LUMEN

Lumen Service Guide

Lumen SASE Solutions

Updated: April 23, 2024

"Lumen" is defined for purposes of this Lumen SASE Solutions Service Guide ("Service Guide") as CenturyLink Communications, LLC d/b/a Lumen Technologies Group or its affiliated entities providing Services subject to this Service Guide. Terms used but not defined in this Service Guide will have the meaning set forth in the Agreement. This Service Guide is subject to change. This Service Guide sets forth a description of Lumen SASE Solutions Service ("SASE Service" or the "Service") offered by Lumen, including technical details and additional requirements or terms. The specific details of the Service ordered by Customer will be set forth on the relevant Order. SASE Service may depend on location and type of connectivity purchased by Customer.

1. Service Description.

Lumen SASE Service is a portfolio of WAN and security solutions: Software Defined WAN (SDWAN), Security as Next Generation Firewall (NGFW), Secure Web Gateway (SWG), and Remote Access/Zero Trust Network Access (ZTNA). Lumen SASE is offered in conjunction with SASE partners which may be designated as "Lumen SASE with Fortinet" or "Lumen SASE with VMware" or "Lumen SASE with Versa". SASE Services can be deployed at a Customer premises, Customer edge location or in a cloud environment. Lumen supports SASE Services using Lumen provided and managed diverse network infrastructure or diverse cloud infrastructure and a password-protected Lumen management portal. Through the Lumen management portal Customer will also have access to the Lumen partner portal(s). SASE Service is offered as a Self-Managed or Pro-Managed service.

The specific SASE Service features differ based on Customer's chosen SASE partner. See Section 3 for specific service descriptions for each partner.

1.1 SDWAN Service allows Customer to securely route traffic over its various network connections between Customer's branch locations and to the internet based on configurations developed by Lumen and Customer.

1.2 Next Generation Firewall (NGFW). Firewall provides monitoring of Customer's web and file transactions using a unified threat management (UTM) software installed by Lumen within a device or cloud instance. Firewall uses template-based firewall configurations to filter inbound and outbound traffic. The Firewall feature also gives Customer the ability to create security logs that provide reports of corporate web activity and malicious content blocked. Security logs are only retained for a limited period of time and Lumen has no obligation to store or provide log data to Customer. Firewall features may include, but are not limited to Intrusion Detection and Prevention (IDS/IPS); Application awareness and control; URL content filtering; and Data Loss Prevention (DLP).

1.3 Secure Web Gateway. A secure web gateway protects web surfing endpoints from infection and enforces company security policies. Secure web gateway will include web traffic inspection, malicious code detection, file filtering, application control and policy enforcement. The secure web gateway may also include IPS/IDS and DLP depending on the Lumen SASE partner that is deployed.

1.4 ZTNA and Remote Access. Zero Trust Network Access is an enhanced security control that delivers an identity and context-based approach to access applications or a set of applications. Access is managed by a centralized trust broker that verifies the identity, context, and company policy adherence for the specified endpoint before allowing access and also prohibits lateral movement in the network.

1.5 CPE. Service utilizes software either deployed on a Lumen-provided customer premise equipment ("CPE") appliance at Customer's data center or branch location ("SASE Device"). The CPE associated with SASE is provided on a rental basis as ("Rental CPE").

1.6 Lumen Hosted Gateway. Service utilizes software deployed in Lumen-provided cloud-based resources and will include one SDWAN instance and one NGFW or SWG instance. Customer may choose from multiple Lumen Hosted Gateway sizes based on the performance and data throughput requirements. Hosted Gateway is currently only available in the US.

2. Roles and Responsibilities for SASE Services.

2.1 Connectivity. Network connectivity is required to utilize SASE Service. Customer may purchase Lumen provided connectivity or Customer may provide their own connectivity. If Customer elects to purchase Lumen provided connectivity, Customer understands that is contracted separately.

2.2 Administration. Lumen will manage and provide administration to all SASE Services for the Customer with Single Sign on (SSO) to Lumen and partner portals and multi-factor (MFA) authentication when available. After the first administrator is created, Customer will be responsible for maintaining what Customer users have access to Services. For configuration consistency and accountability, all system administration and passwords will be managed by Lumen. Lumen will not provide direct access to partner portals and Customer must use single sign on (SSO) methods to the Lumen management portal to access partner portals.

2.3 Reporting. Reporting will be available and limited to what reporting functions are included in the partner portals. Dashboard and reporting may vary based on the partner and the Services ordered.

