

Service Schedule K – FirstLight Managed Solutions

1. FirstLight Managed Solutions Overview

FirstLight Managed Solutions are managed service offerings that may or may not include hardware, software, and support which may include but is not limited to: the provisioning of network hardware, provisioning of management software, provisioning of security software, monitoring of network devices and software, alerting customers of fault events, providing upgrades (at the discretion of FirstLight) of software, providing engineering support, and professional services set forth on a FirstLight provided Statement of Work (SOW).

2. FirstLight Managed Solutions Definitions

A. Managed Solutions Service

- i. Managed SD-WAN Solution is a software based solution consisting of hardware and software to manage a customer's wide area network and utilize external network connections such as Internet service provided by FirstLight Direct Internet Access (DIA) service(s), 3rd Party Direct Internet Access (DIA) Internet Service(s), MPLS or LTE/5G. The Managed SD-WAN Solution is transport agnostic and allows for connection diversification.

B. FirstLight Cloud Security Service

- i. FirstLight Cloud Security Service is a Cisco powered, cloud-based security platform that provides the first line of defense against threats on the Internet by blocking requests to malicious destinations (domains, IPs, URLs) before a connection is established. It provides protection against threats over all ports and protocols, and can protect Internet access across all network devices, office locations, and roaming users.
- ii. FirstLight Cloud Security Service Software Service Terms through Cisco: For detail on the software service terms, see the following: <https://umbrella.cisco.com/terms>
- iii. FirstLight Cloud Security Service Software License Terms through Cisco: For detail on the software license terms, see the following article: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf

C. Managed Firewall: FirstLight Managed Firewall Solution is maintained, and deployed by FirstLight that leverages FirstLight's Internet and transport services and/or third-party Internet DIA services

D. Managed Wi-Fi: FirstLight Managed Wi-Fi is an 802.11 wireless solution consisting of hardware and software that enables end-user devices (such as, but not limited to: laptops, mobile phones, scanners, VoIP telephones, etc.) to access network resources via 802.11 radios (hereto referred to as access points). These access points are deployed, managed, monitored, and maintained by FirstLight.

E. Managed Access: FirstLight Managed Access is a switching network solution consisting of hardware and software that enables end-user devices and hosts to access network resources via Customer supplied Category 5, 5e, 6, 6a cabling and/or multimode fiber cabling and/or single mode fiber cabling. These switches are deployed, managed, monitored, and maintained by FirstLight.

F. Network Monitoring is defined as a monitoring service of FirstLight's Internet Service via the interface of FirstLight's internet edge router. Enterprise Monitoring is defined as a monitoring service of network infrastructure devices within a Customer's local and/or wide area network, limited by the number of nodes purchased. Features provided for Network or Enterprise monitoring are limited to the feature level purchased:

Feature Levels	Network Monitoring FirstLight IP Network	Enterprise Monitoring Your Entire Network Infrastructure
Level 1:	• Web portal to view network inventory • Dashboard to view capacity and utilization for Internet Service interfaces • Node/port/circuit status • Bandwidth usage statistics per node interface	
Level 2:	• All level 1 features • Alert on device status • Alert on bandwidth usage • Alert on interface errors and drops • Alert on interface status	
Level 3:	• All level 1 and 2 features • Ad-hoc historical reporting • Email scheduled reports • High level network topology map detailing device status	

FirstLight will monitor devices specified in the applicable Service Order and as outlined in the terms stated below, 24 hours a day, seven days a week. FirstLight will perform internet control message protocol ("ICMP") ping operation at intervals determined by FirstLight at the time of onboarding. The ICMP ping operation is performed to determine whether the device runs without fault. FirstLight will monitor the devices through simple network management protocol ("SNMP") trap/polling, or like protocol in order to obtain performance statistics and status of devices.

