MANAGED WIRELESS LAN SERVICE

1.   **GENERAL**

1.1   **Service Definition.** Verizon's Managed Wireless LAN service (Managed WLAN) extends Customer's Verizon-managed WAN or LAN infrastructure to include wireless LAN access.

1.1.1   **Platforms**. Except where explicitly stated otherwise, these terms apply to Optimized Service and non-Optimized Service.

1.2   **Standard Service Features.** Optimized Managed WLAN is offered at three service levels. Non-Optimized Managed WLAN is offered only at the Full Management service level.

Service features and responsibilities are summarized in the table below:

Division of Responsibilities – Management Levels (Each Level includes all of the items of the previous Level)		
Monitor and Notify (Optimized Service only)	**Physical Management (Optimized Service only)**	**Full Management**
Customer Manages: • Strategic Direction • Fault Isolation • Fault Restoration-Logical • Fault Restoration-Physical • Maintenance-Break/Fix	• Strategic Direction • Fault Restoration-Logical • Change Management-Logical	• Strategic Direction • Security Policy

	• Change Management-Logical • Change Management-Physical • Configuration Back-Up • Security Policy and Patching	• Change Management-Physical • Security Policy and Patching	
Verizon Manages:	• Monitoring • Fault Notification • Performance Reporting	• Monitoring • Fault Isolation • Fault Notification • Fault Restoration-Physical • Maintenance-Break/Fix • Configuration Back-Up • Performance Reporting	• Monitoring • Fault Isolation • Fault Notification • Fault Restoration-Logical • Fault Restoration-Physical • Maintenance-Break/Fix • Change Management-Logical • Change Management-Physical • Configuration Back-Up • Performance Reporting • Security Patching

To enable the flow of data traffic to support Customer's business applications (e.g., email), tunnels will be set up between an access point identified below and another device or infrastructure identified below:

Access Point or Service Node	Device or Infrastructure	Enables Flow of Traffic to:
Aruba Instant Access Point (IAP)	Virtual Wireless LAN Controller	Customer's wireless applications
Lightweight Access Point (LAP)	Wireless LAN Controller	Customer's wireless applications
Cloud-Controlled Access Point (CCAP)	Cloud Infrastructure*	Customer's wireless applications
Software Defined Wireless LAN (SD WLAN)	Cloud Infrastructure*	Customer's wireless applications
* The Cloud Infrastructure is maintained in a redundant fashion, with multiple data centers backing up each other. Failover Cloud Infrastructure instances run in stand-by mode and activate if primary Cloud Infrastructure instances fail.		

1.2.1 **Monitor and Notify Service Level.** The most basic level of Managed WLAN is Monitor and Notify, under which Verizon, provides the capabilities described below:

1.2.1.1 **Monitoring.** Verizon proactively monitors all Managed Device designated by Customer up to the local area network (LAN) interface 24 hours a day, seven days a week.

1.2.1.2 **Notification.** Verizon will create a trouble ticket and send a notification to Customer's designated point of contact within 15 minutes of Verizon's determination of a Managed Device or transport failure. Upon the creation of a trouble ticket, Verizon will (a) troubleshoot the transport service until the problem has been verified as fixed and the ticket will then be closed, if the trouble is due to a Verizon transport service; or (b) inform Customer of the fault and monitor the ticket if the trouble is due to causes other than a Verizon transport service.

Page 2 of 10   335959_12
                       Page 2 of 9   335959_121

1.2.1.3 **Managed Services Customer Portal.** Verizon will provide a managed services portal on the Verizon Enterprise Center (VEC) (www.verizon.com/business/service_guide/www.verizonenterprise.com or other website provided by Verizon from time to time). The VEC provides a consolidated view of Customer Network information 24 hours a day, seven days a week and real time access to project status, contact information, and information about Managed Devices. The Cloud-Controlled Routing (CCR portal (Web Portal) is separate from the VEC, but is accessed via the VEC. Several portal permissions are generally available for the VEC, however, currently, only one Web Portal permission is available per VEC user. The Software Defined Wireless LAN (SD WLAN) portal (SD WLAN Portal) is available at

1.2.1.41.2.1.3 https://verizon.mist.com/ or another URL provided by Verizon from time to time.

