E-Class Secure Remote Access Series

Enable mobile and remote worker productivity while protecting from threats

Easy, secure mobile and remote access for the enterprise
The proliferation of mobile devices in the workplace has increased the demand for secure access to mission-critical applications, data and resources. In parallel, a growing mobile malware threat has caused mobile protection to become a business imperative. Because legacy, client-based VPNs can be cumbersome for mobile workers to use and manage, IT departments are looking for easy-to-use, cost-effective and secure mobile access solutions that address the needs of their increasingly mobile workforces.

The Dell™ SonicWALL™ E-Class Secure Remote Access (SRA) Series appliance provides mobile and remote workers using smartphones, tablets or laptops—whether managed or unmanaged BYOD—with fast, easy, policy-enforced access to mission-critical applications, data and resources without compromising security.

For smartphones and tablets, the solution includes the SonicWALL Mobile Connect™ application that provides iOS , Android and Windows 8.1 devices with fast, easy access to network resources, including shared folders, client-server applications, intranet sites and email. Users and IT administrators can download the SonicWALL Mobile Connect application via the Apple App Store℠ and Google Play. New with Windows 8.1, Windows tablets and laptops ship pre-installed with the Mobile Connect application. For PCs and laptops, including Windows®, Mac OS® and Linux® computers, the solution supports clientless, secure browser access and thin-client access.

Built on the powerful SonicWALL Aventail SSL VPN platform, E-Class SRA connects only authorized users and trusted devices to permitted resources. When integrated with a Dell SonicWALL next-generation firewall as a Clean VPN™, the combined solution delivers centralized access control, malware protection, application control and content filtering. The multi-layered protection of Dell SonicWALL Clean VPN™ decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment.

Benefits:

- Cross-platform support for increased mobile worker productivity
- Single access gateway to all network resources, clientless or web-delivered clients and a management dashboard work to lower IT overhead and TCO
- Common user experience across all operating systems facilitates ease of use from any endpoint
- Mobile Connect app for iOS, Android and Windows 8.1 offers mobile device ease of use
- Context aware authentication ensures only authorized users and trusted mobile devices are granted access
- Session Persistence technology gives users a secure, seamless mobile experience without the need to re-authenticate
- Smart Tunneling delivers fast, easy access to all application platforms
- Secure Virtual Assist gives technicians remote control of customer devices
- Adaptive addressing and routing deploys appropriate access methods and security levels
- Setup wizard makes deployment easy
- Efficient object-based policy management of all users, groups, resources and devicess

Features

Cross-platform support—E-Class SRA can be deployed across a wide range of environments and devices, including smartphones, tablets, laptops, PCs, kiosks and unmanaged devices over wired and wireless networks. Dell SonicWALL SRA makes your users more productive by providing easy access to email, files, applications and more from a wide range of environments—including iOS and Android smartphones and tablets; Windows 8.1 tablets and laptops; and Mac OS®, Windows and Linux computers.

Single access gateway, clientless or web-delivered clients, management dashboard—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. An at-a-glance management dashboard makes monitoring remote access quick and easy, lowering IT overhead even more.

Common user experience across all operating systems—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 operating systems—including Windows, Apple Mac OS and iOS, Google Android and Linux—from managed or unmanaged devices.

SonicWALL Mobile Connect app—SonicWALL Mobile Connect™, a single unified client app for iOS and Android, provides smartphone and tablet users and Windows 8.1 tablets and laptops users with easy network-level access to corporate and academic resources over encrypted SSL VPN connections. Mobile Connect is easily downloadable from the Apple App Store^SM or Google Play and embedded with Windows 8.1 devices.

Context aware
Access to the corporate network is granted only after the user has been authenticated and mobile device integrity has been verified.

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

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

Adaptive addressing and routing—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 Dell SonicWALL WorkPlace Portal.

Dell SonicWALL setup wizard—All E-Class SRAs are easy to set up and deploy in just minutes. The set-up wizard provides an easy, intuitive “out-of-the-box” experience with rapid installation and deployment.

