SMA 1000 series

Delivering robust access security for all remote and mobile workers, through a powerful and granular access control engine

Industry challenges

As businesses move out of the confines of a secure building, managing access to sensitive corporate resources has become a top concern for CISOs. There is a need for an intelligent access security solution that provides policy-based access to guests, customers, partners and employees. Trends such as BYOD, cloud and remote working bring their own unique set of challenges, but fundamental problems remain.

- Unauthorized users gaining access to company data and applications
- Malware infected devices acting as conduits to infect company systems
- Maintaining a reliable service across different mobile platforms with zero impact to business
- Interception of company data in transit on unsecured public Wi-Fi networks
- Compliance with audit and regulatory requirements

SonicWall Solution

The SMA 1000 series is an advanced access security gateway that provides secure access to network and cloud resources from any device.

SMA Overview

Access Control Engine

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data, both on network and in the cloud. For organizations wishing to embrace agile working practices, such as BYOD, flexible working or off shore development, SMA becomes the central enforcement point across them all.

The SMA Access Control Engine ensures risks originating from users, endpoints or applications are evaluated prior to granting data access. Remediation actions, such as session quarantining and alerting are enforced to minimize user frustration and reduce helpdesk calls.

Secure access

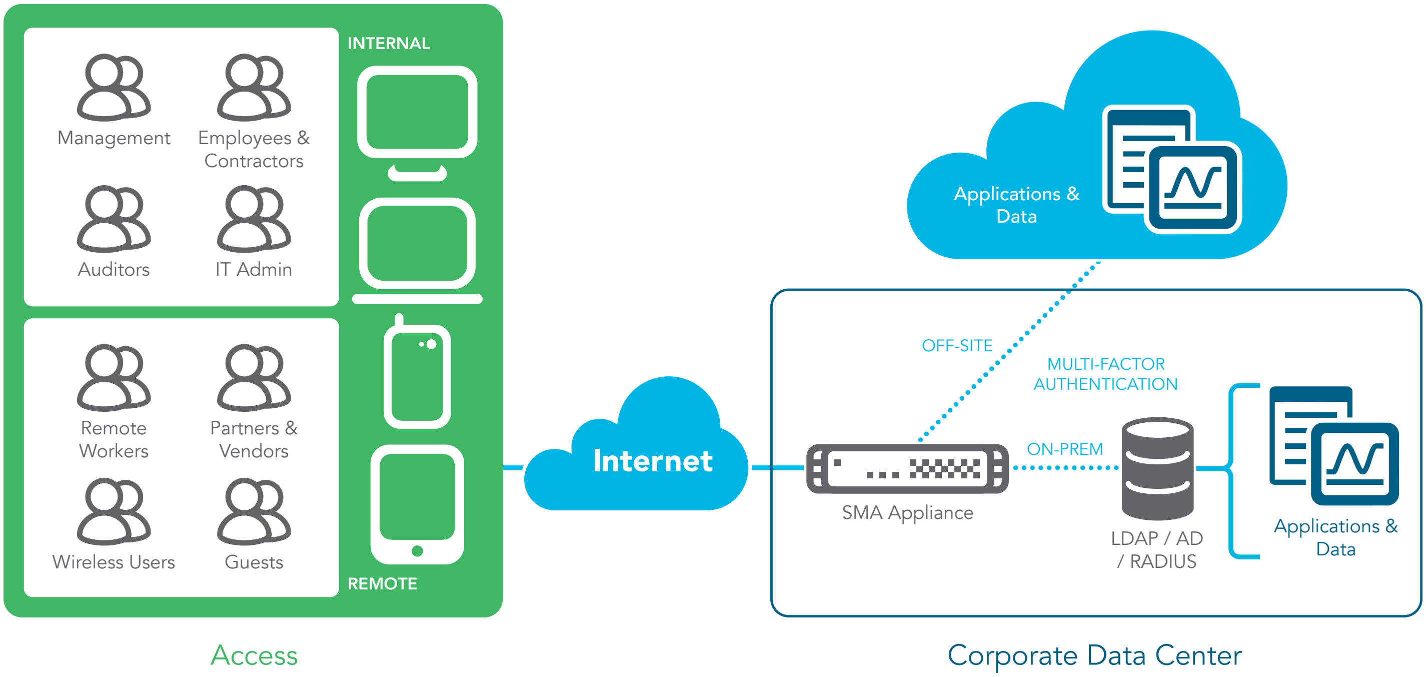
The SMA 1000 series empowers your users with secure remote access to the files, applications and resources they need to be productive with an intuitive client that is easy to deploy on Windows, Mac OSX, Linux, iOS, Android, Chrome OS, Windows Mobile and Kindle Fire devices. SMA delivers best-in-class security to minimize surface threats, while making organizations more secure by supporting latest encryption algorithms and ciphers.

