Vocus New Zealand

SD-WAN Service Schedule

1. Definition

1.1. Defined terms in the Standard Terms and Conditions have the same meaning in this Service Schedule unless expressed to the contrary. In this Service Schedule, unless the context otherwise requires:

Advanced Licensing or Advanced Security License means the additional security capabilities described on the Meraki website here: https://documentation.meraki.com/General_Administration/Licensing/Meraki_MX_Security_and_SD-WAN_Licensing

Base Service means Vocus-Managed with Advanced Licensing.

Customer means the Customer described in the Service Order and any of its employees, sub-contractors, agents and representatives.

Customer-Managed means that customer has full administrative control over the Meraki Dashboard.

Customer Requirements Template means a document which is used to capture detailed customer requirements for Onboarding.

End Users means any users accessing or utilising Services on behalf of the Customer.

Enterprise Licence or means the additional security capabilities described on the Meraki website here: https://documentation.meraki.com/General_Administration/Licensing/Meraki_MX_Security_and_SD-WAN_Licensing

Legacy Applications means applications hosted by the customer in a customer or 3rd party Data Centre / hosting service which need to be accessible to branches over the (SD) WAN Overlay via the Internet WAN Underlay.

Meraki Dashboard – The browser-based interface used to control and manage the Base or Variant services.

Professional Services Rate Card means the document setting out Vocus' then current rates and charges for services not expressly stated as included with the Service in the Agreement which is available to the Customer upon request.

Reference Architectures are common customer use cases comprised of designs Vocus know work as expected. Customer sites which are compliant with Reference Architectures will be provided with Service Levels better than Reasonable Endeavours.

Services mean the SD-WAN services purchased by a Customer, including the Base and or Variants and Uplifts specified in the Service Order.

Service Delivery Point means the site(s) at which Vocus will install Vocus Equipment necessary to provide the Services.

Standard Terms and Conditions means the standard terms and conditions between Vocus and the Customer governing the general terms and conditions on which Services are provided under this Service Schedule and any applicable Service Order from time to time, available at http://www.vocus.co.nz/legalcontracts.

Uplifts means addons to the Base or Variant services which deliver additional functionality.

Variant Service means Customer-Managed or Vocus Managed with Enterprise License.

Vocus Equipment means the equipment to be installed at the Service Delivery Points which Vocus uses to provide the Service.

Vocus-Managed – means that Vocus have administrative control over the Meraki Dashboard.

Vocus SLA means the Vocus service level agreement which can be found at http://www.vocus.co.nz/legalcontracts, as updated from time to time.

WAN Overlay means the encrypted VPN established by the Service. Runs over the top of the WAN Underlay.

WAN Underlay or **Access Circuit** means the Internet service used in conjunction with the Service.

Web Dashboard means the Meraki Web Dashboard provided with the Service.

2. The Services

2.1 This Service Schedule will apply to the first and any subsequent Service Orders for Services executed by the Customer and Vocus.

2.2 Vocus will provide the Base and or Variants and Uplifts of the Service and any Uplifts specified in a Service Order to the Service Delivery Points specified in the Service Order. Vocus will only provide the scope of

installation at each Service Delivery Point as specified in the Service Order. Additional services or non-standard installations will incur additional charges.

2.3 Vocus will provide the Services to the Customer on the terms of the Standard Terms and Conditions, this Service Schedule and any applicable Service Orders, all of which are binding on the Customer. The Customer must use the Services (and, where applicable, will ensure that its End Users use the Services) in accordance with the terms of the Standard Terms and Conditions, this Service Schedule, any applicable Service Orders and all applicable laws.

2.4 Vocus may vary the Service if reasonably required for technical, operational or commercial reasons. Vocus may vary the Service without prior notice to Customer provided such variation does not have a material adverse effect on the Customer. If a change to the Service is likely to have a material adverse effect on Customer, Vocus will provide at least 30 days' notice to Customer. If Customer does not agree to the proposed change, it may terminate this Service Schedule by notice in writing to Vocus prior to the change taking effect.

2.5 If Customer requests additional Services beyond it agrees to pay for those services in accordance with appropriate Rate Card.

2.6 Without limiting any exclusions or limitations of liability under the Standard Terms and Conditions, Vocus is not liable to the Customer under or in connection with this Agreement or the Services (including for any breach of confidentiality or breach of the Customer's Intellectual Property Rights) for any loss or damage arising from:

a. problems on servers operated by third parties outside the Vocus Network;

b. security incidents or failures on supplier platforms provided for the purpose of managing the Service;

c. internet failures / problems;

d. incoming or outgoing cyber security attacks

e. security breaches occurring outside the Vocus Network, including any eavesdropping or interception.

2.7 In order to use the Service, Customer is required to accept the standard terms and conditions that apply to your use of the Meraki SD-WAN including the Web Dashboard and or firmware.

