

# E-Class Secure Remote Access Series

Secure remote access for the enterprise

## Easy, secure and clientless remote access for the enterprise

With maturing mobile technologies, booming global markets and heightened focus on disaster preparedness, remote access control has become a business imperative. IT is now mandated with providing secure remote access that is easy to use and cost-effective to implement. Client-based VPNs can be cumbersome to use and manage. Dell® SonicWALL® Aventail® E-Class Secure Remote Access (SRA) delivers full-featured, easy-to-manage, clientless or thin-client “in-office” connectivity for up to 20,000 concurrent mobile enterprise users from a single appliance. E-Class SRA enhances productivity and business continuity with policy-enforced remote access to network resources from Windows®, Windows Mobile, Apple® Mac OS®, iOS, Linux®,

and Google® Android™ devices. Built on the powerful SonicWALL Aventail SSL VPN platform, E-Class SRA connects only authorized users to only accepted resources. When integrated with Dell SonicWALL Next-Generation Firewall as a Clean VPN™, the combined solution delivers centralized access control, malware protection, application control and content filtering over the internal wireless network.

This solution is a part of Dell SonicWALL’s E-Class—a line of premium, enterprise-class solutions offering outstanding protection and performance while delivering elegant simplicity and unparalleled value. The E-Class portfolio of products and services includes a comprehensive line of network security, email security and secure remote access solutions.



- Increases productivity
- Lowers IT overhead and total cost of ownership
- Easy-to-use from any endpoint
- Full iOS and Android support
- Robust mobile solution
- Access to all application platforms
- Remote support
- Eliminates routing conflicts
- Single access gateway
- Rapid set-up and deployment
- Easy-to-control with Unified Policy Management

## Features and benefits

### **Increases productivity**

E-Class SRA works on more platforms, including home PCs, kiosks, smartphones, tablets and unmanaged devices over wired and wireless networks. SonicWALL Aventail SRA makes your users more productive by providing easy access to more applications from more environments—including Windows, Apple Mac OS, and Linux computers and Windows Mobile, iOS and Google Android mobile devices.

### **Lowers IT overhead and total cost of ownership**

E-Class SRA lowers IT costs by enabling network managers to easily deploy and manage a single secure access gateway that extends remote access via SSL VPN for both internal and external users to all network resources—including web-based, client/server, host-based and back-connect applications like VoIP. E-Class SRAs are either clientless or use lightweight web-delivered clients, reducing management overhead and support calls.

### **Easy-to-use from any endpoint**

E-Class SRA technology provides transparent access to network resources from any network environment or device. An E-Class SRA provides a single gateway for all access and a common user experience across all platforms—including Windows, Windows Vista®, Windows Mobile, Apple Mac OS and iOS, Google Android and Linux—from managed or unmanaged devices.

### **Full iOS and Android support**

Dell SonicWALL Mobile Connect™, a single unified client app for Apple iOS and Google Android, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.

### **Robust mobile solution**

E-Class SRAs provide the most robust secure access solutions for mobile smartphones and tablets, featuring Session Persistence across office, home or mobile IP addresses without re-authentication.

### **Access to all application platforms**

SonicWALL Aventail Smart Tunneling™ delivers fast and easy access to all applications—whether they are web-based, client/server, server-based or host-based—over a unique architecture that combines the application layer control of SSL with the reach of a Layer 3 tunnel.

### **Remote support**

Dell SonicWALL Secure Virtual Assist enables technicians to provide secure on-demand assistance to customers while leveraging the existing infrastructure.

### **Eliminates routing conflicts**

Adaptive addressing and routing dynamically adapts to networks, eliminating addressing and routing conflicts common with other solutions.

### **Single access gateway**

E-Class SRA gives network managers a single secure access gateway for all users, internal and external, to all resources with complete control. Administrators have even greater control over portal access, content and design with the newly enhanced SonicWALL Aventail WorkPlace Portal.

### **Rapid set-up and deployment**

All E-Class SRAs are easy to set up and deploy in just minutes. The redesigned SonicWALL Aventail's Set-up Wizard provides an easy, intuitive "out-of-the-box" experience with rapid installation and deployment. Dell SonicWALL Mobile Connect for iOS and Android unified client app is easily downloadable from the App Store<sup>SM</sup> or Google Play. Improved management workflow makes it much easier to understand and manage policy objects.