Clientless access security

The SMA OS 12 HTML5 application agents provide a secure window to the most frequently utilized data types, while providing protection from malicious attacks and malware propagation. These feature rich agents keep parity with native application functions, which is critical for a great user experience. Clientless security provides zero-day device support, requires zero need for installation and thus leaves ”zero” footprint, making it perfect for third party or un-managed end point access.

Benefits:

- Defines who has access to what resources through its fine-grained Access Control Engine
- Interrogates every connecting device and grants or denies access based on the health of the endpoint, via the Advanced Endpoint Control module
- Enables traffic optimization and zero impact failover, through its Global High Availability platform
- Ensures data protection and superior security by leveraging the latest ciphers
- Helps meet regulatory compliance with a comprehensive audit trail



SMA solutions provide secure access for all users, devices and applications.

Access management

Continual access enforcement both at the endpoint and at the edge helps secure corporate data from loss and theft. Through its robust and granular policy management engine, SMA ensures confidentiality and integrity of data. SMA validates every user, endpoint and application, before it enters the network, thus safeguarding data and empowering users.

Access Control Engine (ACE)	Administrators grant or deny access based on organizational policies and set remediation actions when quarantining sessions. ACE object-based policy utilizes elements of network, resource, identity, device, application, data and time.
End Point Control (EPC)	EPC allows the administrator to enforce granular access control rules based on the health status of the connecting device. With deep OS integration, many elements are combined for type classification and risk factor assessment. EPC interrogation 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 applicability of signature file update.
App Access Control (AAC)	Administrators can define which specific mobile applications are allowed to access which resources on the network through individual app tunnels. AAC policies are enforced both at the client and server, providing robust perimeter protection.

Superior security

SMA ensures that the highest security stance is maintained for compliance and data protection by utilizing the latest ciphers and strongest encryption available. SonicWall supports the federal, healthcare and finance industries with their regulatory requirements by routinely submitting all hardware models through rigorous industry security testing and certification.

Layer 3 SSL VPN	The SMA 1000 series delivers high performance layer-3 tunneling capabilities to a wide variety of client devices running in any environment.
Cryptography support	Configurable session length Ciphers: AES 128 + 256 bit, Triple DES, RC4 128 bit Hashes: MD5, SHA-256, SHA-1 Elliptic Curve Digital Signature Algorithm (ECDSA)
Advanced ciphers support	SMA 1000 solutions provide strong security stance out-of-the box for compliance, with default configuration ciphers, and administrators can further refine for performance, security strength, or compatibility.
Security certifications	Certified for FIPS 140-2 Level 2, ICSA SSL-TLS

Global High Availability

The SMA 1000 series provides a turnkey solution to deliver a high degree of business continuity and scalability. Global High Availability (GHA) empowers the service owner through a series of tools to deliver a service with zero downtime and allows very aggressive SLAs to be fulfilled.

SonicWall Global Traffic Optimizer (GTO)	SMA offers global traffic load-balancing with zero-impact to users. Traffic is routed to the most optimized and highest performing datacenter.
Dynamic high availability	SMA OS 12 provides active/active configuration for high availability, whether deployed in a single datacenter or across multiple geographically-dispersed datacenters.
Scalable performance	SMA 1000 appliances scale performance exponentially by deploying multiple appliances, thus eliminating a single point of failure. Horizontal clustering fully supports mixing physical and virtual SMA appliances.
Dynamic licensing	User licenses no longer have to be applied to individual SMA appliances. Users can be distributed and reallocated dynamically among the managed appliances, based on user demand.

Central management & monitoring

SMA provides a web-based management platform to streamline appliance management while providing extensive reporting capabilities.