- 3. Service Terms and Restrictions for Network Monitoring.** To receive Service, the Customer is subject to the following rules and restrictions:
- A.** Network Monitoring is limited to internet services and includes the bandwidth and state of the FirstLight internet edge router interface associated with the Customer's service(s) using SNMP and the state of the path between the Customer CPE device and the internet edge router via an ICMP echo request.
 - B.** Customer must allow ICMP Echo request to their devices and their devices must also respond to the ICMP Echo request.
 - C.** Network Monitoring requires a three (3) interface minimum to be configured on the Customer Service Order, and a minimum 12-month term.
- 4. Service Terms and Restrictions for Enterprise Monitoring.** To receive Service, the Customer is subject to the following rules and restrictions:
- A.** Enterprise Network Monitoring is limited to the following device types unless otherwise noted on the Service Order: routers, ethernet switches, firewalls, 802.11 wireless access points, and controllers.
 - B.** Customer must have SNMPv3 enabled and configured with a read-only community string and is accessible via an on-premise appliance provided by FirstLight. If SNMPv3 is not enabled or accessible by the on-premise appliance the Customer can request additional professional services that are not included as part of this service.
 - C.** Customer must provide FirstLight approved detailed network documentation required to facilitate the Service including, but not limited to, network inventory including model name, serial number, location address, SNMP read only community strings, and other information related to network and security policies as requested by FirstLight.
 - D.** Customer must be willing and able to place a network device on their premises in order to facilitate a virtual private network between the FirstLight monitoring platform and the Customer network.
 - E.** Customers with large numbers of network nodes, may require multiple VPN appliances for redundancy purposes.
 - F.** A FirstLight high-speed Internet connection is recommended for proper transmission of the Service. Customer may choose to use a third-party high-speed internet connection if FirstLight Services are not available. FirstLight is not responsible for the integrity and/or quality of data transmitted across computer networks or telecommunication facilities (including but not limited to the internet) which are not owned, operated, or controlled by FirstLight. Regardless of how the network connections are sourced, Customer is responsible for procuring and maintaining the network connections that connect the Customer's network to the CPE equipment provided by FirstLight in order to facilitate the Service.
 - G.** Enterprise Monitoring requires a 10 Node minimum to be configured on the Customer Service Order, and a minimum 12-month term.
 - H.** FirstLight shall have no liability for failure of equipment hardware or software if the failure is related to actions taken by the Customer. The Customer shall defend, indemnify, and hold FirstLight, its principals, officers, directors, agents, and employees harmless from and against any loss, cost, damage, liability, claims and expenses of any kind arising directly or indirectly from the installation, operation, support of equipment hardware or software, or from the Customer's or any of the Customer's subcontractors' or agents' acts or omissions including, but not limited to, reasonable attorneys' fees and court costs, except to the extent such loss, damage, cost or expense is due to the gross negligence or willful misconduct of FirstLight, its employees or agents.
 - I.** FirstLight will provision, maintain, and manage the Service based on a Managed Solution bundle configuration accepted by the customer in writing prior to the installation.
- 5. Suspension, Termination and Cancellation Charges**
- A.** FirstLight may suspend the Service immediately: (i) if a Customer or end user uses the service in any way that exposes imminent harm to: (a) FirstLight's network or other necessary FirstLight facilities or systems; or (b) FirstLight's ability to provide Services to other customers, and the Customer does not (or fails to cause it's end users to) immediately cease the activity causing harm upon receiving notice from FirstLight of such imminent harm; or (ii) when Customer or End Users are unlawfully using the Services and the Customer does not (or fails to cause it's end users to) immediately cease upon receiving notice of such unlawful use from FirstLight.
 - B.** In the event of suspension under Subsection 3.1 above, FirstLight shall provide the Customer with an opportunity to cure as set forth in the Agreement.
 - C.** Customer will remain responsible for any applicable early termination charges if Customer chooses to terminate Service as a result of FirstLight's discontinuations of service for cause.
- 6. Service Requirements and Restrictions**
- A.** Required supporting documentation to be submitted with Customer-acknowledged network order.
 - i. Customer contact information that includes valid telephone number and email address.
 - B.** Customer Provided Equipment
 - i. FirstLight will not support, as part of this Agreement, Customer-provided equipment. Support for Customer-provided equipment, including any configuration necessary for that equipment to interface with the Service, will be provided by Customer. Service rendered by FirstLight to provide configuration or material support for Customer-provided equipment will result in a time and material charge at FirstLight's current rate for Time & Materials.
 - ii. For Customer-provided equipment, Customer acknowledges and accepts that there is no guarantee that this equipment or any of the Customer's previously purchased and installed manufacturer-specific software or feature will work with Service.