2.4 Updates. Lumen may periodically require the update of software, hardware, or other components of the SASE Service to maintain the latest supported version of the partner services. If Lumen determines an update is necessary and has successfully completed testing, Lumen will notify Customer and require Customer to plan a self service update or schedule an update with Lumen, depending on the Customer's service level. If Customer has not made the update or scheduled with Lumen within 15 business days of notice from Lumen, Customer will be ineligible for SLA credits as defined in the SLA for SASE Services. If Lumen determines that an emergency update is required, Lumen will make a reasonable attempt to contact the Customer's technial contact prior to deploying the service update.

2.5 Backup and Storage. Lumen will backup and store off-site the latest running configuration for Lumen SASE SDWAN and Next Generation Firewall services for the period of time in which the Customer maintains Services with Lumen.

2.6 Customer Responsibilities. Customer is responsible for any tasks not designated as Lumen provided tasks in this Service Guide. Customer acknowledges and agrees that its failure to perform its obligations set forth in this Service Guide or elsewhere in the Agreement and Service Schedule may result in Lumen's inability to perform the Services and Lumen will not be liable for any failure to perform in the event of Customer's failure. Lumen assumes no responsibility whatsoever for any damage to, loss, corruption or destruction of, or unauthorized disclosure of any Customer's hardware, software, files, data, information or peripherals, including andy damages or losses which may result from Customer's use of Service or Customer's errors or omissions as noted in this Service Guide.

2.7 Network Topology or Physical Changes. The Customer must notify Lumen in advance of any network topology or physical network changes that may affect the Service or the effectiveness of the agreed policies. Failure to notify Lumen of these changes may result in the inability for Lumen to perform its obligations.

2.8 Additional Requirements.

2.8.1 Neither Customer nor it representatives will attempt in any way to circumvent or otherwise interfere with any security precautions or measures of Lumen relating to the Service or any other Lumen equipment.

2.8.2 Customer acknowledges and agrees that is solely responsible for ensuring all Customer-owned devices, software and hardware are updated to meet Lumen SASE partner configurations.

2.8.3 If any configuration, version, or component of the Service is identified as either unsupported or no longer available by a Lumen SASE partner, then Lumen will notify Customer. Customer may be required to sign a new Service Order to ensure the impacted Services are updated or migrated to a supportable version. The new Service Order may require a new Service Term and/or a change in pricing. If Customer remains with the unsupported or unavailable Services, Customer acknowledges the Services are subject to all of the following conditions and/or requirements: (i) Customer's service will be provided on a best efforts basis and ineligible for any SLA credits; (ii) Lumen, in its resonable discretion may elect to charge the Customer for any support or additional task/work incurred by Lumen resulting from the Customer's continued use of the unsupported configuration until Customer obtains the required and supported updates from Lumen or the partner. Customer's failure to do so may result in Lumen's inability to provide the Services and Lumen will have no liability therefrom.

2.8.4 Customer consents to Lumen's and its affiliates or subcontractors' use and transfer to the United States, or other countries information (including Customer Contact information such as names, phone numbers, addresses and/or e-mail addresses) of the Customer for the sole purpose of: (i) fulfilling its obligations under this Agreement; and (ii) providing information to Customer about Lumen's products and services. Customer represents that it will ensure that all information provided to Lumen is accurate at all times and that any business contact has consented to Lumen's processing of such information for the purposes identified in this Service Guide.

3. Lumen SASE Partners Service Components.

3.1 Lumen SASE with Fortinet. Lumen SASE with Fortinet provides a full SASE solution with the following components. All software licenses sold under Lumen SASE with Fortinet also include FortiCare to provide on-going 24 x 7 support for the platform.

3.1.1 SDWAN is available as a service license with Fortinet and is powered by FortiOS. SDWAN includes key functions including, but not limted to, application identification and control, SD-WAN application based policies, advanced SD-WAN remediation such as forward error correction (FEC) and packet duplication, full mesh and hub and spoke topologies, QoS, advanced routing (IPv4/IPv6), VPN/overlay tunneling, high availability, and additional advanced networking functionality.

3.1.2 Next Generation Firewall (NGFW) is available as a service license with Fortinet and is powered by FortiOS. This Next Generation Firewall ("NGFW") and Unified Threat Management (UTM) includes, but is not limited to, antivirus, anti-malware, web filtering and firewall, intrusion detection and prevention (IDS/IPS), and data loss prevention. Customer may use NGFW to create a secure web gateway.

