Secure Mobile Access Appliance

Safeguard corporate data while supporting remote worker and BYOD initiatives

Mobile and BYOD are creating a new wave of security, compliance and access challenges for IT organizations. 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 address these challenges, many organizations are considering or have already deployed hosted virtual desktop (HVD), enterprise mobility management (EMM) or other data encryption solutions to secure business data on mobile and remote devices. This a great start, but if only on-device data protection is addressed, company data and networks are still at risk. Security is an end-to-end mobile workflow challenge.

End-to-end data protection and security

The Dell Secure Mobile Access (SMA) gateway enables administrators to easily provision secure mobile access and role-based privileges for managed and unmanaged devices. You can provide mobile workers with policy-enforced per-app VPN access to the allowed enterprise data and resources that they require — while protecting the corporate network from mobile security threats.

The SMA gateway integrates with all leading EMM vendors, including Dell Enterprise Mobility Management, to provide the most secure end-to-end mobile management and security solution for bring-your-own (BYO), choose-your-own (CYO) and managed devices. EMM technology establishes on-device data protection policies and app management, and SMA completes the end-to-end data protection and security solution by enforcing access control policy — thereby ensuring that only trusted users and devices and authorized, validated mobile apps are granted VPN access and only to allowed company networks and resources.

In addition, 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. 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.

Secure access for mobile devices

For mobile device users, the solution includes the intuitive Dell Mobile Connect app. In combination with the SMA gateway, this app provides iOS, Mac OS X, Android, Kindle Fire or Windows 8.1 devices with 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, Remote Desktop Protocol (RDP) and Dell vWorkspace.

Benefits:

- Enables mobile worker productivity with secure SSL VPN connection and granular, policy-enforced access to resources
- Restricts VPN access to an allowed set of trusted mobile apps while reducing business risk by enabling IT to manage and enforce BYOD authorization policy terms
- Includes the Mobile Connect app, which provides iOS, Mac OS X, Android, Kindle Fire or Windows 8.1 devices with easy per-app VPN access to permitted resources
- Provides context-aware authentication to ensure that only authorized users and trusted mobile applications and devices are granted VPN access
- Enables efficient object-based policy management of all users, groups, resources and devices

Dell SMA Workplace portal

For clientless browser access, the SMA Workplace portal provides secure access to web applications, client/server applications and file shares from iOS, Android, Windows, Apple Mac or Linux endpoint devices. The portal supports access to resources using standard HTML 5 browsers (available for most smartphones, tablets and laptops), including access to RDP published apps and desktops, Citrix Xendesktop and Xenapps (ICA support). Users with HTML5 browsers can now securely access these resources without the Java or ActiveX browser plug-ins that legacy web browsers require, reducing threat risk and complexity. Also, users with devices that traditionally don't support Java or ActiveX web browser plug-ins, such as iOS devices, can use a standard HTML5 browser to gain access to allowed resources.

Multi-layer threat protection

When integrated with a Dell SonicWALL next-generation firewall as a Clean VPN, the SMA 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.

Features

Secure, policy-enforced access to network resources

IT can easily provision policy-enforced SSL VPN access and role-based privileges for mobile users with managed and unmanaged devices. With the Mobile Connect app, mobile workers can initiate an encrypted SSL VPN connection to an SMA gateway appliance and quickly access the allowed corporate data, applications and resources they need — including web-based, client/server, host-based, VDI and back-connect applications like voice over IP (VoIP). The solution protects the corporate network from mobile security threats, such as unauthorized access to data and malware attacks.

Per-application VPN

Administrators can establish and enforce policies to designate which mobile apps on a mobile device are granted VPN access to the network. This ensures that only authorized mobile business apps gain VPN access. Plus, the SMA gateway 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

If a user attempts access from a mobile device that has not yet been registered with the SMA appliance, the user is presented with a personal device authorization policy. Administrators can customize the terms of the security policy. The user must accept the terms of the policy to register the device and gain access to allowed corporate resources and data. Requiring policy acceptance reduces the business risk associated with implementing a BYOD policy.