1.2.1.51.2.1.4 **Managed WLAN Reporting.** This feature provides Customer with comprehensive daily and ad hoc reporting to quickly assess the health and performance of Managed WLAN, and may include – depending upon the type of reporting received (see below) – any of the following: daily uptime reports, daily managed device summary reports, daily inventory reports, daily new rogue reports, configuration audit reports, and wireless net usage reports.
- Managed WLAN reporting is available on the VEC.
- Managed WLAN reporting for Customers using the CCAP is available in the Web Portal.
- Managed WLAN Reporting for the SD WLAN feature is available in the SD WLAN Portal.

1.2.1.61.2.1.5 **Web Portal and SD WLAN Portal Administrative Access.** Monitor and Notify Management CCAP and SD WLAN Customers have write administrative access to logically manage their Managed Devices.

1.2.2 **Physical Management Service Level.** Customer can choose Physical Management which contains the capabilities of Monitor and Notify plus additional capabilities described below:

1.2.2.1 **Design Services.** Verizon will create a Customer design document (CDD) based on a written statement of requirements (SOR) agreed to by Customer. Software or CPE upgrades that may require Customer investment will be included in the SOR, particularly if such upgrades are required to address Customer's requirements for particular functionality. Customer will purchase any required CPE pursuant to a separate Order. Verizon will activate, monitor, and manage the Managed Devices as designed in the CDD.

1.2.2.2 **Monitoring and Management.** Verizon provides physical fault detection, isolation, and monitoring services for Managed Device, 24 hours per day, seven days per week. Verizon will resolve physical faults whether caused by Verizon, Customer, or third-party issues. Managed Device logical faults are Customer's responsibility. Customer will inform Verizon of physical faults once it has completed its logical troubleshooting if Verizon is maintenance provider for Customer's Device.

1.2.2.3 **CCAP and SD WLAN Network Image.** For CCAP and SD WLAN, a live image of Customer's network is stored on the Cloud Infrastructure. A roll-back to previous configurations is not supported.

1.2.3 **Full Management.** Customer can choose Full Management, which contains the capabilities of Physical Management plus additional capabilities described below:

1.2.3.1 **Monitoring and Management.** Verizon will resolve both logical and physical issues, with Customer's cooperation, either remotely or by dispatching a technician, whether caused by Verizon, Customer or a third party.

1.2.3.2 **Change Management Activities.** Verizon will perform the Standard Change Management activities shown in the Customer Portal at no additional Charge. Optional Change Management activities will be performed at the rates shown below.

1.2.3.3 **Managed Device Software Release Management**
- **Installation.** Verizon will provide relevant software patches and updates as provided by the Managed Device manufacturer from time to time for installation during a fixed update time period, mutually scheduled by the parties. Warranties on software updates, if available, will be provided directly by the Managed Device manufacturer to the Customer.
- **Testing.** At Customer's request, Verizon will make commercially reasonable efforts to make available the resources of Verizon's Customer Test Center (CTC) for the purpose of testing Managed Device manufacturer software prior to the implementation of such software. Verizon's ability to control the implementation of any new Managed Device manufacturer software release may be limited by rules established by the Managed Device manufacturer software. CTC testing may be subject to additional fees and result in delay of the software deployment.

1.2.4 **Implementation Options.** Managed WLAN offers two implementation options to bring devices under Verizon management – Managed Implementation and Managed Take Over. With Managed Implementation Verizon provides support for the planning, system engineering, and overall project management of a new network. With Managed Takeover, Verizon reviews, optimizes, and takes over management of a Customer's existing WLAN data network. Both are subject to an SOR to be agreed upon by the Parties.

1.2.5 **Web Portal and SD WLAN Portal Administrative Access.** Full Management level CCAP and SD WLAN Customers have read-only administrative access in the respective portals.

1.3 Optional Service Features

1.3.1 **Network Engineering (NE) Service (for larger Customer Networks, i.e., those with 20+ Managed Devices under Full Management).** With NE, Verizon provides additional reporting, analysis, engineering planning, design, and change-management support services.