### **Easy-to-control with Unified Policy Management**

SonicWALL Aventail Unified Policy™ offers easy object-based policy management of all users, groups, resources and devices, while enforcing granular control based on both user authentication and endpoint interrogation. Policy Zones can ensure unauthorized access is denied, or quarantined for remediation.

## Detect the security of any endpoint

### Robust interrogation for secure control of the endpoint

Only SonicWALL Aventail End Point Control™ (EPC™) lets you enforce granular access control rules for Windows®, Windows Vista, Windows 7, Windows Mobile, Apple Mac OS and iOS, Google Android and Linux endpoints. EPC combines pre-authentication interrogation to confirm endpoint criteria such as anti-virus updates. SonicWALL Aventail Policy Zones™ apply detected endpoint criteria to automated policy enforcement. For example, a user's access may be quarantined—and redirected to remediation instructions—until a security patch is installed. Device watermarks allow access from a lost or stolen device to be easily

revoked, based upon detection of client certificates. Device Identification enables administrators to tie the serial or equipment ID number for a specific Windows, Apple Mac OS, iOS or Google Android device to a specific user or group. SonicWALL Aventail's Virtual Keyboard stops keystroke sniffers on untrusted endpoints. SonicWALL Aventail Recurring EPC performs endpoint scans at user login and at administrator-defined intervals to ensure the ongoing integrity of any endpoint. End Point Control includes capabilities to determine if an Android system has been rooted or an iOS device has been jailbroken.

### Advanced EPC for ultimate protection

Optional SonicWALL Aventail Advanced EPC™ combines granular endpoint control detection with superior data protection. Advanced Interrogator

simplifies device profile set-up using a comprehensive predefined list of anti-virus, personal firewall and anti-spyware solutions for Windows, Macintosh and Linux platforms, including version and currency of signature file update. SonicWALL Aventail Cache Control purges browser cache, session history, cookies and passwords. SonicWALL Aventail Secure Desktop creates a virtual encrypted environment that prevents sensitive information from being left behind. SonicWALL Aventail E-Class SRAs also block suspect email attachments in Outlook Web Access or Lotus iNotes, or block access to financial data or patient records. On E-Class SRAs, connections are closed by default, providing "deny all" firewall-style protection.

## Protect your enterprise resources with ease

### Streamlined policy management

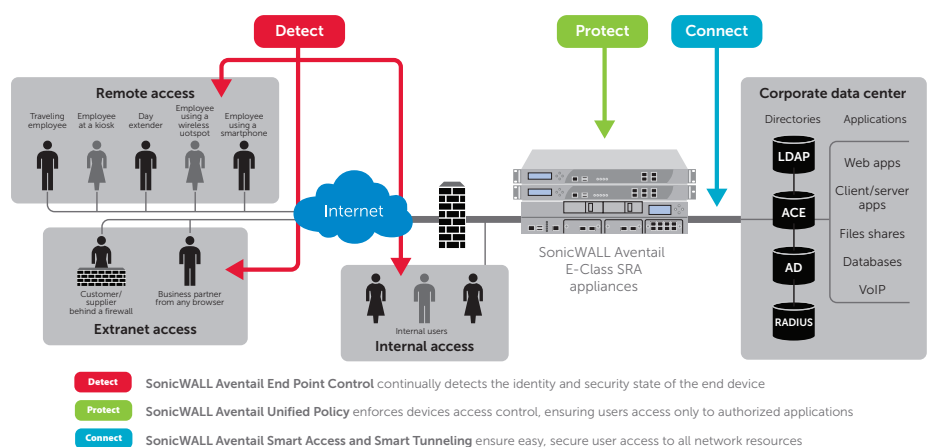
With its context-sensitive help and Set-up Wizard, an E-Class SRA solution is easy to set up and deploy. The extensible, object-based SonicWALL Aventail Unified Policy™ model consolidates control of all web resources, file shares and client-server resources in a single location, so that policy management takes only minutes. Groups can be populated dynamically based on RADIUS, ACE, LDAP or Active Directory authentication repositories, including nested groups. E-Class SRAs support Single Sign-On (SSO) and forms-based web applications. Moreover, users can easily update their own passwords without IT assistance. In addition, SonicWALL Aventail Policy Replication lets IT easily replicate policy across multiple appliance nodes, either in the same cluster or in a geographically distributed fashion. One-Time Password (OTP) support provides a built-in method to generate and distribute secondary factors, for easy and cost-effective two-factor authentication. Administrators can

associate OTPs by Realm for greater flexibility in authentication control.