Easy access to authorized resources

With the intuitive 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 permitted corporate applications and resources.

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

The SMA gateway appliance provides robust and reliable secure access for laptops, smartphones and tablets, featuring session persistence across different locations (office, home or mobile) without re-authentication.

Dell SMA setup wizard

All SMAs are easy to set up and can be deployed in just minutes, thanks to an intuitive setup wizard.

Unified policy

The SMA gateway appliance 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 ensure that unauthorized access attempts are denied or quarantined for remediation.

Detect the security state of any endpoint

Robust interrogation for secure control of the endpoint

Dell SMA 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 provides pre-authentication interrogation to confirm endpoint criteria such as anti-virus updates.

- **Policy zones** apply 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.
- **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 the endpoint. EPC also 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 SMA advanced EPC combines granular endpoint control detection with superior data protection.

- Advanced interrogator simplifies device profile setup 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.
- Cache control purges browser cache, session history, cookies and passwords.
- Dell SMA gateways also block suspect email attachments in Outlook Web Access or Lotus iNotes, and they also block access to financial data or patient records.
- Connections on SMAs are closed by default, providing "deny all" firewall-style protection.

Protect your enterprise resources with ease

Setup and policy management

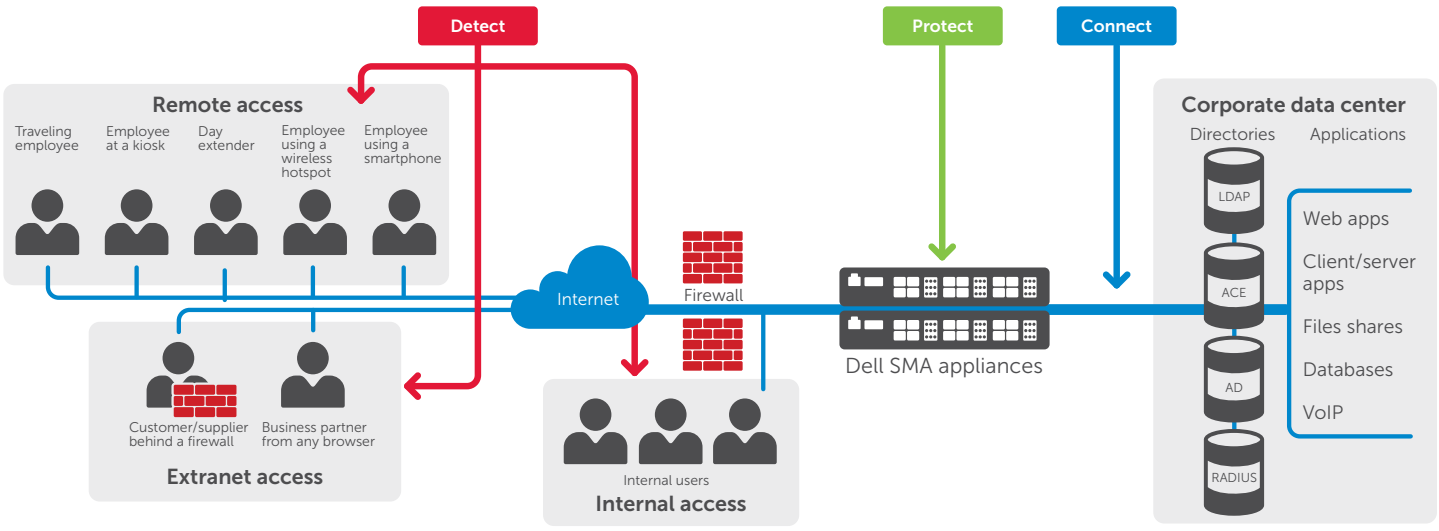
With its context-sensitive help and setup wizard, the SMA solution is easy to deploy. Unified policy consolidates control of all web resources, file shares and client-server resources in a single location, so policy management takes only minutes. Groups can be populated dynamically based on RADIUS, LDAP or Active Directory authentication repositories, including nested groups. Policy replication lets IT easily replicate policy across multiple appliance nodes, either in the same cluster or in a geographically distributed fashion.