1.3.2 **Guest Access.** Verizon offers three options per IAP, LAP, CCAP, or SD WLAN as applicable, to enable Customer's guests to obtain wireless access to Customer's network (Guest Access): a) Cisco Meraki, with additional information available at the Web Portal; (b) Mist Systems, with additional information available at https://verizon.mist.com/ or other URL provided by Verizon from time to time (the SDWLAN Portal) and (c) Purple WiFi, with additional information available at https://purpleportal.net or other URL provided by Verizon from time to time (the Guest Access Portal). These Guest Access options provide the following functionality:
- **Mobile Location Analytics (MLA).** This feature enables Customer to choose to, entirely at its discretion and control (a) capture information broadcast by the wireless devices of guests and end users (collectively, referred to as MLA Data); and (b) use MLA Data for the protection of Customer's Network and marketing purposes, subject to applicable laws and regulation.
- **Content Filtering (Purple WiFi only).** Customer can block inappropriate content by requesting either a specific category of websites to be blocked or the specific websites. Customer also has the option to limit traffic via bandwidth controls.

1.3.3 **Wireless Assessment.** Customer may request a wireless site assessment via a separate Professional Services engagement with Verizon or provide a completed wireless assessment from a third party agreed to by Verizon. The wireless site assessment determines the wireless requirements, suitable locations for the Managed Devices, and identifies possible interference based on the results of a radio frequency (RF) analysis. If Customer opts not to contract for or provide such a wireless assessment, Verizon will deploy and monitor the WLAN based upon Customer's requirements, but no SLA will apply to such WLAN.

1.3.4 **Network Discovery.** Network Discovery is provided to Managed Takeover Customers for certain management features as part of the implementation. Otherwise, Customers may order Network Discovery subject to an additional Charge. If Customer orders Network Discovery, Verizon will electronically collect information on CPE connected to Customer's Network.

1.3.5 **Device Management.** To effectively manage the Customer Network, all Customer Sites with CCAP, CCR, Cloud-Controlled Switching (CCS), Cloud-Controlled Camera (CCC), or SD WLAN must be at the same management level.

1.4 **Customer Responsibilities**

1.4.1 **In Band Access.** At all times, Customer shall not add, move or remove devices, licenses or administrators to or from the Web Portal, and must:
- Not modify the administrators that are used for the provisioning and fault monitoring interface with Verizon's systems. Verizon must have write administrative access to Managed Devices for provisioning and management through the Web Portal.
- Be responsible for application of the Verizon-provided SNMP read access community string for all monitored WLAN Controllers, or (with respect to Optimized Service) Virtual Wireless LAN Controllers with IAP Management and the application of Verizon-assigned management IP addresses, as required for Verizon management. Customer will provide Verizon the Simple Network Management Protocol (SNMP) read/write community string to any Managed Device whose configuration it wants Verizon to automatically backup.

1.4.2 **Out of Band (OOB) Access.** Where available, OOB Access is a Managed WLAN service option that can be selected by Customer for Managed WLAN with the Physical Management or Full Management service level. Unless otherwise agreed, Customer will provide OOB Access to each WLAN Controller over a separate PSTN line (Analog OOB) or wireless connection (Wireless OOB). Direct console access connections are used to provide OOB Access to the Managed Devices. Console access works without an actual configuration on the Managed Device. Inline management requires a configured Managed Device. OOB Access is not required for WLAN Controllers with the Monitor and Notify service level. Where Verizon provides OOB Access, Customer will not interfere with it, or use it for any purpose other than enabling OOB management by Verizon. Unless otherwise agreed to by Verizon, disconnecting the OOB Service voids any SLAs provided by Verizon.

For Customer Sites with Verizon's Managed WAN or Secure Gateway RRO (RRO) with two or more circuits, Customer may utilize the Alternate Circuit or Backup Wireless options, where the backup access is used in lieu of either Analog OOB or Wireless OOB for inline management access to the Managed Devices, either connecting into two separate Managed Devices or into a single Managed Device as part of Managed WAN or RRO. Verizon also offers the No OOB option to Customers that do not have any OOB Access or backup access that can be used for management access.

1.4.3 **Authorized Users**. Customer is responsible for all guests' and other end users' use of the Customer's WLAN. Verizon will inform Customer by email when it detects a rogue access point. Customer is responsible for determining whether or not the access point in question is unauthorized.

1.4.4 **Supported CPE.** Except for CCAP or SD WLAN CPE where the minimum maintenance coverage is at least eight hours a day x five days a week with a next business day response time, Managed CPE must be under minimum maintenance coverage of at least seven days per week by 24 hours per day by four hours response time.