Central Management System (CMS)	CMS provides centralized, web-based management for all SMA capabilities.
Custom Alerts	Alerts can be configured to generate SNMP traps that are monitored by any IT infrastructure Network Management System (NMS).
SONAR monitoring	SonicWall SONAR allows the IT administrator to quickly and easily diagnose access issues, gaining valuable insight for troubleshooting.
SIEM Integration	Real-time output to central SIEM data collectors allows security teams to correlate event driven activities, to understand the end-to-end workflow of a particular user or application. This is critical during security incident management and forensic analysis.
Scheduler	The scheduler enables users to schedule maintenance tasks such as deploying policies, replicating configuration settings and restarting services, without manual intervention

Extensibility

SMA's extensibility program connects our product to complementary security solutions, and empowers our customers, partners and third-parties by integrating with industry leaders and providing powerful APIs.

Management APIs	Management APIs allow full programmatic administrative control over all objects within a single SMA or global CMS environment.
End User APIs	End User APIs provide complete control over all logon, authentication and endpoint workflow.
MDM integration	SMA integrates with leading enterprise mobile management (EMM) products such as Airwatch and Mobile Iron.
Other 3rd party integration	SMA integrates with industry leading vendors such as OPSWAT to provide advanced threat protection

Advanced Authentication

The SMA 1000 series provides a consistent and simple user experience through single sign-on (SSO), while protecting against threat actors and credential harvesting.

Cloud single sign-on	SMA SAML IdP proxy enables SSO via a single portal to both traditional AD username/password and SaaS cloud resources, while enforcing stacked multifactor authentication for added security.
Multifactor authentication	X.509 digital certificates Server-side and client-side digital certificates RSA SecurID, Dell Defender and other one-time password/two-factor authentication tokens, using RADIUS protocol Common Access Card (CAC) Dual or stacked authentication Captcha support, username/password
SAML Gatekeeper Support	SMA provides air gap security to your campus hosted SAML IdP through credential chaining technology in its FIPS certified edge point appliance.
Authentication repositories	SMA provides simple integrations with industry standard repositories for easy management of user accounts and passwords. User groups can be populated dynamically based on RADIUS, LDAP or Active Directory authentication repositories, including nested groups. Common or custom LDAP attributes can be interrogated for specific authorization or device registration verification.
Layer 3-7 application proxy	SMA provides flexible proxy options, for example vendor access can be provided through direct proxy, contractor access through reverse proxy and employee access to Exchange through ActiveSync.
Kerberos Constrained Delegation	SMA provides authentication support using an existing Kerberos infrastructure, which does not need to trust front-end services to delegate a service.

Intuitive user experience

A positive user experience ensures users adopt the strongest security policies and avoid shadow IT scenarios, which pose a serious risk of data loss.

Secure Network Detection (SND)	SMA's 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.
Clientless access to resources	SMA provides secure clientless access to resources via HTML5 browser agents delivering RDP, ICA, VNC, SSH and Telnet protocols.
User portal	The WorkPlace portal provides users with a customizable and intuitive landing page of dynamically personalized resources.
Layer 3 tunneling	Administrators can choose Split-Tunnel or enforce Redirect-All mode with SSL/TLS tunneling and optional ESP fallback for maximum performance.
Session persistence	SMA provides session persistence across different locations without re-authentication.
Mobile OS integration	Mobile Connect is supported on all OS platforms, providing users complete flexibility in mobile device choice.

Feature summary

Client Access

- Layer 3 tunnel
- Split-tunnel and redirect-all
- Auto ESP encapsulation
- HTML5 (RDP/VNC/ICA/SSH)
- Secure Network Detection
- File browser (CIFS/NFS)
- Citrix XenDesktop/XenApp
- VMware View
- On Demand browser tunnel
- Chrome/Firefox extensions
- CLI tunnel support
- Multi client OS

Mobile

- Per app VPN
- App control enforcement
- App ID validation

User Portal

- Branding
- Customization
- Localization
- User defined bookmarks
- Custom URL support
- SaaS application support

Security

- FIPS 140-2
- ICSA SSL-TLS
- Suite B ciphers
- Dynamic EPC interrogation
- Role Based Access Control
- Endpoint registration
- Endpoint quarantine
- OSCP CRL validation
- Cipher selection
- PKI and client certificates
- Forward proxy