3.1.3 Rapid Threat Defense (RTD). Rapid Threat Defense is powered by intelligence from Lumen's Black Lotus Labs®. Rapid Threat Defense is an automated threat detection and response capability designed to detect and block threats to enhance Customer's defined SASE firewall policies. Rapid Threat Defense is added to Lumen SASE with Fortinet at no additional charge. It will be enabled by default

when a Customer purchases Lumen SASE with Fortinet and Customer may disable RTD in the SASE Manager. Due to the varying nature of malicious activity, Lumen cannot guarantee that all malicious activities or sites intended to be blocked will be identified, detected and blocked. Customer acknowledges that Lumen is providing Rapid Threat Defense as another security tool for Customer's security program and Lumen is not responsible for the effectiveness of the blocking of all offending sites or malicious activities.

3.1.4 ZTNA and Remote Access is available as FortiClient with EMS. FortiClient provides the ability to configure full Zero Trust Network Access to all users on the network at an application and context level.

3.2 Lumen SASE with VMware. As of March 15, 2024, Lumen SASE with VMware is no longer available for new orders. Lumen SASE with VMware provides a full SASE solution with the following components. All software licenses sold under Lumen SASE with VMware also include a cloud management platform.

3.2.1 SDWAN is available as a service license with VMware. SDWAN includes key functions including, but not limted to, application identification and control, SD-WAN application based policies, advanced SD-WAN remediation such as forward error correction (FEC) and packet duplication, full mesh and hub and spoke topologies, QoS, advanced routing (IPv4/IPv6), VPN/overlay tunneling, high availability, and additional advanced networking functionality.

3.2.2 Secure Web Gateway is available as a service license with VMware offered as VMware Cloud Web Security. It is a cloud-hosted service that protects users and infrastructure accessing internet applications. Cloud Web Security is delivered through a global network of VMware SASE points of presence (PoPs) for optimal access to applications.

3.3 Lumen SASE with Versa. Lumen SASE with Versa provides a full SASE solution with the following components. Lumen supports Lumen SASE with Versa Service using diverse network controllers or diverse cloud infrastructure.

3.3.1 SDWAN is available as a service license with Versa and is powered by Versa VOS. SDWAN includes key functions including, but not limted to, application identification and control, SD-WAN application based policies, advanced SD-WAN remediation such as forward error correction (FEC) and packet duplication, full mesh and hub and spoke topologies, QoS, advanced routing (IPv4/IPv6), VPN/overlay tunneling, high availability, and additional advanced networking functionality.

3.3.2 Next Generation Firewall (NGFW) is available as a service upgrade to SDWAN with Versa and is powered by Versa VOS. This Next Generation Firewall ("NGFW") includes, but is not limited to web filtering, layer 7 application detection, antivirus, and intrusion detection and prevention (IDS/IPS). Customer may use NGFW to create a secure web gateway.

3.3.3 ZTNA and Remote Access is available as Versa Secure Private Access (VSPA). Versa VSPA provides the ability to configure full Zero Trust Network Access to all users on the network at an application and context level.

4. Lumen SASE Service Management Options.

4.1 Administration and Management. The SASE Service is offered as a Self-Managed or Pro-Managed service. Lumen will provide Customer with access credentials to remotely manage the SASE Service through the Management Portal. Within the management portal, Customer may make network configuration changes such as routing and security policies on an as needed basis. Lumen resources are available 24x7 for support. Lumen is not responsible for outages that occur due to Customer changes or configuration. Lumen or its supplier will maintain global administrative access to SASE Service at all times and will maintain the root password for all functions. Lumen is not responsible for any services, systems, software, or equipment Customer uses with SASE Service which are not provided by Lumen. Lumen will not debug problems on, or configure, any internal or external hosts or networks (examples include, but are not limited to the following: routers, DNS servers, mail servers, WWW servers, and FTP servers). Lumen will not manage Customer's cloud environment. See **Table 1.0** for specific tasks included with each management option.

4.1.1 Pro-Managed service option includes Lumen monitoring and management of the Lumen Managed SASE Platform that is required to support the SASE Services. Pro-Managed service will also include design and implementation and management of the SASE Service for the entire term of the Service. Pro-Managed service does not include security operations center ("SOC") services. Customer is responsible for monitoring the security events or alerts generated by the Service and responding as it deems appropriate. Customer response could include refining its policies. If so, Lumen will implement Customer requested policy changes. Lumen will only monitor and respond to alarms listed in the Alarm Guide.

4.1.2 Self-Managed service option includes Lumen monitoring and management of the Lumen Managed SASE Platform that is required to support the SASE Services. Customer may purchase additional add-on services from Lumen to support design, implementation, and management of their SASE Services.