1.4.5 **Interference.** Customer will inform Verizon prior to any deployment of industrial, scientific, and/or medical wireless equipment or other equipment that could affect the performance of Managed WLAN.

1.4.6 **Remediation Work.** Verizon will notify Customer if any remediation work is required on the Managed Device, which must be completed by Customer prior to Managed Implementation or Managed Take-over. Customer will also be responsible to ensure Managed Device remains supportable.

1.4.7 **Detected Failures.** Customer will report detected Managed WLAN failures and provide any related information to the appropriate Verizon Customer service contact.

1.4.8 **Guest Access Notice.** Customers utilizing the MLA feature must display a notice, in a conspicuous location proximate to the area where the MLA data is collected, that at a minimum: (a) identifies Customer as the Data Controller (as defined in applicable law); (b) describes the type of personal data collected; (c) describes the purpose(s) for which guests' and end users' personal data is processed; (d) provides a summary of Customer's privacy practices and/or a link to its privacy policy; (e) describes any third parties to which Customer will disclose the personal data of guests and end users and the countries to which such personal data may be transferred; (f) explains how guests and end users can contact the privacy officer or other person who is accountable for the Customer's privacy practices and how to access and/or correct their personal information; (g) explains how such guests and end users can opt out from the collection and processing of their personal data; and (h) notifies guests and end users that their decision not to opt out constitutes consent to the collection, processing, transfer and use of their personal data. Where the guest or end user is located outside of the United States, the opt out requirement in subsections (g) and (h) above will not apply and instead the notice must: (1) include an "opt-in" click box or other mechanism that guests and end users must check or accept prior to gaining access to the MLA feature; and (2) notify guests and end users that their decision to opt-in constitutes express consent to the collection, processing, transfer and use of their personal data in accordance with the terms described in (a) through (f) herein.

2. **SUPPLEMENTAL TERMS**

2.1 **Scope.** Managed WLAN includes coverage for only those items – radios, LAN ports, or interfaces – that are directly connected to Managed Device. With Managed WLAN +, Customer can request a change to the management level (i.e., Monitor and Notify, Physical, Full) for Managed Device by executing a Change Order amendment to its Agreement.

2.2 **Network Discovery.** Customer will provide Verizon with accurate information about proper scope of the Network Discovery, represents that it has all necessary authority to have Verizon undertake the Network Discovery requested under these terms, and will indemnify Verizon and its employees, affiliates and agents against any liability if it does not. Verizon reserves the right to stop or withhold from performing Network Discovery, at its sole discretion. Customer's sole remedy for any failure, inadequacy or other problem of Network Discovery is to request that Verizon re-perform it. Network Discovery is not included within the Managed WLAN SLA.

2.3 **Data Loss.** Neither Verizon nor its vendors are responsible for data or files lost during the performance of Managed WLAN.

2.4 **Restriction on Encryption Functionality in India.** Prior to connecting any encryption equipment to Verizon Facilities in India Customer must obtain prior evaluation and approval from the relevant telecom authority.

2.5 **CPE or Managed Device for End-Use in China, Russia and Venezuela.** Without limiting the foregoing or its obligations to comply with applicable export law, Customer specifically represents that the CPE or Managed Device and related software used in conjunction with any services provided hereunder, including equipment or software that is virtualized or cloud based, will not be used by a military end-user or for a military or any other prohibited end-use, as defined by the US Export Administration Regulations, in China, Russia or Venezuela.

2.6 **Customer Changes After Wireless Assessment.** Changes to Customer Network may affect, Verizon's ability to provide Managed WLAN in whole or in part. Such changes will suspend application of the SLA until a new Wireless Assessment has been done and any necessary adjustments are completed at Customer's expense.

2.7 **Online Content.** With respect to Verizon's provision of optional Guest Access, Customer acknowledges that Verizon does not provide any online content to, or interact with end users or Customer's guests.

2.8 **End User License Requirement.** Customer must cause guests to consent to an end user license agreement (EULA). The EULA must state that guests' Wi-Fi-based activity will be monitored and information from such monitoring will be used for protection of Customer's Network, content filtering, and marketing purposes.