Authentication

- LDAP, RADIUS
- Kerberos (KDC)
- NTLM
- SAML IdP gatekeeper
- Biometric device support
- Chained authentication
- Remote password change
- Forms based SSO
- Team ID session persistence
- Auto logon
- Reverse proxy

Access Control

- Group AD
- LDAP attributes
- Continual monitoring

Management

- Dedicated OOB (Serial and Eth)
- Global load balancing
- TCP state replication
- Cluster state failover
- Active/active high availability
- Horizontal clustering scalability
- Centralized management
- Device HTTPS and SSH admin
- SNMP MIBS
- Syslog and NTP
- Configuration rollback
- Burst licensing
- Centralized session licensing
- Event-driven auditing
- Single or multiple FQDNs
- L3-7 Smart Tunnel proxy
- L7 Application proxy
- Central reporting

Integration

- Management REST APIs
- Authentication REST APIs
- TPAM password vault
- EMM and MDM product support
- SIEM product support

Licensing Options

- Subscription (support included)
- Perpetual (support required)

Hardware appliance

SMA 6200 / 7200

SRA EX9000

Performance	SMA 6200	SMA 7200	SRA EX9000
Concurrent sessions / Users	Up to 2,000	Up to 10,000	Up to 20,000
SSL VPN Throughput (at max CCU)	Up to 400 Mbps	Up to 3.75Gbps	Up to 3.75 Gbps
Attributes	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Form Factor	1U	1U	2U
Dimensions	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)	17.0 x 16.5 x 1.75 in (43 x 41.5x 4.5 cm)	27.0 x 18.9 x 3.4 in (68.6 x 48.2x 8.8 cm)
Encryption Data Acceleration (AES-NI)	YES	YES	YES
Dedicated Management Port	YES	YES	YES
SSL Acceleration	YES	YES	YES
Hard Drive	2 X 500 GB SATA	2 X 500 GB SATA	2 X 2TB SATA
Interfaces	6 (6-port 1GE)	8 (6-port 1GE + 2-port 10Gb SFP+)	12 (8-port 1GE + 4-port 10Gb SFP+)
Memory	8GB DDR3	16GB DDR3	32 GB DDR3
TPM chip	YES	YES	NO
Processor	4 cores	4 cores	2 X 4 cores
MTBF	200,064 hours at 25°C (77°F)	233,892 hours at 25°C (77°F)	129,489 hours at 25°C (77°F)
Operations and Compliance	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Power	Fixed power supply	Dual power supply, hot swappable	Dual power supply, hot swappable
Input rating	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A	100-240 VAC, 2.8.5 A
Power Consumption	78 W	127 W	320 W
Environmental	WEEE, EU RoHS, China RoHS		
Non-operating shock	110 g, 2 msec		
Emissions	FCC, ICES, CE, C-Tick, VCCI; MIC		
Safety	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme		
Operating Temperature	0°C to 40°C (32°F to 104° F)		
Certifications	FIPS 140-2 Level 2 with anti-tamper protection		

Virtual appliance specifications

	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper V)
Concurrent sessions	Up to 5000	Up to 250
SSL-VPN throughput (at max CCU)	Up to 1.58 Gbps	Up to 1.2 Gbps
Allocated memory	8 GB	
Processor	4 cores	
SSL acceleration	YES	
Applied disk size	64 GB (default)	Admin Configurable
Operating system installed	Hardened Linux	
Dedicated Management port	YES	

Core SKUs

SMA Appliance	SKU number
SMA 8200v	01-SSC-8468
SMA 6200	01-SSC-2300
SMA 7200	01-SSC-2301
SRA EX9000	01-SSC-9574
50 User CCU	01-SSC-7859
250 User CCU	01-SSC-7861
1,000 User CCU	01-SSC-7863
250 User 3 Year Support	01-SSC-2331
1,000 User 3 Year Support	01-SSC-2337