4.1.3 "Lumen Managed SASE Platform" is defined as the infrastructure, management platform, and portals to support the SASE Services. Examples of Lumen Managed SASE Platform components include: FortiManager, FortiAnalyzer, FortiEMS, VMware Cloud Orchestrator (VCO), and Versa Director, Controller, Analytics (DCA). Individual Customer managed devices or SASE software running on any Customer or end user device are not part of the Lumen Managed SASE Platform.

4.2 Service Support Service Summary.

The following table illustrates the tasks Lumen will perform depending on the management option selected by Customer. If a task is designated with an "x" as provided by Lumen, it is not the Customer's responsibility. If a task is not designated with an "x", then it is a Customer Responsibility.

Table 1.0 - Service Support Roles and Responsibilities.

Activity	Task	Self-Managed	Pro-Managed
Features / Administration	Provide Customer access to all software and required licenses to support the SASE Services that have been ordered.	X	X
	Establish, manage, and monitor the Lumen Managed SASE Platform components to support the SASE Services that have been ordered.	X	X
	Knowledgebase – documentation and tutorials made available in the Lumen SASE management portal.	X	X
	Customer handbook – standard guidance from Lumen available in the Lumen SASE management portal.	X	X
	Lifecycle management – notification of end of sale/end of support.	X	X
Design and Implementation	Collect network assets information including WAN/LAN details and network topology in coordination with Customer technical detail engineer. Customer must schedule the activity with Lumen technical design team.		X
	Map network assets including WAN/LAN IP information to default configuration.		X
	Customize network profiles and policies for network profiles to include class of service, network address translation, and DHCP. Customer must provide guidance for Lumen engineer to configure in the partner portal.		X
	Customize security profiles to support Customer's rule based security and internet policies for next generation firewall, secure web gateway, zero trust network access or remote access. Customer must provide guidance for Lumen engineer to configure in the partner portal.		X
	Custom design site profile, creation of site specific or site type specific design profiles.		X
	Build configuration in partner portal.		X
	Deploy and manage remote access and/or ZTNA client software to Customer's end user devices.	X	X
	Automated Zero Touch Provisioning (ZTP) per site – CPE is pre-configured and shipped to Customer ready to connect to the SASE infrastructure.	X	X
	Test, turn-up, activation per site – Customer must schedule activation for Lumen engineer to remotely support a service activation. Includes validation SASE Service is online, deployment of site configurations, and final testing by the Customer.		X
	High availablilty configuration and activation per site – if ordered, Lumen will configure and support the activation of a high availability design to include a total of 2 CPE or VMs acting in a redundant pair.		X
	Documentation and knowledge transfer made available through the Lumen SASE management portal.	X	X
	Standard project plan to include the product lifecyle for the standard service implementation.		X
Portal /Reporting	Provide Customer access to the management portal for configuring SASE Services.	X	X
	Access to partner portals – provide access to the partner portal via SSO methods. Customer can access the partner portals through the Lumen SASE management portal. By default Customer will receive read-write access for Self-Managed service option and read-only access for Pro-Managed service option. Customer can request read-write access as desired.	X	X

	Assist Customer with allocating SASE Services to service locations in the Lumen SASE management portal.		X
Monitoring and Alerts	Monitor device status (Up/Down) – proactive monitoring of device software status and interface status for WAN/LAN.		X
	Support for configuring Customer access standard logs, reports of security events, environment, and routing events.		X
	Support for configuring access to standard dashboards for health and availability status (up/down state) and service and links (logical interfaces) for: device, WAN, ICMP, SNMP traps, syslog.		X
Incident Response	Support for an unplanned interruption or reduction in quality to the SASE Node and Lumen Managed SASE Platform. Includes troubleshooting, fault detection, isolation diagnosis for configuration, policy issues, network integration interoperability, portal visibility, service repair and product clarification issues. For remote access and/or ZTNA service, Lumen will only troubleshoot and work to repair the management portal supporting the service. End user devices such as desktops, laptops, and mobile devices are not included.		X
	CPE break/fix (RMA) – warranty support for failed devices and processing the return material authorization (RMA) replacement requests with the support services team.	X	X
Change Management	Change management for Customer network and/or security profiles and policies – limited to 5 Customer level changes per month for Lumen Pro-Managed. For remote access and/or ZTNA service, configuration changes are limited to Customer policies in the management portal. Individual user devices configuration is not included.		X
	Configuration management – Backup of existing configuration. Storage of most recent running configuration for rollback/disaster recovery purposes.	X	X
	Configuration management – Restore of existing configuration. Support for restoration of latest running configuration.		X
	Software patch management – support of periodic software upgrades to support new features and lifecycle code version control.		X
	Capacity management – review and revision of bandwidth and performance policies to manage and improve Service.		X
	Security signature updates – configure the update of security threats on a regular interval.	X	X

4.3 SASE Optional Service Support – Roles and Responsibilities. Customer may purchase additional service options to include, but not limited to: Design and Implementation (per location), On-Site Installation (per location), and Technical Services (per task), where available. The tasks Lumen will perform for each optional service are listed in the tables below.