- iii. All Customer-provided equipment must be in sound working order. Any defective components that impact the proper configuration, testing and operation of the Service FirstLight technician, and must be replaced at the Customer's expense.
 - iv. If, after diagnosing a problem with the Service FirstLight determines that the Customer-provided equipment, hardware or software is the cause of the problem, Customer will be responsible for servicing such equipment, hardware or software.
- C. Physical Plant**
- Customer must provide a well-maintained, cable plant consisting of customer-owned and certified category 5, 5e, 6, 6a cabling, and/or multimode fiber cabling, and/or single-mode fiber cabling. All cables must be terminated with appropriate connectors for the application prior to equipment deployment. Customer must provide all patch cabling between the wall/ceiling/station jack and the end station device(s).
- D. Network Function Virtualization (NFV) Appliance Policies**
- i. Customer must deploy the NFV image to their infrastructure (unless managed by FirstLight directly). FirstLight will not install, manage, or maintain NFV images or image repositories for customer owned/managed infrastructure.
 - ii. Customer must provide FirstLight administrative access to the deployed virtual appliance. FirstLight must have adequate rights within the customer-owned environment to operate, configure, monitor, and maintain the virtual appliance.
 - iii. Customer deploying managed NFV appliances offered by FirstLight are solely responsible for the virtual infrastructure supporting the NFV appliance including, but not limited to, computer hardware and related software, storage hardware and related software, networking hardware and related software, hypervisor software, management software, backup software, etc.
 - iv. FirstLight will not provide any support, as part of this Agreement, for virtualization infrastructure deployed and/or owned by the Customer. This includes services deployed at the Customer's premises, in a colocation facility (including FirstLight's Colocation services) in a cloud service such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, or others.
 - v. If, after diagnosing a problem with the Service FirstLight determines that the customer-provided virtual infrastructure is the cause of the problem, Customer will be responsible for servicing such equipment, hardware or software.
 - vi. Services rendered by FirstLight to provide configuration or material support for Customer-provided virtualization infrastructure will result in a time and material charge at FirstLight's current rate for Time & Materials.
- E. To be eligible for coverage under the provided SLA a managed Wi-Fi site must have:**
- i. A FirstLight Managed Access (or equivalent FirstLight Engineering Services Contract covering equipment supported by FirstLight).
 - ii. An RF site survey completed by FirstLight certifying the deployment prior to implementation.
- F. FirstLight Cloud Security Billing and Usage:**
- FirstLight Cloud Security Billing and Usage is dependent upon the license agreement between FirstLight, Customer, and Cisco. Two license models are available today: Managed Service License Agreement (MSLA) and Term License Agreement.
- 7. The sections below outline the difference in terms for both MSLA and Term license agreements:**
- A. Managed Service License Agreement (MSLA) Terms**
- i. Customer will be initially billed for the requested license amount, per the agreed upon service order, for the first billing period. Customer has the ability to provision additional users at will within the provided portal. Additional users added after the initial billing period will be modified per the following agreement:
 - ii. User Licenses used for fifteen (15) days or less in a given month will not be charged for that month and licenses used for sixteen (16) or more days in a given month will be charged for the entire month (no proration of license fees for proportion of month used).
 - iii. FirstLight will audit this usage on a quarterly basis for all customers.
 - iv. Customer will only be billed forward for usage.
- B. Term License Agreement Terms**
- i. Customer will be initially billed for the requested license amount, per the agreed upon service order, for the first billing period. Customer will need to request a change order from their FirstLight sales representative if additional users are required.
- C. Verification**
- i. Upon request from FirstLight, Customer will make information available to FirstLight to facilitate verification of the number of licenses that the customer has installed, deployed, or activated. Customer acknowledges that from time to time FirstLight and/or Cisco may conduct audits with the purpose of monitoring and ensuring compliance by Customer of license usage and payment related thereto, including (but not limited to) data extracts from the electronic records in order to review records related to the usage of the Software and may conduct additional specific audits with the purpose of monitoring and ensuring compliance by the Customer of license usage and payment related thereto. During the term, if FirstLight and/or Cisco reasonably believes and provides evidence that there has been inaccurate accounting of software licenses, FirstLight and/or Cisco will have the right upon ten (10) business days prior written notice to Customer, to perform and audit of Customer's records to obtain the correct number of such licenses. In the event that FirstLight and/or Cisco finds inaccurate accounting of software license usage, Customer agrees to pay for any unreported Software license use within thirty (30) days of such findings. Customer agrees to bear, and/or promptly repay, all costs, fees and expenses, incurred by FirstLight and/or Cisco

