Versa SASE Portal Overview

For supported software information, click here.

The Versa SASE portal is a cloud-based, single pane-of-glass portal that allows you configure and manage your SASE deployment. The SASE portal delivers secure and reliable client-to-cloud connectivity. It enables and delivers consistent security policies, network policies, business policies, user policies, and application policies seamlessly between on-premises devices and cloud services.

The SASE portal provides key services:

- Versa Secure Access (VSA)—Securely connect to enterprise-hosted applications using zero-trust principles.
- Secure Web Gateway (SWG)—Securely browse the internet and access internet-based applications.

The SASE portal allows you to configure the following:

- Real-time protection
  - Internet protection rules—Firewall rules that are applied to traffic destined to and received from the internet. Internet protection rules, which are available to enterprises for which the SWG service is enabled, scan traffic and apply policies based on application and URL filtering, user and user group rules, geolocation, traffic filtering by source and destination zones, and IP addresses. The actions you can apply in rules are allow, deny, and reject, and you can apply advanced security profiles such as DNS filtering, file filtering, intrusion protection system (IPS), malware protection, and URL filtering.
  - Private application protection rules—Firewall rules that are applied to traffic bound to applications or destinations in an enterprise private network. Private application protection rules are available to enterprises for which the VSA service enabled. Private application protection rules protect internal applications by restricting which users can and cannot communicate with the applications. These rules match traffic based on private applications, user and user group rules, geolocation, traffic filtering by source and destination zones and IP addresses, and other conditions. The actions you can apply on the rules are allow, deny, and reject, or you can apply advanced security profiles like malware protection and IPS.
- Secure client access—Rules and profiles to manage VSA client applications running on personal computers and mobile phones. These rules and profiles allow you to select gateways, select authentication methods, and perform other tasks.
- TLS decryption—Transport Layer Security (TLS) decryption is an industry-standard protocol that is used to provide a secure communications channel between clients (end devices) and servers (destination sites) over the internet. TLS decryption is available to enterprises for which SWG professional services are enabled.
- Settings—You can configure the following global settings:
  - Certificates—A certificate authority (CA) certificate verifies a digital entity's identity on the internet. CA certificates are an essential part of secure communication. You can use Versa self-signed trusted certificates, or you can upload additional certificates. You use these certificates when you configure profiles and rules.

- Mobile device manager (MDM)—An MDM allows you to administer mobile devices, such as smartphones, tablet computers, and laptops. You create an MDM profile to retrieve device information from a Microsoft Intune server using the device ID and other information, such as a user profile, using a user ID.
- Site-to-site tunnels—You can configure GRE or IPsec tunnels from Versa SASE gateways to your enterprise network (data centers or on-premises routers).
- Users and groups—For each enterprise, you can configure one Lightweight Directory Access Protocol (LDAP) authentication profile, one Security Assertion Markup Language (SAML) authentication profile, or one Versa Directory users and user groups profile.
- User-defined objects—You can define custom objects in the following categories:
  - Address groups
  - Applications
  - Schedules
  - Services

Supported Software Information

Releases 11.1 and later support all content described in this article.

Additional Information

Concerto Home Screen Overview
Configure SASE Certificates
Configure SASE Internet Protection Rules
Configure SASE Private Application Protection Rules
Configure SASE Secure Client Access Rules
Configure SASE Site-to-Site Tunnels
Configure SASE TLS Decryption
Configure SASE User-Defined Objects
Configure Users and Device Authentication
Configure the SASE Mobile Device Manager