



# Stonesoft SSL VPN Appliance Comparison Datasheet

## Premium Security

No direct access to back-end systems: Stonesoft SSL VPN acts as a proxy server between the user and back-end systems.

- Authentication according to your needs

Select your authentication method from multiple alternatives, ranging from One Time Password sent via mobile text message to a plain password or to the new Invisible Token authentication method, where the browser is your token.

Advanced Password Policies enable administrators to restrict how passwords are set and reset, for example, to disallow specific combinations of characters in a password. The most suitable method can be chosen for each resource separately.

- Built-in two-factor authentication: One Time Password via mobile text (SMS), Java clickable Webpad, PIN/Challenge based MobileID free software token, Invisible Token
- Integration with backend external authentication and directory services: LDAP, Active Directory, User Certificate, General RADIUS, SecurID, NTLM, Basic, Extended User Bind, Form Based Authentication, Windows Integrated Login, BankID, BankID Signer, OATH Service, SafeWorld
- Single sign-on for transparent authentication to multiple systems, including Web Applications, Windows File Share, Remote Desktop and legacy applications like SSH or Telnet
- Support for identity federation scenarios based on SAML 2.0 or ADFS as Service Provider and/or Identity Provider
- Granularity in access control Access can be granted to selected applications only. Access can be granted or denied based on:
  - IP address of incoming client
  - Client device
  - Authentication method(s)
  - Date and time restrictions
  - User group memberships

**STONESOFT**

With the Stonesoft SSL VPN solution, you are not limited to application access. File shares and client-server applications can be accessed as well. Stonesoft SSL VPN is a truly secured connection that provides a variety of different VPN protocols and encryption algorithms:

- TLS v 1.0, SSL v 2.0, SSL v 3.0, AES- 128, DES, 3DES, RC2-128, RC4-128

Secured sessions – End-point integrity control & session trace removal

End-point integrity – Prevents the device from being used as a stepping stone into the corporate network.

Inspects the client device (for example, laptop or PDA) before it connects to the corporate network. Real-time scans for continuous integrity checking:

- Firewall and anti-virus software
- Operating system and patches
- Spyware checking
- Device type
- Network configuration
- Windows Center to determine the security status of the client device before allowing access
- Hardware assessment (motherboard, memory and hard disk IDs)

Only approved devices can connect to the VPN tunnel. Non-compliant devices may be refused access or given restricted access, or be referred to software update sites.

Traffic Recording enables you to record any transaction between a user and the target system.

Clean-up – Removes all traces from the end-point on completion of the session:

- Cookies
- URL history
- Cached pages
- Registry entries
- Downloaded components

## Total Mobility

Encrypted Mobile Access over the Internet using any Web-enabled device

- Client and location independent solution
- Adaptive and intuitive application portal
- Full TCP and UDP tunneling using an automatically downloaded (Java or ActiveX) access client
- Single sign-on and identity federation
- Secure ActiveSync for Microsoft calendar and e-mail

## Ease of Management

**Comprehensive, yet unified management with easy-to-use tools for compliance auditing.**  
**Easy-to-use Web-based management:**

- Remote software upgrades
- E-Mail and SMS (text message)
- Alerts
- Easy-to-use Administration Wizards
- Fast and extensive monitoring and reporting through local Web-based interface and Stonesoft Management Center (SMC)
- Log viewing using built-in log browser and SMC ○ Granular audit trail to satisfy demanding compliance requirements

# Stonesoft SSL VPN Appliances for flexible and Secure Remote Access

Stonesoft SSL VPN solution offers a flexible and secure remote access to enterprise information, applications and networking resources. It delivers the secure access cost-effectively by establishing an encrypted VPN tunnel across the Internet. The solution brings network resources as close as the nearest Internet connection, regardless of connectivity media or device.

The Stonesoft SSL VPN solution is ideal for organizations that need to easily provide controlled yet flexible remote access for employees, partners, or customers. The solution enables organizations to fully control the information that can be accessed. Access to different applications can be granted based on user identity, method of login, access location and the security level of the access device. The solution guards the security of the network while providing access from anywhere, at anytime, and with any device.

APPLIANCE SPECIFICATIONS	SSL-1035	SSL-3202
Concurrent users	up to 1000	up to 15 000
Mirrored Configuration for HA	yes	yes
Mobile Two-Factor Authentication	yes	yes
Authentication server	included	included
Pre-authorization and Continuous Assessment	yes	yes
Trace removal	yes	yes
Additional Authentication Methods	+20	+20
Adaptive Web and Legacy Application SSO	yes	yes
Multi-Domain Support	yes	yes
Reporting/Auditing System	yes	yes
Network interfaces	4 x 10/100/1000 Mbps Ethernet Ports	2 x 10/100/1000 Mbps Ethernet Ports
Form Factor	1U rack	2U rack
Redundant Power Supply	-	yes
Dimensions (W x H x D)	(W x H x D) 426 x 44 x 300 mm/ 16.77" x 1.73" x 11.81"	(W x H x D) 437 x 89 x 450 mm/ 17.2" x 3.5" x 17.7"
Module slots	1	3
Optional modules	MOD-EM1-GE-4 MOD-EM1-GE-8 MOD-EM1-GE-SFP-4 MOD-EM1-10G-SFP-2	Quad Port Gigabit Ethernet Copper Module Eight Port Gigabit Ethernet Copper Module Quad Port SFP Gigabit Ethernet Module Dual Port SFP+ 10GB Module