in the performance of any audit and/or investigation that discloses any breach of the Program Terms. FirstLight agrees and acknowledges that any such audits may not be conducted more than once during any twelve (12) month period unless such audit indicated inaccurate accounting, in which case FirstLight has the right to perform additional audits to verify compliance. Customer is required to retain records for a period of (1) year following the occurrence of the events reflected in the Records.

8. Device Monitoring and Alerting

- A. For purposes of monitoring the Service quality and diagnosing root cause of Service-impacting issues, FirstLight provides monitoring of all devices deployed as part of the service 24 hours a day, seven days a week.
- B. FirstLight will notify Customer when a Managed Solution(s) is not functioning properly (i.e., a fault event). FirstLight's network operation center ("NOC") will create a trouble ticket and take commercially reasonable measures to promptly notify Customer. The FirstLight NOC will verify, troubleshoot and resolve issues if the issue is related to the FirstLight network and/or provided service(s). If it is determined that the issue is related to a Third-Party Network, it is Customer's responsibility to notify its third party network provider for resolution.

9. Third Party Networks

- A. FirstLight will provide configuration of the devices deployed to support Third-Party networks. Third-Party networks must be operating within the domestic United States. Upon FirstLight's request, Customer must provide a Letter of Authorization to the Third-Party to allow FirstLight to work with the service provider of the Third-Party and provide the Services described herein. FirstLight will not be liable for any issues, installation delays, any degradation or failure of the Service, or any material changes stemming from the Third-Party access or provider.
- B. Letter of Authorization. While providing Service to Customer, FirstLight will possess Customer account information from third parties that Customer contracts in conjunction with the FirstLight Managed Solutions to be managed by FirstLight. Customer grants FirstLight permission to contact such third parties on behalf of Customer when FirstLight requires information from the third parties in order to provision, configure or troubleshoot Customer's network.

10. Installation Service Level

FirstLight and/or its contractors will exercise commercially reasonable efforts to install any FirstLight Managed Solutions on or before the Customer specified Firm Order Commitment date. This Installation Service level may be affected by Customer Orders that contain incorrect or invalid information supplied by Customer or Customer Orders that are altered at Customer's request after submission and acceptance by FirstLight, or by equipment availability from the manufacturer and/or distributor at the time of order.