### Intuitive management and reporting

The SonicWALL Aventail Management Console™ provides a rich, centralized set of monitoring capabilities for auditing, compliance, management and resource planning. Optional SonicWALL Aventail Advanced Reporting™ audits who accessed what enterprise resources, at what time, from which remote location,

using standard or custom reports that can be viewed from any web browser. Visual tools provide real-time information on system state and direct, intuitive options for managing system objects. Enhanced user monitoring features streamline auditing and troubleshooting of current and historical user activity. Administrators can easily view or filter activity by user, time, throughput, realm, community, zone, agents or IP address.



SonicWALL Aventail E-Class Secure Remote Access solutions provide secure access for all users, devices and applications.

## Connect users to resources— simply and seamlessly

### **Broadest application access from the most endpoints**

E-Class SRA appliances deliver intelligent access to web-based, client/server, server-based, host-based and back-connect applications such as VoIP. SonicWALL Aventail SRAs work seamlessly across Windows, Windows Vista, Windows 7, Windows Mobile, Apple Mac OS and iOS, Linux or Google Android platforms, from desktops, laptops, kiosks, smartphones and tablets, as well as application-to-application. This significantly increases productivity, while reducing support costs. From the user's perspective, SonicWALL Aventail Smart Access™ dynamically determines and deploys the appropriate access method and security level based on the type and state of the device, user identity and resources needed. Zone-based provisioning enables administrators to extend control over what access agents are deployed based upon the remote user's End Point Control classification. Adaptive addressing and routing dynamically adapts to networks, eliminating conflicts. Smart Access streamlines installation and activation of any required agents on Windows devices according to Microsoft standards.

### **Clientless web-based access or full "in-office" experience**

SonicWALL Aventail E-Class Secure Remote Access appliances offer both clientless browser-based access and full access to client/server and legacy applications from Windows, Windows Vista, Windows 7, Windows Mobile, Macintosh and Linux environments. SonicWALL Aventail WorkPlace™ delivers a policy-driven, device-optimized web portal that provides easy access to web-based and client/server applications from desktops, laptops, smartphones and tablets, even from wireless hotspots and kiosks. Users can define shortcuts to frequently used resources. Workplace

can be customized with different logos and color schemes for partners and employees. SonicWALL Aventail WorkPlace access is well suited for devices not managed by your organization. SonicWALL Aventail Connect™ access delivers an "in-office" experience for Windows, Windows Vista, Windows 7, Windows Mobile, Mac OS, or Linux users, enabling full access to client/server and web-based applications and all other network resources. Enabled through a lightweight, web-deployable agent, or through an easily provisioned standard MSI installation, SonicWALL Aventail Connect is ideal for full access from IT-managed devices that require strong desktop security, split-tunneling control and personal firewall detection. SonicWALL Aventail Smart Tunneling™ offers a Layer 3 technology that supports UDP, TCP and IP protocols, and back-connect applications like VoIP. In NAT mode, no set-up of IP address pools is required.

### **A solution customized to users' needs**

Optional SonicWALL Aventail Native Access Modules™ offer additional native access to Windows Terminal Services, VMWare View (using SonicWALL Aventail OS) as well as native support for load-balanced Citrix farm environments via the WorkPlace Portal as an alternative to expensive Citrix nFuse implementations. Virtual Hosts provide clientless access to a wide range of complex web applications, including those using Flash and JavaScript.

### **Most complete access solution for mobile devices**

E-Class SRA Series appliances offer web-based and client-based access to critical network resources from iOS, Google Android and Windows Mobile devices, as well as email access from iOS, Android and Symbian devices, with complete security and control. SonicWALL Aventail SRA solutions provide centralized management of all devices with granular access control

and the ability to prohibit access from the device if it is lost or stolen. Moreover, with Session Persistence, mobile users can have the flexibility to retain a current session as they switch between networks—on the go between office, commute, home and hotel—without needing to re-authenticate.