Unified Policy—Dell SonicWALL 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 Dell SonicWALL End Point Control™ (EPC™) lets you enforce granular access control rules for Windows, Apple Mac OS and iOS, Android and Linux endpoints. EPC combines pre-authentication interrogation to confirm endpoint criteria such as anti-virus updates. Dell SonicWALL 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 device to a specific user or group. Dell SonicWALL's Virtual Keyboard stops keystroke sniffers on untrusted endpoints. 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 iOS device has been jailbroken or an Android system has been rooted.

Advanced EPC for ultimate protection

Optional Dell SonicWALL 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, Mac and Linux platforms, including version and currency of signature file update. Dell SonicWALL Cache Control purges browser cache, session history, cookies and passwords. Dell SonicWALL Secure Desktop creates a virtual encrypted environment that prevents sensitive information from being left behind. Dell SonicWALL 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.

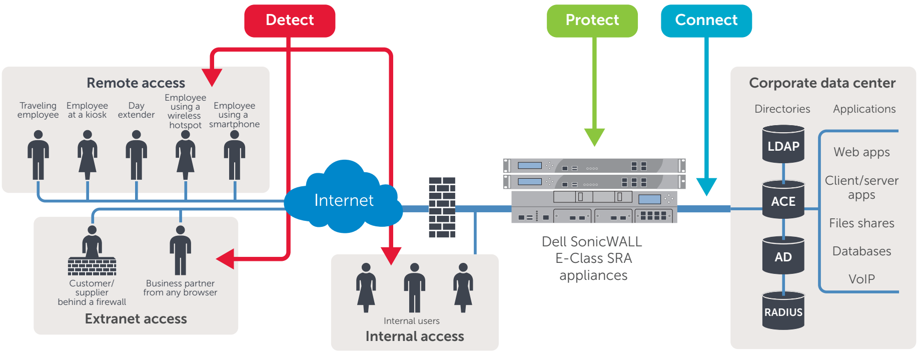
Protect your enterprise resources with ease

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 Dell SonicWALL 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, Dell SonicWALL 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 Dell SonicWALL management console provides an at-a-glance management dashboard and a rich, centralized set of monitoring capabilities for auditing, compliance, management and resource planning. Optional Dell SonicWALL 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.



🟥 Detect **Dell SonicWALL End Point Control** continually detects the identity and security state of the end device

🟩 Protect **Dell SonicWALL Unified Policy** enforces devices access control, ensuring users access only to authorized applications

🟦 Connect **Dell SonicWALL Smart Access and Smart Tunneling** ensure easy, secure user access to all network resources

Dell SonicWALL 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. Dell SonicWALL E-Class SRAs work seamlessly across Windows, Apple Mac OS and iOS, Linux or Android devices, from smartphones, tablets, laptops, desktops and kiosks, as well as application-to-application. This significantly increases productivity, while reducing support costs. From the user's perspective, Dell SonicWALL 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

Dell SonicWALL E-Class Secure Remote Access appliances offer both clientless browser-based access and full access to client/server and legacy applications from Windows, Mac and Linux environments. Dell SonicWALL 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. Dell SonicWALL WorkPlace access is well suited for devices not managed by your organization. Dell SonicWALL Connect access delivers an "in-office" experience for Windows, Mac OS, and 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, Dell SonicWALL Connect is ideal for full access from IT-managed devices that require strong desktop security, split-tunneling control and personal firewall detection. Dell SonicWALL 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 Dell SonicWALL Native Access Modules offer additional native access to Windows Terminal Services, VMWare View (using Dell SonicWALL 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 access to critical network resources from iOS and Android smartphones and tablets as well as Windows 8.1 tablets and laptops via SonicWALL Mobile Connect, an easy to use mobile application that authenticates and provides one-click access to authorized corporate applications, data and resources. Dell SonicWALL E-Class 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 Dell SonicWALL 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 Dell SonicWALL 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 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 and mobile access.