11. Support Service Level

FirstLight will provide material support and ongoing hardware and software maintenance as part of the Service. These services include Telephone Support, Email support, Incident Response, Change Response, Device Replacement, and Software/Hardware Maintenance. This material support and maintenance is subject to the following schedules:

FirstLight SMB and Enterprise SASE Bundle, Managed Firewall, Managed Wi-Fi and Managed Access Support Service Level Feature Schedule:

Feature						
Support Level	Telephone and email support	Incident Response	Configuration change response	Proactive device monitoring	Device replacement	Software and Hardware Maintenance
Network Assurance	24x7	24x7, 4 hour response	24 hour completion of requested changes	Enhanced Included	8x5, next day	Included

12. Support Service level Warranty

- A. During the term, the managed service described above will meet or exceed the stated service level(s) in any calendar month. Determination of performance shall be calculated by review of all tickets requested by the customer for all service locations within the calendar month. If FirstLight does not meet the stated service level during the calendar month and if the customer meets its obligations under this Agreement, then Customer may be eligible to receive a service credit per the schedule below. In no event shall the total amount of credits issued to Customer per month exceed the monthly recurring charges invoiced to Customer for the affected Service for that month.

FirstLight Foundation SD-WAN Solution, Managed Firewall, Managed Router, Managed Wi-Fi and Managed Access Support Service credit schedule:

Response Time Performance	Credit
85% – 94%	5%
76% – 84.9%	10%
< 76%	20%

- B. Customer must request service credit to receive any of the service credits described above. Customer must notify FirstLight in writing within 30 days from the time Customer becomes eligible to receive a service credit. Failure to comply with this requirement will forfeit customer's right to receive a service credit.
- C. The aggregate maximum amount of service credit to be issued by FirstLight to its customers for failure to meet performance levels that occurs in a single calendar month will not exceed 20%. Notwithstanding the foregoing, In no event shall the total amount of credits issued to Customer per month exceed the monthly recurring charges invoiced to Customer for the affected Service for that single calendar month.
- D. Service Level Credits will be applied only to the service charge that corresponds to the affected location or locations where FirstLight fails to meet performance levels.

13. Customer Representations and Warranties

In addition to the representations and warranties as set forth in the Agreement, Customer acknowledges that the Service governed by the Agreement is subject to U.S. export laws and regulations and that any use or transfer of the Service must be authorized under those laws and regulations. Further, use of the Service outside of the U.S. may subject Customer and/or Customer's End Users to export or import regulations in other countries. Without limiting the foregoing, goods, software or technical data related to the Service are prohibited for export or re-export to Cuba, Iran, Sudan, North Korea, Syria or foreign nationals thereof, or any other country that is subject to U.S. economic sanctions or comprehensive export controls restricting such export or re-export, as well as to persons or entities barred from engaging in export transactions by the U.S. Departments of Commerce, State or Treasury. Customer represents and warrants that it will comply with such export controls set forth above. Customer is responsible for notifying its End Users of such restrictions and agrees to be responsible for End Users' use. Customer will not use, distribute, transfer or transmit, directly or indirectly, information or any immediate product (including processes and services) utilizing the Service, except in compliance with U.S. export laws and regulations.

14. Ownership; Customer Data

By using the Service, Customer understands and agrees that data is being collected on the devices that connect to the Customer's Network and how that Network is being used, including the types of data described below. By means of the Hardware, Customer is then transferring that data to FirstLight and its partners for processing and storage, including data that may contain personally identifiable information from the Customer's Network Users (collectively, "Customer Data"). FirstLight and its partners may process and store Customer Data. The Service includes functionality that limits or restricts the types of information collected, and Customer may make use of that functionality. Customer retains all right, title and interest in and to Customer Data, however FirstLight and its partners are permitted to use Customer Data as reasonably required to provide the Service(s) and, only to the extent necessary, to protect FirstLight's rights in any dispute with Customer or as required by law. It is Customer's responsibility to provide notice to, and obtain any necessary consent from, their Network Users regarding collection, processing, transfer and storage of Customer Data.

- A. Traffic Information - information about devices that connect to the Customer Network, such as MAC address, device name, device type, operating system, geolocation information, and information transmitted by devices when attempting to access or download data or content (e.g., hostnames, protocols, port numbers, and IP addresses) via the Customer Network. We process and store Traffic Information on Customer's behalf so they can monitor the use and performance of their Network and exercise control (such as network traffic shaping) over the traffic on your Network.
- B. Location Analytics- Customer collects the MAC address and relative signal strength of Wi-Fi-enabled devices that are within range of Customer's wireless Network. FirstLight and its Partner's do not store these MAC addresses on its servers, except in a de-identified form, and they are not stored on Customer's Hardware. Customer is responsible for whether and how they configure the API to transfer this data to non-FirstLight/FirstLight Partner servers/services and what happens to this data following such a transfer.