### **Reliable high availability and flexibility**

For added reliability, E-Class SRA appliances offer active/active high availability (HA) with integrated load balancing and active/active stateful failover on the SRA EX9000, EX7000 and EX6000, eliminating the added cost of a third-party load balancer. In addition, with an optional SonicWALL Aventail Spike License Pack, you can temporarily and cost-effectively increase your remote user count to the maximum capacity of those E-Class SRA appliances for disaster recovery or planned business cycle peaks, whether it is a few dozen or a few thousand additional users.

### **The clear business choice**

The SonicWALL Aventail E-Class Secure Remote Access Series includes the award-winning EX Series of SSL VPN hardware and virtual appliances, offering your business the best solution for secure remote access control. With Dell SonicWALL, you can enhance your enterprise network security, increase your mobile workforce productivity for greater return on investment (ROI) and reduce IT overhead for a lower total cost of ownership (TCO). Dell SonicWALL's best-of-breed technology gives you flexible access options for disaster recovery and supports easy audits to help you comply with FIPS, Sarbanes-Oxley, HIPAA, Basel 2 and other regulatory requirements, even during unexpected business disruptions. And E-Class SRA appliances make an ideal replacement strategy for IPSec VPNs. From any business perspective, Dell SonicWALL is the easy choice for secure remote access.

# Specifications

Performance	EX6000	EX7000	EX9000
<b>Concurrent users</b>	Support for up to 250 concurrent users per node or HA pair	Support for up to 5,000 concurrent users per load-balanced node or HA pair	Support for up to 20,000 concurrent users per node or HA pair
<b>Hardware</b>			
<b>Form factor</b>	U rack-mount	U rack-mount	2U rack-mount
<b>Dimensions</b>	17.0 x 16.75 x 1.75 in (43.18 x 42.54 x 4.44 cm)	17.0 x 16.75 x 1.75 in (43.18 x 42.54 x 4.44 cm)	27.0 x 18.9 x 3.4 in (68.6 x 48.2 x 8.8 cm)
<b>Processor</b>	Intel Celeron 2.0 GHz 1 GB DDR533	Intel Core2 Duo 2.1 GHz 2 GB DDR533	Intel Quad Xeon 2.46 GHz
<b>Network</b>	4 Stacked PCIe GB	6 Stacked PCIe GB	(4) 10GbE sfp, (8) 1 GbE
<b>Power</b>		Fixed power supply	Dual power supply, hot swappable
Input rating	100-240 VAC, 1.2 A	100-240 VAC, 1.5 A, 50-60 Hz; or -36 - -72 VDC, 3.2 A*	100-240 VAC, 2.8A
Power consumption	75W	150W	320W
MTBF	MTBF 100,000 hours at 35° C (95° F)	MTBF 100,000 hours at 35° C (95° F)	MTBF 120,000 hours at 35° C (95° F)
<b>Environmental</b>	WEEE, EU RoHS, China RoHS		
Operating temperature:	0°C to 40°C (32°F to 104° F)		
Non-operating shock	110g, 2msec		
<b>Regulatory approvals</b>			
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC	FCC, ICES, CE, C-Tick, VCCI; MIC	FCC, ICES, CE, C-Tick, VCCI; MIC
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB Scheme	TUV/GS, UL, CE PSB, CCC, BSMI, CB Scheme	TUV/GS, UL, CE PSB, CCC, BSMI, CB Scheme
<b>Key features</b>			
<b>Security</b>			
FIPS certification	Yes		Pending
Encryption	Configurable session length, Ciphers: DES, 3DES, RC4, AES, Hashes: MD5, SHA		
Authentication methods	Server-side digital certificates, Username/password, Client-side digital certificates RSA SecurID and other one-time password tokens, Dual/stacked authentication		
Directories	Microsoft Active Directory, LDAP (Active Directory, Sun iPlanet, etc.), RADIUS; Dynamic groups based on LDAP/AD queries, Certificate revocation lists (CRL)		
Password management	Notification of password expiration and password change from the Dell SonicWALL Aventail Workplace portal		
Access control options	User and group, Source IP and network, Destination network, Service/Port (OnDemand and Connect only) Define resources by destination URL, host name or IP address, IP range, subnet and domain, Day, date, time and range, Browser encryption key length, Policy Zones (allows, denies and quarantines access and provides data protection based on end point security profile), File system access controls		
Dell SonicWALL Aventail End Point Control™ (EPC™)	Detection of files, registry keys, running processes and Device Watermarks; Advanced Interrogator: (simplified granular end point detection, including detailed configuration information on over 100 anti-virus, anti-spyware and personal firewall solutions, including McAfee, Symantec, Sophos and Trend) Data Protection: Cache Control (data protection), Secure Desktop (advanced data protection); Includes jailbreak or root detection for iOS and Android devices		
<b>Access and application support</b>			
Dell SonicWALL Aventail Workplace™ Access (browser-based access)	Clientless access to web-based resources, web file access: SMB/ CIFS, DFS, Personal Bookmarks, Multiple optimized Workplace portals for different user groups, Access to any TCP- or UDP-based application via the Workplace portal (leveraging OnDemand Tunnel agent)		
Dell SonicWALL Aventail Workplace Mobile Access	Customized Workplace support for smartphone and tablet browsers		
Dell SonicWALL Aventail Connect™ Access	Pre-installed agent provides access to any TCP- or UDP-based application (Windows, Macintosh and Linux support)		
Dell SonicWALL Aventail Connect Mobile™	Lightweight agent that provides access to both web and client/server applications for Windows Mobile devices		
Dell SonicWALL Mobile Connect™	Lightweight agent that provides access to both web and client/server applications for Apple iOS and Google Android devices		
<b>Management and administration</b>			
Management	Dell SonicWALL Aventail Management Console (AMC): centralized web-based management for all access options, End Point Control configuration, access control policies and Workplace Portal configuration, easy policy replication across multiple appliances and locations, role-based administration		
Auditing	Dell SonicWALL Aventail Advanced Reporting™, RADIUS auditing and accounting integration		
Monitoring and logging	User connection monitoring, event alarms, View logs and performance information via the Dell SonicWALL Aventail Management Console, SNMP integration including Dell SonicWALL Aventail-specific SNMP MIB, Support for central SYSLOG server		
<b>High availability</b>			
High availability	Support for high-availability 2-node clusters with built-in load-balancing and stateful authentication failover		
Clustering	–	–	Support for load-balanced arrays using standard external loadbalancers
<b>E-Class SRA virtual appliance</b>			
Hypervisor	ESG™ and ESX™ (version 4.0 and newer)		
Operating system installed	Hardened SonicLinux		
Allocated memory	2 GB		
Applied disk size	80 GB		
VMware hardware compatibility guide	<a href="http://www.vmware.com/resources/compatibility/search.php">http://www.vmware.com/resources/compatibility/search.php</a>		



