



Succendo[®] SSL VPN

Secure • Versatile • Anywhere

Succendo SSL VPNs deliver on the promise of secure access from anywhere at anytime from notebooks, desktops, PDAs and Smart Phones, thus increasing productivity of your mobile work force, and limiting the information accessible by partners.

- Easy-to-deploy, manage and administer; no change to existing network settings; highly scalable to many users
- No client software to install, maintain or support; only requires a standard Web-browser at the remote client computer
- Provision employees, contractors, suppliers and customers with differing roles and available services
- Fine-grained access control by role, application, protocol, connection time
- Supports all Web-based file sharing services and IP-based applications
- Wide range of access modes provide virtually seamless access to the corporate network
- Customizable login page; user's roles determine the listed available services
- End-user ease-of-use; launches the associated client application upon selecting a service
- Stringent host checks on remote machines ensure uncompromised security of the internal network
- Supports a wide range of authentication protocols: RADIUS, LDAP, AD, PKI
- Supports popular verification methods such as one-time password, dynamic tokens, certificates, RSA SecurID, etc.
- Dynamic access authorization based on user's roles and client security checks enforces security policies
- Detailed logs and monitoring tools for control and audit purposes
- Stateful-failover High-Availability pairing option

	Succendo 502	Succendo 2000	Succendo 5000
Concurrent Users (max)	10-200	100-500	200-2000
Dimension	1U	1U	2U
Communication Ports	4x10/100M	4x10/100M, 2x10/100/1000M	2x10/100M, 4x10/100/1000M
Admin Configuration Port	RS-232, Web, SSH, SNMP		
Liquid Crystal Display (LCD)	No	Yes	Yes
Hardware-accelerated Encryption	No	No	Yes
Storage Capacity	256MB	512MB	1GB
Power Supply	Single Input	Single Input	Dual Input
System Upgrade	Via FTP, HTTP, CLI, Web		
Certifications	Please visit www.o2security.com/product/certifications for the complete list of certifications and awards.		

Succendo SSL VPNs ensure secure, confidential transmission of information over the Internet, permitting access to internal data and resources by remote users from anywhere and from any notebook, desktop, PDA, Smart Phone or kiosk. It is easily deployed in your company's network, and services can be provisioned with minimal effort. User authentication can be integrated with your existing authentication infrastructure through RADIUS, LDAP, AD and PKI. Role-based authorization of access facilitates administration, and fine-grained control ensures that employees and partners can access only permitted services and resources. Access is dynamically limited depending on the client's security posture. With seamless operation and no change in business processes, remote users become productive immediately. The High-Availability option ensures uptime. With minimal IT involvement and operating costs.

Access Modes from Client	
Virtual Service (Vservice)	Supports SSL, Supports Two-Way Certificate Authentication, Supports all TCP Applications
Port Forwarding (Application Tunnel)	Supports all TCP/UDP Applications
Network Connection (NC)	Supports all IP-based Applications
Udesk	Terminal Service (Java)
FilePass	FTP, File Sharing, CIFS
Site-to-Site VPN	Supports all IP-based Applications
Client Operating Systems and supported Modes	
Windows 2000/XP/2003/Vista	Application Tunnel, NC, Udesk, FilePass, Vservice
Windows Mobile 2003, 2005	NC, FilePass, Vservice
Linux/Unix/Mac	Udesk, FilePass, Vservice
Typical Applications	Outlook, File Sharing, Oracle, FTP, Telnet, Web, etc., any IP Application
User Authentication	
Username and Password	Yes
Two-Way Certificate Authentication	Yes
Two-Factor Certificate Authentication	Smart Card, USB Key
Dynamic Password Authentication	Secure Computing, RSA SecureID
Additional Portrayed Code	Yes
User Timeout	Able
User Re-authentication	Yes
One-click Login	Yes
User Authentication Directory	
Local Database	Yes
PKI	Yes
RADIUS Server Support	PAP, CHAP
LDAP	Yes
Windows Active Directory	Yes
NTLM	Yes
LDAP/AD Server Download Group Information	Yes
LDAP/AD Server Download User Information	Yes
Restrict Connection to AD Server via LDAP	Yes
Mass Import of Users	Certificate Users, Password Users
Encryption and Protocol	
Protocol	SSL v2, v3, TLS v1
Symmetric Encryption	RC4, DES, 3DES, AES
Asymmetric Encryption	DH, ADH, RSA (1024 bits, to maximum of 2048 bits)
Hash	SHA-1, MD5
DH Key Exchange	Yes
Certificate	
Generate Self-Signed Certificate	Yes
Certificate Request Message	Yes
Certificate Format	X.509 v2, v3 Compatible
Certification Revocation List	X.509 v2 Compatible
Third Party CA	via Trust Chain, Support Multiple CA
OCSP	Login, Logout, Authentication, Service Accessed, Timeout, Service Volume
OCSP	Yes
Client End Security	
OS Check	Yes
Spyware Check	Yes
Personal Firewall Check	Yes
Anti-Virus Check	Yes
Clear Cache	Yes
Clear Custom Directory	Yes
Execute Custom Script	Yes
Auto-download Client-end Proxy	Yes
Auto-download Policy	Yes
Client-end Program Association	Administrator can set up multiple programs
Auto-launch Client Application	Yes
Categorize Application Service	Yes
Client-end Software Mapping	Yes

Access Control	
Access Control Model	Role-based
Authorization Based on Client-end Condition	Yes
Properties Configuration Based on Client-end Condition	Yes
Restrict Access via Web	Yes
Session Control	Yes
Application Control	Yes
Block Internet	Yes
Split Tunnel	Yes
Content Filtering	FTP, HTTP Commands
User Timeout	Yes
Scheduled Rules	Yes
URL Sub-directory	Yes
Network	
Multiple ISPs	Yes
NAT	SNAT, DNAT
Network Diagnosis	Ping, Traceroute
NTP	Yes
Client-end Intelligent Routing	Yes
Setup Files Upload and Download	Yes
Data Compression	Yes
High Availability	
Dual Host Backup	AP, AA Mode
Load Balancing	Dual-host
Management	
Admin Interface	Web UI, CLI, SSH
Access Control for Administrator	Yes
Administrator Authentication	Password, Certificate
Types of Administrators	System, Configuration, Audit
Customized User Interface	Login Welcome Message, Login UI, Client-end Default Language, Login Page Screen Graphics
Message Broadcast	Based on Roles
SNMP	v3
Logs and Audit	
Syslog	Yes
System Admin Logs	Login, Logout, Authentication, Operation, Timeout
User Log	Login, Logout, Authentication, Service Accessed, Timeout, Service Volume
Storage of Logs	Local, Remote
Automatically Export to Local Disk by Schedule	Export via FTP, Customizable Export Frequency and Content
TOP N Statistics	Services That Generate the Largest Traffic, Users Who are Online the Longest, Users Who Transmit the Largest Amount of Data, Users Who have Logged-in the Most Number of Times
Log Query	Yes
Log Email Alert	Yes
System Monitoring	
System Resources	CPU, RAM, Disk Space
Network Traffic	Port, System
Online Users	User List
Online Services	Yes
Environment	
Power Supply	100 – 250V, 50 – 60Hz
Operating Temperature	0 – 50°C
Non-operating Temperature	-20 – 70°C
Humidity	10% – 90%
Average Uptime	100,000 Hours