2.9 **Indemnity – Guest Access.** Customer will indemnify and hold Verizon harmless from any claims based on the monitoring, capture, storage, use, or sharing of any data collected via Guest Access, including but not limited to claims by a guest or other end user that it did not provide its consent, that a guest or other end user was under the age of thirteen or was not offered a reasonable opportunity to opt-out of the collection of information as required in Guest Access Notice above.

2.10 **Children's Online Privacy Protection Act (COPPA) (U.S.-only).** Managed WLAN does not provide the tools to obtain the parental consent under the Children's Online Privacy Protection Act (COPPA). To the extent that Customer operates a website or other online service to which COPPA applies, Customer acknowledges that it will comply with COPPA, including, without limitation, providing notice and obtaining parental consent in accordance with COPPA.

2.11 **Network Engineering Services Disclaimer.** Customer is solely responsible for determining the suitability of third-party products and services, and Verizon has no liability related to or arising from Customer's contracting for or use of them, even where recommended by Verizon. This provision does not apply to the work of subcontractors or other agents done on Verizon's behalf.

2.12 **BGP Routing.** Verizon may use border gateway protocol (BGP) routing used to access and monitor the Managed Device.

2.13 **Reports.** All copies of any reports, recommendations, documentation, Customer Portal, Web Portal, SD WLAN Portal or Guest Access Portal printouts, where applicable, or other materials in any media form provided to Customer by Verizon are Verizon Confidential Information.

3. **SERVICE LEVEL AGREEMENT.** The Service Level Agreement (SLA) for Managed WLAN may be found at the following URL. The SLA does not apply if Customer has not provided a wireless site assessment, through Verizon or a third-party, as noted above.

SLA for Optimized Managed and non-Optimized WLAN +:
www.verizon.com/business/service_guide/reg/cp_mwlan_sla.pdf

~~www.verizonenterprise.com/external/service_guide/reg/cp_mwlan_sla.pdf~~
[DCL1]
~~SLA for non-Optimized Managed WLAN:~~
~~www.verizonenterprise.com/external/service_guide/reg/cp_mwlan_sla_legacy.htm~~

~~7.~~4. **FINANCIAL TERMS**

4.1 **Optimized Service.** Customer will pay the charges for WLAN + specified in the Agreement, including those below and at the following URL:
www**.**verizon.com/business/service_guide/reg/applicable_charges_toc.htm

verizon

www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm. Charges below are in U.S. dollars and will be billed in the invoice currency. Monthly Recurring Charges (MRCs) and Non-Recurring Charges (NRCs) are based on management level and size of Managed Device.

7.1~~4.2~~ **Administrative Charges.** The following administrative charges are applicable to Managed WLAN. Additional administrative charges are found in the Agreement (as Ancillary Charges).

Administrative Charge	Charge Instance	NRC
Dispatch Charge	Dispatch/Re-Dispatch	$300.00
Expedite Fee	Upon Customer Request	$1,100.00
After Hours: Installation	Per site	$600.00

7.2~~4.3~~ **Managed Device.** The sizes of Managed Device apply to the corresponding rates shown in the Contract.

7.3~~4.4~~ **Optional Change Management (OCM).** OCM provides additional remote change management support for various Managed WLAN changes as shown below. Customer can order specific OCM activities through the Verizon Customer Portal. The Standard Change Management activities shown in the Customer Portal are included in the MRC for Managed WLAN.

Managed WLAN OCM Charges		
Change	**Change Instance (Charged per device unless noted)**	**NRC**
After Hours: Changes	Per request per Site	$600.00
Implementation (Modify Existing)[1,3]	Change per Managed Device	$50.00
Design (Single Feature/Protocol)[2]	Change per Managed Device	$250.00
Design Plus (Multiple Feature/Protocol)[2]	Change per Managed Device	$400.00
Engineering – 1 Hour[4]	Per request and block of hours, 1 hour block	$300.00
Engineering – 5 Hours[4]	Per request and block of hours, 5 hour block	$1,375.00
Engineering – 10 Hours[4]	Per request and block of hours, 10 hour block	$2,500.00
Engineering – 20 Hours[4]	Per request and block of hours, 20 hour block	$4,500.00
Engineering – 40 Hours[4]	Per request and block of hours, 40 hour block	$8,000.00