15. Disclaimers and Limitation of Liability

In addition to the limitation of liability as set forth in the Agreement, FirstLight disclaims any and all liability arising out of the delivery, installation, support or use of any software. FirstLight assumes no obligation to correct errors in any software. Customer understands and accepts all responsibility for any software meeting customer's requirements or expectations.

16. Service and Support

- A. Managed Solutions Service and Support
 - i. After Managed Solutions Service activation, the Customer will be required to contact FirstLight's Network Operations Center to request moves, adds, changes (MACs) to the Service. Only the/an authorized Customer representatives may request changes to the FirstLight Service.
 - ii. support is provided based on the agreed upon Service Level Agreement (SLA).
- B. Managed Solutions Administration
 - i. FirstLight will have Managed Service Provider (MSP) privileges for hardware and software delivered under the Service.
 - ii. Customer Managed Solution Administration
 - a) FirstLight can grant the Customer with limited administrator privileges, upon request, for the purpose of self-administering Managed Solutions such as, Managed Firewall, Managed Access, Managed Wi-Fi, and SD-WAN. FirstLight shall have no liability for failure to provide the Service if the failure is related to actions taken by the Customer. The Customer shall defend, indemnify, and hold FirstLight, its principals, officers, directors, agents, and employees harmless from and against any loss, cost, damage, liability, claims and expenses of any kind arising directly or indirectly from the installation, operation, support, or from the Customer's or any of the Customer's subcontractors' or agents' acts or omissions including, but not limited to, reasonable attorneys' fees and court costs, except to the extent such loss, damage, cost or expense is due to the gross negligence or willful misconduct of FirstLight, its employees or agents.

- b) The Customer administrators and users are responsible for the security of all user ID and password information. This agreement applies to all IDs and passwords associated with the Managed Solutions account. By enrolling for and using the Managed Services, the Customer accepts sole responsibility for the security and confidentiality of all passwords, including immediately updating temporary passwords sent to users via email for their initial portal login.
- c) Accidental or unauthorized disclosure of passwords or user ID or inappropriate use may have serious consequences and FirstLight shall have no liability for failure to securely maintain this information. Additionally, the Customer remains responsible for the use of each of its accounts, whether used under any name or by any person, and for ensuring full compliance with this Agreement by all users of the account. In the event of a breach of security through the Customer's account, Customer shall immediately contact FirstLight.
- d) Only authorized customer contacts can request changes to the Managed Solutions that cannot be performed via the portal. Note that certain remote changes may require a reboot of the device to take effect.

17. Proof of Performance

- A. FirstLight will consider the solution fully installed and in production when all Equipment and Services are activated and operational. The solution(s) is(are) considered to be operational when the following criteria are met:
 - i. All equipment has been installed
 - ii. Devices installed for internet routing can successfully communicate to the internet via ICMP ping request(s) to a public IP address.
 - iii. Firewalls installed for internet routing can successfully communicate to the internet via ICMP ping request(s) to a public IP address.
 - iv. Devices installed for WAN routing can successfully communicate to each other over the internet via ICMP ping request(s) using their outside interfaces.
 - v. End devices, connected to the ethernet switch network, can communicate to the primary internet or layer 3 network gateway IP address via ICMP echo requests.
 - vi. All installed devices (switches, wireless access points, routers, etc.) are shown as available in the management dashboard.
 - vii. Requested SSIDs are broadcasting and connected devices can successfully communicate upon connecting to the provisioned SSIDs.

Upon fulfilling these conditions, FirstLight shall consider the solution fully installed and operational and will begin billing. FirstLight will issue a completion notice upon successful testing of the above conditions.