4.3.1 Design and Implementation Option. Can be purchased on a per location basis for Customers that have selected the Self-Managed service option. Includes Lumen support for design and implementation steps as listed in the table below.

Activity	Task
Design / Implementation (per location)	Collect network assets information including WAN/LAN details and network topology in coordination with Customer technical detail engineer. Customer must schedule the activity with Lumen technical design team.
	Map network assets including WAN/LAN IP information to default configuration.
	Customize network profiles and policies for network profiles to include class of service, network address translation, and DHCP. Customer must provide guidance for Lumen engineer to configure in the partner portal.
	Customize security profiles to support Customer's rule based security and internet policies for next generation firewall, secure web gateway, or zero trust network access and remote access. Customer must provide guidance for Lumen engineer to configure in the partner portal.
	Custom design site profile, creation of site specific or site type specific design profiles.
	Build configuration in partner portal.

	Test, turn-up, activation per site – Customer must schedule activation for Lumen engineer to remotely support a service activation. Includes validation SASE Service is online, site configurations are pushed, and final testing by Customer.
	High availablilty configuration and activation per site – if ordered, Lumen will configure and support the activation of a high availability design to include a total of 2 CPE or VMs acting in a redundant pair.
	Documentation and knowledge transfer made available through the Lumen SASE management portal.
	Standard project plan to include the product lifecyle for the standard service implementation.

4.3.2 On-Site Installation. Self-Managed or Pro-Managed Customers may purchase On-Site Installation on a per location basis, where available. Includes Lumen On-Site Installation services as listed in the table below.

Activity	Task
On Site Installation (per location)	Unpack the CPE device and record the serial number.
	Place the device on Customer provided mounting location.
	Connect and power up the device.
	Connect the Customer's network to the appropriate WAN ports.
	Validate device connects to the SASE management infrastructure.

4.3.3 SASE Technical Services. Can be purchased on a per event basis for customers that have selected the Self-Managed service option. Includes Lumen support for technical support to work through common issues as listed in the table below.

Activity	Task
Technical Service Support (per task)	
	Support for a unplanned interruption or reduction in quality to service the SASE Node and Lumen Managed SASE Platform. Includes troubleshooting, fault detection, isolation diagnosis for configuration, policy issues, network integration interoperability, portal visibility, service repair and product clarification issues. For remote access and/or ZTNA service, Lumen will only troubleshoot and work to repair the management portal supporting the Service. End user devices such as desktops, laptops, and mobile devices are not included.
	One configuration change for Customer network and/or security profiles and policies.
	Configuration management – Backup/Restore of existing configuration. Storage of most recent running configuration for rollback/disaster recovery purposes.
	Software patch management – support of a software upgrade to support new features and lifecycle code version control.

4.4 Service Exclusions. Activites not included as part of SASE Service include, but are not limited to:

- Configuration, installation, or troubleshooting of Customer equipment to include, but not limited to: routers, switches, power equipment, access points, cameras, servers, desktops, mobile devices, printers, and any other equipment that is not part of the Service.
- Monitor and alerts of Customer end user client devices, such as desktops, laptops, and mobile devices.
- SOC services (Ex., Lumen will not resolve or recommend resolution strategies for security events.)
- Accessing or troubleshooting any ***third-party*** hardware, software, or network and circuits.
- For On-Site Installation, any additional wiring, cabling, installation or maintenance of racks or shelves, or any additional hardware such as bolts/screws or connectors that is not included in the On-Site Installation service. Installations with fiber connections include 3 meter fibers. Longer fibers lengths will need to be sourced by Customer.
- For On-Site Installation, troubleshooting or installing the wiring for connectivity to demarcation points unless separately ordered from Lumen and covered by the terms and condition of that Service.
- Optimizing or troubleshooting Customer applications that are not listed in the ordered Service.
- Configuration or design changes during a scheduled activation that extend beyond the scheduled activation time interval for the Services ordered.
- Installation or configuration changes that are results of site additions, deletions, re-locations or changes in Customer's network strategy or design requirements that deviate from the agreed upon design.
- Additional SASE partner products and services that are not listed on the Order are not included. Examples include, but are not limited to: MFA tokens, Sandboxing, Network DLP, SIEM or Managed SIEM, and Remote Browser Isolation.
- Management and renewal of Customer security certificates (SSL certificates).