Lumen® SD-WAN with Versa Networks

Versa Secure Access service

General disclaimer

Although Lumen has attempted to provide accurate information in this guide, Lumen does not warrant or guarantee the accuracy of the information provided herein. Lumen may change the programs or products mentioned at any time without prior notice. Mention of non-Lumen products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED “AS IS,” WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. LUMEN AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

LUMEN AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY LUMEN PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF LUMEN OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any internet protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the Lumen products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by Lumen with any Lumen product, or to create any new or additional warranties or licenses.

Overview

As we set up your Lumen SD-WAN with Versa Networks Secure Access (VSA) service, this guide helps you to follow the process step by step and to know where we'll need your help.

Lumen supports the initial configuration of the Versa SD-WAN and Versa Secure Access service, along with monitoring and managing events associated with the SD-WAN appliance, circuit availability and connectivity to the Versa Secure Access Service (SASE) gateway.

NOTE: You need to have at least 2 active SD-WAN locations before the Versa Secure Access service can be enabled. However, the onboarding process can be started in parallel to the activation of the SD-WAN service, once Lumen receives a signed SOW.

Service description

The Versa Secure Access service (VSA) is a cloud-managed cloud-delivered solution connecting remote users to distributed applications across private cloud, enterprise data centers and public cloud without compromising on security or user experience. The Secure Access Solution consists of:

Cloud Gateways: Globally distributed Points of Presence comprised of Zero Trust Network Architecture (ZTNA) framework and Secure web gateways (collectively called Versa SASE Gateway) provide reliable and secure on-ramps for access to enterprise applications. The ZTNA framework authenticates users, authorizes application access, and secures enterprise network from external threats. Secure Web Gateways (SWG) integrate advanced routing, comprehensive security, and market-leading SD-WAN, with secure access by securely connecting to and integrating with an Enterprise's existing network and datacenter infrastructure.

Desktop Client: A software agent/application that and extends the functionality of a Lumen SD-WAN with Versa networks solution to client devices. The desktop Client creates a secure and encrypted connection from remote devices to the Versa Cloud Gateway. Once authenticated through the Versa SASE framework, users can securely connect to enterprise applications in both the public and private cloud.

Portal: Provides enterprise administrators with the ability to monitor and manage granular visibility of users and applications in a centralized location. The Portal provides real-time and historical reporting at a network, application, and user level. This will be a separate portal than what you are using to view / manage your Lumen SD-WAN with Versa networks service.

Lumen SD-WAN with Versa networks provides you with accelerated network agility, operational efficiency, and enhanced resiliency. When combined with the Versa SASE (Secure Access Service Edge) framework, enterprise customers can integrate SD-WAN, security, routing features in a single platform, with centralized management and monitoring, analytics and reporting, and automation on the WAN Edge

Summary of responsibilities

Your responsibilities

You are responsible for the following:

- Provide necessary data to configure the Versa Secure Access service
- Distribute and download Versa Secure Access client
- Register users
- Test and Accept service

Lumen responsibilities

Lumen is responsible for the following:

- Collect data necessary to configure the Versa Secure Access service
- Configure Versa Secure Access Gateway
- Connect Versa Secure Access Gateway to Customer's SD-WAN network
- Provide customer with link to obtain VSA client
- Provide customer with instructions for registering users / using VSA client
- Provide customer with access to Versa Secure Access portal
- Provide day 2 support of Versa Secure Access service

Get ready

What to expect during the process

1. Once a SOW is signed and returned to Lumen, we will assign your order to a Lumen project manager (PM) to coordinate and communicate the configuration and activation of the Versa Secure Access service. If you ordered Lumen SD-WAN with Versa Networks and Versa Secure Access at the same time, your orders will be managed by the same SD-WAN project manager.