1. Implementation is used to modify existing features or protocols including the following: dynamic host configuration protocol (DHCP), IP network address translation, MNSO IP address/subnet mask change, switch VLAN and Backhaul Tunnel.
2. Design and Design Plus is used for requests to evaluate or add single (Design) or multiple (Design Plus) new or changed features, protocols or applications/policies in the Customer Network, including the following: add DHCP, quality of service (QoS), network address translation (NAT) configuration and traffic filter design.
3. Customer may create a new design at one Site by selecting Design/Design Plus to add the new feature(s) or protocol(s) and then replicate the design across other Sites by selecting Implementation for the remaining Sites.
4. Customer may select Engineering Hours and request additional Engineering OCM hours from time to time as needed. Verizon will track the number of hours spent per OCM request against the hours selected and will report remaining hours to Customer upon request.

7.4~~4.5~~ **Additional Charges**

7.4.1~~4.5.1~~ **Changing Level of Service.** If Customer elects to change its Service Management level, the adjusted NRC and MRC will be presented in a Change Order amendment to its Agreement.

© 2019-2021 Verizon. All Rights Reserved.   Page 8 of 10   335959_12
~~© 2019-210 Verizon. All Rights Reserved.   Page 2 of 9   335959_121~~

~~7.4.2~~4.5.2   **IP Addresses.** Verizon may use secondary IP addressing if Customer is using unregistered IP address space. If secondary IP addressing is not available, Customer will pay reasonable costs for a dedicated management domain or an IP proxy hardware solution.

4.6   **Non-Optimized Service.** Customer will pay the charges for non-Optimized Managed WLAN specified in the Agreement. Online pricing for Managed WLAN provided by a Verizon entity organized in the United States is at:
www.verizon.com/business/service_guide/reg/cp_mwlan_legacy_rates_charges.pdf

~~www.verizonenterprise.com/external/service_guide/reg/cp_mwlan_legacy_rates_charges.pdf~~

5.   **DEFINITIONS.** The following definitions apply to Managed WLAN, in addition to those identified in the Master Terms and the administrative Charge definitions at the following URL:
www.verizon.com/business/service_guide/reg/definitions_toc_2017DEC01.htm
~~www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm~~

Term	Definition
Aruba Instant Access Point (IAP)~~:~~	The equipment that transmits and receives the radio signal at a Customer Site.
Cloud-Controlled Access Point (CCAP)	Cloud Infrastructure-controlled equipment that transmits and receives the radio signal at a Customer Site.
Cloud Infrastructure	The Cloud Infrastructure consists of all cloud-hosted elements that are used to provision and manage the architectural aspects of the system comprised of the CCAP or SD WLAN and related equipment; such aspects to include security policies, intrusion prevention signatures, radio frequency management, and quality of service. Internet access services, non-CCAP or SD WLAN equipment at the Customer Site, including the Managed Devices, are not part of the Cloud Infrastructure.
Customer Network	The Managed Device and related network located at a Customer Site.
Dispatch Charge	A charge applied when a Customer service request results in Verizon going on to, or attempting to go on to, a Customer Site.
Managed Device	WLAN equipment managed by Verizon under the terms of this Service Attachment, whether provided by Customer or purchased by Customer from Verizon, including equipment to be managed by Verizon as part of a Managed Takeover, as applicable. Managed Devices include Wireless LAN Controllers, Lightweight Access Points, Aruba Instant Access Points, Cloud-Controlled Access Points, Software Defined Wireless LAN Access Points, and associated accessories, including but not limited to antennas, power injectors, and mount kits, as applicable, installed at a Customer Site by Verizon for Managed WLAN.
Management Information Base (MIB)	A database of information stored by SNMP-compliant Managed Device.
Lightweight Access Point (LAP)	The equipment that transmits and receives the radio signal at a Customer Site.
MLA Data	MLA Data consists of the information transmitted by the wireless devices of guests and other end users, including the geo-location of those devices and the devices' MAC address before the end user logs onto Customer's Network.
SNMP community string	An SNMP community string is a password that allows access to Managed Device MIB statistics.

Software Defined Wireless LAN (SD WLAN)	Cloud Infrastructure-controlled equipment that transmits and receives the radio signal at a Customer Site.
Wireless LAN Controller (WLAN Controller or WLC)~~:~~	The equipment that handles the system-wide functions of Managed WLAN, including but not limited to security policies, intrusion prevention, radio frequency management, and quality of service.