Single sign-on and two-factor authentication

SMAs support single sign-on (SSO) and form-based web applications. Moreover, users can easily update their own passwords without IT assistance. One-time password (OTP) support provides a built-in method to generate and distribute secondary factors, enabling 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 SMA 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 SMA advanced reporting audits who accessed what enterprise resources at what time and from which remote location, using standard or custom reports that can be viewed from any web browser.



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

Protect **Dell SMA unified policy** enforces devices access control, ensuring users access only to authorized applications.

Connect **Dell SMA smart access and smart tunneling** ensure easy, secure user access to all network resources.

Dell Secure Mobile Access solutions provide secure access for all users, devices and applications.

Specifications

Performance	E-Class SRA 6000	SMA 6200	E-Class SRA 7000	SMA 7200	E-Class SRA 9000
Concurrent users	Support for up to 250 concurrent users per node or HA pair	Support for up to 2000 concurrent users per node or HA pair	Support for up to 5,000 concurrent users per node or HA pair	Support for up to 10,000 concurrent users per node or HA pair	Support for up to 20,000 concurrent users per node or HA pair
Hardware	**E-Class SRA 6000**	**SMA 6200**	**E-Class SRA 7000**	**SMA 7200**	**E-Class SRA 9000**
Form factor	1U rack-mount	1U rack-mount	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 16.5 x 1.75 in (43 x 41.5 x 4.5 cm)	17.0 x 16.75 x 1.75 in (43.18 x 42.54 x 4.44 cm)	17.0 x 16.5 x 1.75 in (43 x 41.5 x 4.5 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 i5-4570S 2.9GHz	Intel Core2 Duo 2.1 GHz 2 Gb DDR533	Intel E3-1725 v3 3.5GHz	Intel Quad Xeon 2.46 GHz
Network	4 stacked PCIe Gb	(6+1) GbE	6 stacked PCIe Gb	(2) 10 Gb (6 + 1) GbE	(4) 10Gb SFP+ (8) GbE
Power	Fixed power supply	Fixed internal	Dual power supply, hot swappable	Dual power supply, hot swappable	Dual power supply, hot swappable
Input rating	100-240 VAC, 1.2 A	100-240 VAC, 1.1 A	100-240 VAC, 1.5 A, 50-60 Hz; or -36 - -72 VDC, 3.2 A	100-240 VAC, 1.7 A	100-240 VAC, 2.8A
Power consumption	75W	78 W	150W	127 W	320W
MTFB	100,000 hours at 35° C (95° F)	-	100,000 hours at 35° C (95° F)	-	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	110 g, 2 msec				
Regulatory approvals					
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC				
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme				
Key features					
Security					
FIPS & ICSA certification *	Yes				
Encryption	Configurable session length; ciphers: DES, 3DES, RC4, AES, Hashes: MD5, SHA				
VPN protocols	TLS 1, 1.1, 1.2, ESP				
Authentication methods	X.509 digital certificates, server-side digital certificates, client-side digital certificates, RSA SecurID, Dell Defender and other one-time password/two-factor authentication tokens, CAC (common access card) , dual/stacked authentication, Captcha support, username/password				
Directories	Microsoft Active Directory, LDAP (Active Directory, Sun iPlanet, etc.), RADIUS; dynamic groups based on LDAP/AD queries, certificate revocation lists (CRLs)				
Password management	Notification of password expiration and password change from the Dell SMA WorkPlace portal, connect tunnel and Mobile Connect				
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, file system access controls, mobile application VPN access control.				
Dell SMA 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 Micro); cache control (data protection); jailbreak or root detection for iOS and Android devices				
Auto-connect VPN	Network-aware VPN client detects when the device is off campus and auto-reconnects the VPN, bringing it down again when the device returns to a trusted network.				
Access and application support					
Dell SMA 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 that provide access to any TCP- or UDP-based application (leveraging OnDemand Tunnel agent); HTML 5 browser access to Citrix XenDesktop, XenApps and RDP published apps and desktops				
Dell SMA WorkPlace Mobile Access	Customized WorkPlace support for smartphone and tablet browsers; HTML 5 browser access to Citrix XenDesktop, XenApps and RDP published apps and desktops				
Connect tunnel	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 (Refer to SonicWALL Mobile Connect datasheet for complete specifications)				
Management and administration					
Management	The management console provides centralized, web-based management for all access options, end-point control configuration, access control policies, mobile application access control policies, and WorkPlace portal configuration. It offers easy policy replication across multiple appliances and locations, and role-based administration from an at-a-glance management dashboard.				
Auditing	SMA advanced reporting, RADIUS auditing and accounting integration				
Monitoring and logging	User connection monitoring, event alarms. View logs and performance information via Dell SNMP integration, including SMA-specific SNMP management interface base (MIB). Support for central SYSLOG server.				
Scheduler	Enables users to schedule tasks (such as deploying, replicating settings and applying changes) without human intervention				
Mobile management integration	Integrates with leading enterprise mobile management (EMM) products such as Dell EMM, Airwatch and Mobile Iron. When deployed with the Dell Mobile Workspace (DMW) container, the container provides policy-based data loss protection (DLP) to data at rest, and SMA enforces edge proxy protection to core activeSync and HTTP traffic. Through the policy engine end-point control, SMA ensures that only the DMW secure browser and email client gain access to data; all other apps on the device are blocked.				
High availability					
High availability	Support for high-availability two-node clusters with built-in load-balancing and stateful authentication failover				
Other					
IPv6 support	Can authenticate a client with IPv6 internet connectivity and allow the client to interact with resources through the SMA 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				
Browser support	SMA supports all industry-leading browsers, including Internet Explorer, Firefox, Chrome and Safari (supported versions are constantly updated), and supports HTML 5 browser access to Citrix XenDesktop, XenApps and RDP published apps and desktops. Users with HTML5-compatible browser can securely access these applications without risking threats introduced with Java and ActiveX plug-ins required with a legacy browser. Also, users with devices that don't support Java or ActiveX can use an HTML5 browser to access the applications via the SMA web portal.				
	E-Class SRA Virtual Appliance				
Concurrent users	Up to 5000				
Hypervisor	ESG and ESX (version 4.0 and newer), HyperV				
Operating system installed	Hardened Linux				
Allocated memory	2 Gb				
Applied disk size	80 Gb				
Hardware compatibility guide	http://www.vmware.com/resources/compatibility/search.php				