2.8 Vocus is not responsible for any breaches of security, attempted or successful intrusion, loss or damage incurred by the Customer as a result of or related to any actual or perceived failure of the Service or other breach of the Customer's security

2.9 The Service have varying technical, performance and service characteristics which may vary according to a range of factors, including customer specific configurations, hardware model, network characteristics and vendor capabilities.

3. Termination

3.1 If Customer fails to provide any information or access necessary for Vocus to provision the Service (and fails to resolve this within 7 days of notice of writing by Vocus), then Vocus may terminate this Services Schedule prior to the completion of provisioning, provided that the Customer must pay Vocus for any costs incurred as a result of feasibility studies, work already completed and any costs incurred as a result of Vocus cancelling orders submitted to third party providers.

4. Customer responsibilities

4.1 To the extent the Service Order specifies that Customer is purchasing Customer-Managed or Vocus-Managed Services:

a. Vocus is not responsible for any actions or omissions of Customer implementing, configuring or using the Services, except to the extent Customer was acting in accordance with direction by Vocus.

b. The Customer must make available to Vocus internal technical resources familiar with the Customer's network required to assist Vocus with completing the Customer Requirements Template and from time to time to assist with assurance

c. Vocus will not configure customer IT systems. Customers are responsible for modifying existing customer IT systems if required.

d. Customers responsible for installing any outdoor antennas.

e. Customers are responsible for procuring infrastructure from the appropriate cloud providers for the virtual (VMX) CPE.

5. Service Level Agreement

5.1. The Customer is responsible for taking all reasonable steps to ensure that any faults reported to Vocus are within the Service before reporting the fault.

5.2. The Service Levels applicable to the Services are set out in the Vocus SLA. Customer acknowledges that different Service Levels will apply depending on the services purchased and whether those service comply with Vocus' Reference Architectures

5.3 The Service Levels for sites will be no better than the underlying access circuit.

6. Connection to the Service

6.1 The Customer agrees that in order to receive and use the Service the Customer must have an Access Circuit. For the avoidance of doubt, an Access Circuit is not a component of the Service provided by Vocus pursuant to this Service Schedule.

6.2 If the Customer orders an Access Circuit from Vocus, Vocus will provide the Access Circuit in accordance with the applicable Service Schedule.

7. Administrator

7.1 The Customer acknowledges and agrees that login IDs and passwords may be used solely to facilitate access to the Service by the Customer and its users of the Service and that Customer will not, and will ensure users do not, disclose any login ID or password details to any person who is not the Customer or the user to whom the login ID or password details relate. Customers may provide to 3rd parties who manage the Customer's IT infrastructure.

8. Web Dashboard

8.1 Vocus will provide the Customer with access to the Web Dashboard as follows:

a. Vocus-Managed Customers will be provided with view only access, except for managing guest wi-fi users where Customers will be provided with limited administrative access.

b. Customer-Managed Customers will be provided with full administrative control.

c. Vocus shall retain full administrative control on customer's dashboards for the purposes of managing the service.

d. The Customer is responsible for obtaining and or developing the capability to access and communicate with the Web Dashboard.

8.2 Vocus documentation and any technical specifications issued to the Customer by Vocus from time to time and may be revoked or restricted by Vocus at any time.

8.3 Where the Customer has access to the Web Dashboard, the Customer warrants that:

a. if applicable, at all times the Customer will transmit accurate and current data to the Web Dashboard;

b. the Customer will use the Web Dashboard for the sole purpose of performing its obligations under the Master Services Agreement, Service Schedule or Service Order; and

c. the Customer will treat all information or information containing Vocus' Intellectual Property Rights obtained or accessed via the Web Dashboard strictly in accordance with clauses 12 and 13 of the Standard Terms and Conditions.

8.4 Vocus may, at its absolute discretion and at any time modify or replace the Web Dashboard.

8.5 Where Vocus modifies the Web Dashboard, Vocus will, wherever it is practicable for it to do so, provide advance notice to the Customer but otherwise always notify the Customer as soon as reasonably possible

8.6 The Vocus Equipment will send a constant stream of data (logs) to the cloud and as such will consume a small amount of the WAN Underlay bandwidth. This data will be drawn from the Customer purchased Access Circuit.

9. Relocations

9.1. In the event the Customer requires a relocation of any of the Service Delivery Points, it must give to Vocus a Service Request in a manner nominated by Vocus. The Customer acknowledges that it may not be possible to relocate all Services to every location.

9.2. Vocus will respond to the request and advise the Customer whether the Services can be relocated and any additional fees that may apply. Depending on the new proposed location, both a one-off fee as well as a change to the monthly recurring fee may be required.

10. Fees

10.1 In addition to monthly plan fees, Vocus will charge fees for Service requests as per its standard published rates except as otherwise specified in a Service Order.

10.2 Some services have variable fees based on usage, which will be billed to Customer monthly in arrears.

11. Management

Customer may choose from one of two management models. Vocus-Managed and Customer-Managed.

11.1 Vocus-Managed

Vocus will manage the configuration of the Service in accordance with, in Vocus' sole opinion, industry best practice. Vocus will make configuration changes on behalf of customers. Customers must submit a Service Request for changes from an authorised person.

