SIA) and remote access (SRA, SPA)

Component	Foundation	Complete	Description
Secure Web Gateway	Yes	Yes	Helps protect from online threats by enforcing company policy and filtering internet-bound traffic
URL Filtering	Yes	Yes	Blocks defined URLs from loading on a company network
Secure Malware Analytics	500/day – Essentials	500/day – Essentials	Secure Malware Analytics rapidly analyses files and suspicious behaviour across your environment. Information about findings is available on the Meraki dashboard.
	Unlimited - Advantage	Unlimited - Advantage	
CASB (Cloud Access Security Broker)	Yes	Yes	Applies your access policies for resources and applications
Cloud Malware Detection	Up to 2 Apps – Essentials	Up to 2 Apps – Essentials	Helps discover and protect against malware infections from cloud-based services.
	All Supported apps - Advantage	All Supported apps - Advantage	
DNS-Layer Security	Yes	Yes	Helps stop malware earlier and prevents callbacks to attackers
L3/L4 Cloud-Delivered Firewall	Yes	Yes	Network and Transport layer firewall
L7 Cloud-Delivered Firewall	Yes	Yes	Application layer firewall
IPS (Intrusion Prevention System) Firewall	Yes	Yes	Intrusion prevention system firewall
CBAC (Client-Based Access Control)	No	Yes	Secure Client establishes a secure access VPN tunnel between the client application and your network
Client-based Access (AnyConnect VPN)	10 free users for 12 months	Yes	AnyConnect VPN client software
Clientless Browser Based Access	No	Up to 10 Apps – Essentials	Allows you to leverage a web browser for user authentication and application access without the need for a VPN client
		Up to 300 Apps - Advantage	
Granular User and app-based access policy	No	Yes	Secure Applications with granular access control so only authorized Users can access them
SAML authentication	No	Yes	Cisco Secure Connect enables you to bring your own identity provider (IdP) for end-user authentication to the Service. Integration establishes a trust relationship with the IdP, which allows

MASTER SERVICES AGREEMENT

SERVICE DESCRIPTION



			your Users to authenticate with their existing credentials via SAML 2.0
Built-in IDP (Intrusion Detection and Prevention)	No	Yes	Intrusion detection and prevention
Posture and Contextual access control	No	Yes	Only allows use of User devices that meet the device posture requirements of your organization
Remote access reporting	No	Yes	View and export remote access logs
Configuration – Co-Management	Where requested Admin write access can be granted to the Meraki Dashboard for the purposes of customer management, configuration and maintenance.		
Service Requests (Move, Add's Changes)	You can raise service requests via the Xport portal. Service requests are a chargeable feature. You will be advised of the charge for the service request at the time of request, unless the service request is POA, in which case you will be advised of the charge once we have assessed the scope and effort required for the service request. A separate Statement of Work may be required.		
Setup and Configuration	Setup and configuration of the Service is chargeable at an hourly rate. The quantity of hours required, and the associated charges will be determined using the hourly rates stated in the Master Services Agreement. A separate Statement of Work may be required if the effort is considered significant.		

SERVICE CONDITIONS

- Early Termination charges apply if you terminate within the Service Initial Term.
- You will need a Connected Business service to be able to subscribe to Connected Business SASE
- We will retain all administration rights in respect of our Equipment and your Configuration.
- Adjustments made by your administrators within the Meraki portal are legally binding.
- Connected Business SASE is a subscription licenced product. At the expiry of your Service Initial Term, we will automatically renew your subscription for an additional 12-month term unless you notify us at least one month prior to the expiry of the Service Initial Term that you do not require renewal. Termination during the additional 12-month term will incur early termination charges equal to the remaining part of the 12-month period.
- Third-Party tools, portals, reports and analytics may stipulate their own end user licence agreements. If you want to use any of these, you will be required to accept or agree to any such licence terms.
- Connected Business SASE relies on Internet connectivity. The Meraki portal provides a cloud-based management portal
- One NZ's Service Levels will not apply to internet access purchased from an alternate provider.
- The Configuration - Co-management portal option allows you to manage your own configuration. Any support we provide due to a fault that results from your configuration will be a chargeable service.