# E-Class Secure Remote Access Appliance

Safeguard corporate data while supporting remote worker and BYOD initiatives

As BYOD becomes more commonplace, IT departments struggle to balance security and compliance with the flexibility of allowing employees to use their own smartphones, tablets and laptops to access corporate data and resources. Security breaches can occur from unauthorized persons accessing lost or stolen devices, unmanaged mobile devices serving as a conduit to infect the network with malware, the interception of corporate data over unsecured third-party wireless networks or mobile services, or rogue apps gaining access to data stored on a device. To enable access for mobile workers while protecting from threats, enterprises must implement solutions that take a new approach, focusing on managing and securing business apps, data and usage, while coexisting with, and respecting, personal apps and data privacy.

Dell™ SonicWALL™ E-Class Secure Remote Access (SRA) with the new Secure Mobile Access (SMA) OS 11.0 enables administrators to easily provision secure mobile access and role based privileges for managed and BYOD unmanaged devices. You can provide mobile workers with policy-enforced per-app SSL VPN access to the allowed enterprise data and resources that they demand, while protecting the corporate network from mobile security threats. With SMA, only authorized users, mobile apps and trusted devices are permitted access to resources. Also, corporate VPN access can be restricted to the set of mobile apps trusted by the administrator while unauthorized mobile apps are prevented from accessing VPN resources. SMA is the only solution that requires no modification of mobile apps for per app VPN access. Any mobile app or secure container can be supported with no modifications, app wrapping or SDK development. The solution also helps enforce and track mobile worker acceptance of device authorization policy terms, reducing legal risk.

For mobile device users, the solution includes the intuitive SonicWALL Mobile Connect™ app that, in combination with the E-Class SRA, provides iOS, Mac OS X, Android, Kindle Fire or Windows 8.1 devices with fast, easy per-app VPN access to permitted resources, including shared folders, client-server applications, intranet sites, email and virtual desktop applications such as Citrix, VMware view, RDP and Dell vWorkspace.

For multi-layer threat protection, when integrated with a Dell SonicWALL next-generation firewall as a Clean VPN™, the solution decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment and the combined solution delivers centralized access control, malware protection, web application control and content filtering.


Benefits:

- Enables mobile worker productivity with secure SSL VPN connection and granular, policy-enforced access control to resources
- Restricts VPN access to an allowed set of trusted mobile apps, and reduces business risk by enabling IT to manage and enforce BYOD device authorization policy terms
- Mobile Connect app for iOS, Mac OS X, Android, Kindle Fire and Windows 8.1 offers mobile device ease of use and deployment
- Context aware authentication ensures only authorized users and trusted mobile devices are granted access
- Efficient object-based policy management of all users, groups, resources and devices

## Features

**Secure, policy-enforced access to network resources**—The Dell SonicWALL E-Class SRA appliance powered by Secure Mobile Access OS 11.0 enables IT to easily provision policy-enforced SSL VPN access and role based privileges for mobile users with managed and unmanaged devices. With the SonicWALL Mobile Connect app, mobile workers can initiate an encrypted SSL VPN connection to a SonicWALL E-Class SRA appliance and gain fast, simple access to the allowed corporate data, applications and resources that they demand, — including web-based, client/server, host-based, VDI and back-connect applications like VoIP, while protecting the corporate network from mobile security threats, such as unauthorized access to data and malware attacks.

**Per-application VPN**—E-Class SRA with Secure Mobile Access OS 11.0 enables administrators to establish and enforce policies to designate which mobile apps on a BYOD device can be granted VPN access to the network. This ensures that only authorized mobile business apps utilize VPN access. SMA 11.0 is the only solution that requires no modification of mobile apps. Any mobile app or secure container can be supported with no modifications, app wrapping or SDK development.

**BYOD device registration and security policy management**—New with SMA 11.0, prior to granting network access, if a mobile device has not previously registered with the E-Class SRA appliance, the user is presented with a personal device authorization policy for acceptance. The user must accept the terms of the policy to register the device and gain access to allowed corporate resources and data. The terms of the security policy are customizable by the administrator. Enforced policy acceptance and reporting helps reduce business risk associated with implementing a BYOD policy.

**Easy access to authorized resources**—With the intuitive SonicWALL Mobile Connect app, iOS, MacOS X, Android, Kindle Fire and Windows 8.1 mobile devices can connect to allowed network resources over encrypted SSL VPN connections. Once a user and device are verified, Mobile Connect offers pre-configured bookmarks for one-click access to corporate applications and resources for which the user and device has privileges.

**Context aware authentication**—Access to the corporate network is granted only after the user has been authenticated and mobile device integrity, including jailbreak and root status, device ID, certificate status and OS version, 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.

**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.

**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 state 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 X and iOS, Android, Kindle Fire 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 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.

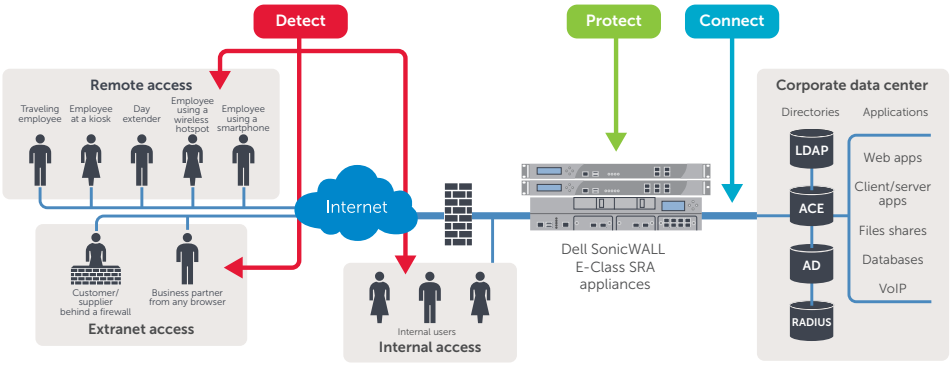
## Protect your enterprise resources with ease

### Streamlined policy management

With its context-sensitive help and set-up wizard, an E-Class SRA solution is easy to set up and deploy. SRA solutions with Unified Policy consolidate 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.




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

## 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 & ICSA 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, Captcha support | | |
| 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 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, Mobile application VPN access control | | |
| Dell SonicWALL 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); 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 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 WorkPlace Mobile Access | Customized WorkPlace support for smartphone and tablet browsers | | |
| Dell SonicWALL 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, Mac OS X, Kindle Fire, Android and Windows 8.1 devices | | |
| Management and administration | | | |
| Management | Dell SonicWALL Management Console (AMC): centralized web-based management for all access options, End Point Control configuration, access control policies, mobile application 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 Advanced Reporting, RADIUS auditing and accounting integration | | |
| Monitoring and logging | User connection monitoring, event alarms, View logs and performance information via the Dell SonicWALL SNMP integration including Dell SonicWALL-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. | | |
| Disability Worker Support (ADA 508) | 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) and supports HTML 5 browser access to RDP and VNC applications. Users with HTML5 compatible browsers can securely access RDP and VNC applications without risking threats introduced with Java and ActiveX plugins. Also, users with devices that don't support Java or ActiveX can now use HTML5 browsers to access RDP and VNC applications via the SRA web portal. | | |
| | **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

**About Dell Software**
Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. DellSoftware.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.


DataSheet-EClassSRA-US-TD625-20130325