Identity Vendor Integration

Unify SSO, SCIM provisioning, directory services, MFA, and certificate-based authentication with inline SASE enforcement.

Key Benefits

- Standards-based identity with SAML SSO, LDAP/AD, SCIM 2.0, and certificates.
- Automated lifecycle and layered authentication for users, groups, devices, and certificates.
- Inline enforcement and audit across SASE policies, logs, and access decisions.

Challenges

Identity is now the control point for access, but identity telemetry is often disconnected from network and security enforcement. Traditional SSO can authenticate a user at login, yet it does not always ensure that user, group, device, and certificate context is continuously reflected in SASE policy. When directory updates, role changes, and risky access conditions are delayed or siloed, organizations face privilege drift, compliance gaps, and increased exposure to compromised credentials.

Solution

VersaONE integrates Identity Providers, directories, and certificate authorities directly to the SASE control plane and enforcement points. Administrators can use SAML/SSO with Microsoft Entra ID and Okta, SCIM 2.0 provisioning with Entra, Okta, and Ping Identity, AD/LDAP for directory-backed users and groups, Versa Directory for local identity, and device or user certificates for cryptographic validation. Versa then applies identity-aware policies across private applications, SaaS, internet access, SD-WAN, NGFW, and cloud security services.

Business Value

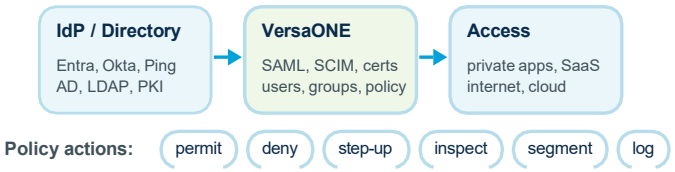
Use Case/ Challenge	1. Identity, SASE, and directory controls are often operated separately. 2. Stale user or group data can allow excessive access after role changes. 3. Credential-only access leaves gaps when users connect from risky devices or shared systems.
Solution	1. Integrate Microsoft Entra ID, Okta, Ping Identity, AD/LDAP, Versa Directory, and PKI with VersaONE SASE. 2. Use SCIM 2.0 to synchronize user and group lifecycle changes into Versa policy. 3. Enforce SAML/SSO, LDAP, MFA, device certificates, and user certificates before granting access.
Benefits	1. Faster onboarding and deprovisioning for users and groups. 2. Consistent identity-based access across private apps, SaaS, internet, and cloud. 3. Stronger Zero Trust enforcement through user, group, device, certificate, and policy context. 4. Audit-ready visibility into identity, provisioning, and access decisions. Technical Solution

Technical Solution

Versa SASE uses authentication profiles, SCIM integration, and identity-aware policy to connect enterprise IAM systems with real-time enforcement. The Versa SASE Gateway can authenticate users through SAML, LDAP/AD, Versa Directory,

device certificates, and user certificates; SCIM keeps users and groups synchronized so access rules reflect current IdP state. For Microsoft environments, Versa also supports API-based integration with Microsoft Entra Internet Access to automate secure connectivity and simplify time to deployment.

Identity-to-SASE Enforcement Loop



Vendor Integration Patterns

Microsoft Entra ID	Okta
SAML SSO, SCIM, and Entra Internet Access Authenticate users with Entra ID, synchronize users and groups through SCIM, and automate secure connectivity to Microsoft Entra Internet Access through API-based workflows.	SAML SSO and SCIM provisioning Use Okta as the SAML identity provider, include group claims in SAML assertions, and provision users and groups to Versa through SCIM 2.0 workflows.
Ping Identity	**AD/LDAP, Versa Directory, and PKI**
SAML-based SCIM provider support Support identity lifecycle automation from SAML-based SCIM providers so user and group changes can be reflected in SASE gateway policy.	Directory, local identity, and certificate trust Authenticate against enterprise directories, use local Versa Directory where needed, and add device or user certificates to validate trusted endpoints and identities.

Key Capabilities

- Identity Provider SSO: SAML-based authentication with Microsoft Entra ID and Okta, including user and group attributes for policy matching.
- SCIM 2.0 Lifecycle Sync: Create, read, update, and delete user and group changes from IdPs into Versa SASE services and gateways.
- Directory-Based Access: AD/LDAP integration validates credentials and retrieves group or role attributes for least-privilege enforcement.
- Layered Certificate Authentication: Device and user certificates can validate trusted endpoints and individual users before SAML or LDAP authentication completes.
- Unified Policy Enforcement: User, group, device, certificate, app, location, and risk context drive consistent rules across ZTNA, SWG, CASB, NGFW, and SD-WAN.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa
Versa, the global leader in unified networking and security, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while providing a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission-critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.

Part# SB_SASE-IDSECURITYCAP-01.0