Specifications

Performance	EX6000	EX7000	EX9000
Concurrent users	Support for up to 250 concurrent users per node or HA pair	Support for up to 5,000 concurrent users per load-balanced	Support for up to 20,000 concurrent users per node or HA pair
Hardware	**EX6000**	**EX7000**	**EX9000**
Form factor	1U rack-mount	1U rack-mount	2U rack-mount
Dimensions	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)
Processor	Intel Celeron 2.0 GHz 1 GB DDR533	Intel Core2 Duo 2.1 GHz 2 GB DDR533	Intel Quad Xeon 2.46 GHz
Network	4 Stacked PCIe GB	6 Stacked PCIe GB	(4) 10GbE sfp, (8) 1 GbE
Power	Fixed power supply	Dual power supply, hot swappable	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
MTFB	MTBF 100,000 hours at 35° C (95° F)		MTBF 120,000 hours at 35° C (95° F)
Environmental	WEEE, EU RoHS, China RoHS		
Operating temperature:	0°C to 40°C (32°F to 104° F)		
Non-operating shock	110g, 2msec		
Regulatory approvals			
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC		
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB Scheme		
Key features	**EX6000**	**EX7000**	**EX9000**
Security			
FIPS certification		Yes	
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 Virtual Desktop (advanced data protection); Includes jailbreak or root detection for iOS and Android devices		
Secure network detection	Secure network detection automatically detects whether the endpoint is connected to an internal network or remote and applies the appropriate security policies		
Access and application support			
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, Mac and Linux support)		
SonicWALL Mobile Connect	Full network level access for web and client/server applications from Apple iOS, Google Android and Windows 8.1 devices		
Management and administration			
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 at-a-glance management dashboard		
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 SNMP integration including Dell SonicWALL Aventail-specific SNMP MIB, Support for central SYSLOG server		
Scheduler	Enables the ability schedule tasks such as deploying, replicating settings and applying changes without human intervention		
High availability			
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
Other			
IPv6 support	Provides the ability to authenticate a client with IPv6 internet connectivity and allow the client to interact with resources through the E-Class SRA appliance.		
ADA 508 support	ADA 508 support within the management console, Workplace and Connect tunnel to comply with section 508 of the Americans Disabilities Act including keyboard usability and compatibility with assistive technologies		
Browsers supported	E-Class SRA supports all the industry leading browsers such as Internet Explorer, Firefox, Chrome, and Safari (supported versions are constantly updated)		
	E-Class SRA Virtual Appliance		
Concurrent users	5,000		
Hypervisor	ESG™ and ESX™ (version 4.0 and newer)		
Operating system installed	Hardened Linux		
Allocated memory	2 GB		
Applied disk size	80 GB		
VMware hardware compatibility guide	http://www.vmware.com/resources/compatibility/search.php		

SRA EX9000 Appliance	01-SSC-9574
SRA EX7000 Appliance	01-SSC-9602
SRA EX6000 Appliance	01-SSC-9601
E-Class SRA Virtual Appliance	01-SSC-8468
E-Class SRA 5 Lab User License–Stackable	01-SSC-7855
E-Class SRA 5 User License–Stackable	01-SSC-7856
E-Class SRA 10 User License–Stackable	01-SSC-7857
E-Class SRA 25 User License–Stackable	01-SSC-7858
E-Class SRA 50 User License–Stackable	01-SSC-7859
E-Class SRA 100 User License–Stackable	01-SSC-7860
E-Class SRA 250 User License–Stackable	01-SSC-7861
E-Class SRA 500 User License–Stackable	01-SSC-7862
E-Class SRA 1,000 User License–Stackable	01-SSC-7863
E-Class SRA 2,500 User License–Stackable	01-SSC-7864
E-Class SRA 5,000 User License–Stackable	01-SSC-7865
E-Class SRA 7,500 User License–Stackable	01-SSC-7948
E-Class SRA 10,000 User License–Stackable	01-SSC-7949
E-Class SRA 15,000 User License–Stackable	01-SSC-7951
E-Class SRA 20,000 User License–Stackable	01-SSC-7953

For more information on Dell SonicWALL's solutions, please visit **www.sonicwall.com**.

For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.