Vocus will curate the firmware and update the Meraki Equipment as appropriate.

11.2 Customer-Managed

Customers may select to self-manage the configuration of the service, and as such will be provided with full administrative rights on the Web Dashboard. This means that customer can modify the configuration of the Service as required. The customer is entirely responsible for the configuration of the Service.

All customer-managed sites will be deemed to be non-complaint with Reference Architectures as Vocus no longer have exclusive control over the configuration of the Service.

Customers should have the appropriate Meraki knowledge and expertise.

Technical assistance may also be obtained directly from Meraki as per https://meraki.cisco.com/support/..

Customers are responsible for curating and updating the firmware.

Where the head-end (hub) site(s) are non-complaint with Reference Architectures the WAN Overlay SLA for spoke site Availability will drop to Reasonable Endeavours.

SLAs can be no better than WAN Underlay.

Customers must not use their administrative rights to prevent or curtail in any way Vocus' full administrative access the Web Dashboard as Vocus require this access for license management and service management purposes.

Indirect customers will responsible for providing L1-L3 support for their customers.

11.3 Reference or Non-Reference Architectures

Customer sites can be either Reference or non-Reference Architecture sites.

Reference Architecture Sites

Reference Architectures are sites which comply with Vocus' Reference Architectures. Reference Architectures are designs which Vocus know perform to a known level of reliability and performance.

Vocus will monitor the Base or Variant Service, and alerts will be sent to the Vocus Network Service Centre for handing in accordance with Service Levels.

Non-Compliant Reference Architecture Sites

Non-Reference Architecture sites are sites, which for a range of reasons, do not comply with Vocus' Reference Architectures. Customer-Managed sites are deemed to be non-complaint with Reference Architectures.

Vocus will monitor the Base or Variant Service, and alerts will be sent to customers. Customer will need to interpret alerts, and where a fault exists with the Service, log an incident with the Vocus.

Non-Compliant Reference Architectures sites will be provided with Reasonable Endeavours Service Levels, expect for Hardware Replacement Service Levels which remain unchanged.

Customers are responsible for managing any issues arising from Meraki firmware updates.

Customers may request technical assistance from Vocus and this will be a chargeable activity at Vocus' standard published rates except as otherwise specified in a Service Order.

12. Licensing

12.1 Service Requests to change the type of security licence (e.g. from Advanced Licensing or Advanced Security License to Enterprise Licence or vice versa) will be considered on a case by case basis.

13. Cyber Security

Like all solutions the SD-WAN security capability has its limitations.

Meraki MX devices provide a network firewall. The 'Advanced Licensing' can detect malware and network intrusion attempts. The 'Enterprise Licensing' option cannot and only provides network firewalling.

General Limitations

A network firewall, even one that provides Advanced Licensing is only one layer in customers' cyber defences. Customers should deploy a defense-in-depth strategy comprised of many layers of defense as part of a security policy appropriate for their business. Best practice controls at a minimum should include: network firewalling, end-point malware prevention / firewalling, content filtering, application & device whitelisting, regular patching, user education and the limiting of administrative permissions on end points.

Customers should also assume that at some point they will their systems will be compromised. Systems such as regular backups and incident handling processes should be developed. Customers should review the advice provided by https://wdww.cert.govt.nz/ at a minimum. The advice of an independent security specialist is strongly recommended.

Vocus do not provide a managed security service. We provide a managed & monitoring CPE-based service with either Enterprise or Advanced Licensing capabilities. We do not manage or interpret security alerts arising from CPE. Vocus will configure the Service in accordance with the customer security policy to the extent supported by the CPE and licensing, however from an operational perspective we don't provide any security incident or event management (SIEM).

If the customers security policy changes we will work with the customer to implement that policy on the CPE.

Enterprise Licensing Limitations

This licensing option only provides basic firewalling. The CPE will not detect unauthorised access or viruses. This will save 20-30% on Vocus monthly fees, however the customer will almost certainly need to take additional security measures on their network, and may have an increased risk of security incidents.

Advanced Licensing Limitations

Advanced Licensing, while reasonably advanced has a number of limitations, including:

- Exploits must be known as detection is based on signatures
- The CPE needs to be online to perform file reputation checking as each file is checked against an online database
- Any MX CPE deployed in VPN Concentrator Mode will only have Enterprise Security Licensing / Functionality
- Encrypted SSL traffic will not be checked for malware or exploits.

Note: Encrypted SSL traffic will not be checked for malware or exploits – Note that increasing numbers of websites / web-services have deployed SSL to encrypt internet traffic. This is a good security measure as it keeps communications between users (clients) and applications (servers) (i.e. your bank, Facebook, Zoom, etc.) secure. Any bad actor who might attempt to snoop traffic would only get a collection of random characters, however this also means that network security devices cannot decrypt and inspect traffic (a.k.a. snoop), and therefore any malware or exploits within that SSL stream will not be prevented from getting to the end point.