* FIPS &ICSA certifications in process for SMA 6200/7200 appliances

Ordering information

Product	SKU
E-Class SRA 6000	01-SSC-9601
SMA 6200	01-SSC-2300
E-Class SRA 7000	01-SSC-9602
SMA 7200	01-SSC-2301
E-Class SRA 9000	01-SSC-9574
E-Class SRA Virtual Appliance	01-SSC-8468
Dell SMA 5 User License–Stackable	01-SSC-7856
Dell SMA 10 User License–Stackable	01-SSC-7857
Dell SMA 25 User License–Stackable	01-SSC-7858
Dell SMA 50 User License–Stackable	01-SSC-7859
Dell SMA 100 User License–Stackable	01-SSC-7860
Dell SMA 250 User License–Stackable	01-SSC-7861
Dell SMA 500 User License–Stackable	01-SSC-7862
Dell SMA 1,000 User License–Stackable	01-SSC-7863
Dell SMA 2,500 User License–Stackable	01-SSC-7864
Dell SMA 5,000 User License–Stackable	01-SSC-7865
Dell SMA 7,500 User License–Stackable	01-SSC-7948
Dell SMA 10,000 User License–Stackable	01-SSC-7949
Dell SMA 15,000 User License–Stackable	01-SSC-7951
Dell SMA 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. www.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

Datasheet-SMA-US-KS-26075