2. The Lumen PM will coordinate a kickoff call to review your SD-WAN network design and collect the data necessary to start the VSA configuration process. The kickoff call will include representatives from both Lumen and Versa. The data that will be collected includes information such as:

    - customer / enterprise name
    - region(s) / countries(s) of end users
    - number of users
    - FQDN / email domain
    - authentication mechanism (local or enterprise AAA)
    - IP address endpoint for site-to-site VPN termination
    - IKE version (v1 / v2) for IPSec backhaul
    - direct internet access (at client / gateway)
    - IP addresses/prefixes and locations
    - number of backhaul S2S IPSec tunnels
    - any restrictions related to the region(s) the users can connect from (e.g., GEO fencing)
    - end user device management methodology and details around it.
    - security policies to be configured on the cloud security gateway (VSA Professional Tier only)

    Because Lumen SD-WAN is a managed service, some of the data to be collected (such as customer / enterprise name / IPSEC / IKE / peering IPs etc.) is already known and will be provided by the Lumen.

3. Once the data has been collected, the Lumen PM works with Versa to configure your VSA service, connect your SD-WAN network to the Versa Secure Access Service Edge (SASE) gateway, and provide access to the Versa Secure Access portal.

    - If using LDAP / SAML for authentication, you are expected to configure users in your local server.

    - If using a local server for authentication, the users will be built for you in the local database as part of the configuration process, as well as the generation of a one-time password (OTP) needed to set up a user account.

4. Once the service has been configured, you can download the Versa Secure Access client and test your service.

5. You have five business days to test your VSA service. Upon acceptance (or five business days), your service delivery will be considered complete.

Activate

Step 1: Create user account (local database users only)

If your end users are configured in a local user database, you will receive an email from Lumen that includes a link to verify your end users and a one-time password (OTP) for each user to set up individual passwords.

After setting the password, user details like first name, last name, email address and other important information present in local user database, the user information is propagated to all the Versa Secure Access Service gateways.

Step 2: Download Versa Secure Access client

After the above step is completed or if you are using LDAP / SAML for authentication, you can download the Versa Secure Access Client (for Windows or MAC) and access the Quick start guide.

Step 3: Complete the registration process

Once the Versa Secure Access client is downloaded and started, you will be prompted to register for the VSA service. Lumen will provide you with the following information required to complete the registration process and log into your Versa Secure Access portal:

- List of configured gateways
- Portal FQDN/IP
- Enterprise Name
- Versa Secure Access Client User ID (**Note:** User ID is only supplied for customers using a location database for authentication. Customers using LDAP / SAML will use the user ID set up / supplied by the network administrator.)
- Versa Secure Access portal credentials

Once the registration and authentication process has been completed, the configuration for the VSA client and user profile is downloaded and automatically configured. Your end user is now ready to use the VSA client.

Step 4: Test and accept the VSA service

Follow these steps to validate that the Versa Secure Access client is working correctly before distributing to your enterprise.

- Confirm Secure Access client is successfully registered for a sample of users.
- Confirm user can select a gateway. **Note:** Versa Secure Access will automatically provide the user the best available gateway by default and won't need to select a gateway unless there are unique circumstances.
- Validate successful enforcement of security policies for sample set of users (Professional tier)
- Sign in to Versa Secure Access portal and validate the following analytics logs are visible:

- authentication events
- end user tunnel events
- portal registration status
- gateway connect status
- user session log

Get help

End users should direct connectivity issues to their corporate contact to troubleshoot the device connectivity and end user profile.

If further assistance is needed, your company admin should create a repair ticket with Lumen for assistance using Control Center or by calling: 877-453-8353, option 1, then 2, then 4, then 2. The ticket should be opened against an SD WAN location that is connected to the Versa Secure Access gateway.

Once a ticket is created, Lumen will troubleshoot the connection between your SD-WAN network and the VSA gateway. If these connections test clean, Lumen will engage Versa for Tier 2 support of the Secure Access service.

It is recommended to execute the diagnostics feature on the VSA client to assist with Lumen / Versa troubleshooting. The diagnostic report can be exported and attached to the Lumen ticket.