



SecureSpan™ XML VPN Client

Securely bridge communications between divisions, branch offices, affiliates and third-party services without coding.

The SecureSpan XML VPN Client offers:

Secure X-Domain Communications

Securely bridge identity silos by enforcing client-side authentication and provider-side authorization, while ensuring sensitive identity data remains protected.

Rapid SOA Deployment

Eliminate the need to re-code and re-test client applications when a Web service provider's security, routing, and transaction preferences change.

To learn more about Layer 7 and how it can address your organization's cloud and Web services needs, call 1-800-681-9377 (toll free within North America) or +1.604.681.9377. You can also email us at info@layer7.com; friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at layer7.com, or follow-us on twitter [@layer7](https://twitter.com/layer7).

Centralized organizations with semi-autonomous departments, agencies, and territories, or that want closer ties to arms-length affiliates and contractors can now cost-effectively create a loosely-coupled network of services while ensuring security.

Securing Cross-Domain Communications

As more and more organizations spin off business entities and outsource services to third-party providers, concerns arise over ensuring interactions between these "separate but integral" entities remain secure. But determining exactly who, from which organization has access to which applications and services in each separate security domain can be problematic. While many solutions to this identity bridging problem have been tried over the years, most have proven too expensive in terms of administration and/or infrastructure costs.

The SecureSpan XML VPN Client (XVC) works in conjunction with the SecureSpan XML Firewall or SOA Gateway to effectively overcome the separation of authentication and authorization tasks across trust boundaries, delegating authentication to the service requestor while preserving control over authorization for the provider hosting the service.

In this way, organizations can ensure authorization happens close to the service provider; passwords never leave the source network, and yet identity is preserved for logging and auditing purposes. Avoid the pitfalls inherent in consolidating identity stores or setting up inter-LDAP/Active Directory trust or delegation.

Speeding Deployment

In addition to acting as a near "drop-in" solution to the federated identity problem described above, the XVC also reduces deployment time for client applications. When accessing business services, client applications must conform to the access control and security policies layered onto the service. This typically entails coordinating policy requirements at design-time, coding into the client any modifications or additions required, and then testing and/or debugging the resulting interaction with the service.

The XVC, deployed as either a standalone application on a client system or incorporated into the client-side application itself, automatically negotiates policy-specific security, routing, and transaction preferences with the SecureSpan XML Firewall or SOA Gateway in real time. In this way, the XVC eliminates the need to program the client (or re-program it as industry standards, business policies and government regulations change), automating and speeding the deployment of client-side, XML-based applications.

Key Features	
Trust and Identity Infrastructure	
SAML Support	Interfaces with Security Token Service (STS) via WS-Trust or WS-Federation enabling federated identity deployments.
Built-in Trust Store	Streamlines authentication by storing X.509 certificates issued by the SecureSpan XML Firewall or SOA Gateway onboard Certificate Authority.
Credentialing	Supports client credentials from a broad range of identity sources including LDAP, Active Directory, and X.509 certificate-based Public Key Infrastructure (PKI).
SSO Extensibility	Leverages and extends most popular SSO/access management systems, including CA SiteMinder, IBM Tivoli Access Manager, Novell CentraSite, and Sun OpenSSO.
Management and Administration	
Automatic Policy Negotiation	Automatically coordinates policies with the SecureSpan XML Firewall or SOA Gateway.
System-to-System Interaction Support	No end-user runtime interaction is required. Optionally runs as a service in Microsoft Windows environments.
Delegated Message Decoration	Allows the offloading of message signing, encryption, compression and security decoration from client applications speeding to time deployment by eliminating the need to re-code and re-test.
Form Factors	
Standalone Executable	Supports Linux and Windows platforms.
Hardware	Integrated inside a SecureSpan XML Firewall or SOA Gateway for “drop-in” Web services federation.
Software	Software class library available for custom thick client development.
Supported Standards	
XML, JSON, SOAP, REST, PCI-DSS, AJAX, XPath, XSLT, WSDL, XML Schema, LDAP, SAML, XACML, OAuth, PKCS, POP3, X.509 Certificates, FIPS 140-2, Kerberos, XML Signature, XML Encryption, SSL/TLS, SNMP, SMTP, IMAP4, MQ Series, HTTP/HTTPS, JMS, Tibco EMS, FTP/FTPS, WS-Security, WS-Trust, WS-Federation, WS-SecureExchange, WS-I BSP, WSIL, WS-I, WS-Addressing, WS-SecureConversation, WS-MetadataExchange, WS-Policy, WS-SecurityPolicy, WS-PolicyAttachment, UDDI, WSRR, MTOM, IPv6, WCF	

The SecureSpan XML VPN Client can be deployed in conjunction with all currently shipping versions of Layer 7's SecureSpan and CloudSpan Gateways.

To learn more about Layer 7 call us today at +1 800.681.9377 (toll free within North America) or +1.604.681.9377. You can also email us at info@layer7.com; friend us on [facebook.com/layer7](https://www.facebook.com/layer7); visit us at layer7.com, or follow-us on twitter [@layer7](https://twitter.com/layer7).