## E-Class SRA EX9000

SRA EX9000 Appliance 01-SSC-9574  
 Lab Box User License\* 01-SSC-9610  
 5,000 Concurrent User License 01-SSC-8470  
 10,000 Concurrent User License 01-SSC-9942  
 15,000 Concurrent User License 01-SSC-9946  
 20,000 Concurrent User License 01-SSC-9948  
 \*Includes appliance add-ons



## E-Class SRA EX7000

SRA EX7000 Appliance 01-SSC-9602  
 Lab Box User License\* 01-SSC-9610  
 50 Concurrent User License 01-SSC-9614  
 100 Concurrent User License 01-SSC-9616  
 250 Concurrent User License 01-SSC-9618  
 500 Concurrent User License 01-SSC-9647  
 1,000 Concurrent User License 01-SSC-9649  
 2,000 Concurrent User License 01-SSC-9651  
 5,000 Concurrent User License 01-SSC-8470  
 \*Includes appliance add-ons



## E-Class SRA EX6000

SRA EX6000 Appliance 01-SSC-9601  
 Lab Box User License\* 01-SSC-9610  
 25 Concurrent User License 01-SSC-9612  
 50 Concurrent User License 01-SSC-9614  
 100 Concurrent User License 01-SSC-9616  
 250 Concurrent User License 01-SSC-9618



## E-Class SRA Virtual Appliance

E-Class SRA Virtual Appliance 01-SSC-8468  
 10 Concurrent User License 01-SSC-9611  
 25 Concurrent User License 01-SSC-9612  
 50 Concurrent User License 01-SSC-9614

For license and support SKUs please visit [www.sonicwall.com](http://www.sonicwall.com)

For more information on Dell SonicWALL's E-Class solutions, please visit [www.sonicwall.com](http://www.sonicwall.com).

Security Monitoring Services from Dell SecureWorks are available for this appliance Series. For more information, visit [www.dell.com/secureworks](http://www.dell.com/secureworks)