Optional SKUs

SMA Add-on	SKU Number
CMS Base (up to 3 Appliance)	01-SSC-8535
CMS up to 100 appliances 1yr	01-SSC-8536
50 User Pooled License*	01-SSC-2401
250 User Pooled License*	01-SSC-2403
1,000 User Pooled License*	01-SSC-8539
FIPS Add-on for SMA 7200	01-SSC-2406
FIPS Add-on for SMA 6200	01-SSC-2405
10 DAY 5- 1000 SPIKE FOR SMA 6200	01-SSC-2368

**GTO and SONAR included with pooled licensing*

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-SMA-1000Series-US-KJ-24735

Secure Mobile Access 100 Series

Enable mobile and remote worker productivity while protecting your organization from threats

The SonicWall Secure Mobile Access (SMA) 100 Series 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 mobile devices, the solution includes the intuitive SonicWall Mobile Connect app that provides iOS, Android, Kindle Fire, Windows, Chrome and Mac OS X devices secure access to allowed network resources, including shared folders, client/server applications, intranet sites and email.

Users and IT administrators can download the Mobile Connect app via the Apple App Store, Google Play, Kindle and Microsoft store. The solution also supports clientless, secure browser access, including support for industry standard HTML 5 browsers and thin-client VPN access for PCs and laptops, including Windows, Mac OS X and Linux computers.

To protect from rogue access and malware, the SMA 100 Series appliance connects only authorized users and trusted devices to permitted resources. When integrated with a 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 Clean VPN decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment.

Why you need SMA

The proliferation of mobile devices in the workplace has increased the demand for secure access to mission-critical applications, data and resources. Granting that access offers important productivity benefits to the organization, but introduces significant risks as well.

For example, an unauthorized person might access company resources using a lost or stolen device; an employee's mobile device might act as a conduit to infect the network with malware; or corporate data might be intercepted over third-party wireless networks. Also, loss of business data stored on devices can occur if rogue personal apps or unauthorized users gain access to that data.

Securing these devices is becoming increasingly difficult, as organizations may no longer influence device selection or control device management. Organizations must implement solutions that safeguard access to ensure only authorized users and devices that meet security policy are granted network access, and that company data in-flight and at rest on the device are secure. Unfortunately, this often involves complex multi-box solutions from multiple vendors and adds significantly to the total cost of ownership behind providing mobile access. Organizations are looking for easy-to-use, cost-effective and secure mobile access solutions that address the needs of their increasingly mobile workforces.

Benefits:

- Single access gateway to all network resources, via mobile app, clientless or web-delivered clients, works 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, Windows, Chrome and Mac OS X offers mobile device ease of use
- Context aware authentication ensures only authorized users and trusted mobile devices are granted access
- One-click secure intranet file browse and on-device data protection
- HTML5 enhancements that allow everything to be run from within the context of the browser window
- Adaptive addressing and routing deploys appropriate access methods and security levels
- Setup wizard makes deployment easy
- Easy-to-use "policy wizards" making IT administrators more productive and lowering company's overall TCO
- Efficient object-based policy management of all users, groups, resources and devices
- Web Application Firewall enables PCI compliance
- Geo IP detection and Botnet protection

Features

Single access gateway for mobile app, clientless or web-delivered clients — SMA 100 Series 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 (such as virtual desktop) and back-connect applications (such as VoIP). SMAs are either clientless with browser access to the customizable SMA Workplace portal or use mobile apps or lightweight web-delivered clients, reducing management overhead and support calls.

Common user experience across all operating systems — SMA technology provides transparent access to network resources from any network environment or device. A SMA appliance provides a single gateway for smartphone, tablet, laptop and desktop access and a common user experience across all operating systems — including Windows, Mac OS X, iOS, Android, Kindle, Chrome and Linux — from managed or unmanaged devices.

Mobile Connect app — Mobile Connect app for iOS, Mac OS X, Android, Kindle, Chrome and Windows mobile devices provides 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, Google Play, Microsoft or Kindle store and embedded with Windows 8.1 devices.

HTML5 Enhancements — Provides end-users a rich access experience within their own choice of web browser, which eliminates their need to download, install and maintain additional software on their systems. Everything can be run from within the context of the browser window, making connection to resources very easy and zero day support for all major OSs and browsers.

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

Protects data at rest on mobile devices — Authenticated users can securely browse and view allowed intranet file shares and files from within the Mobile Connect app. Administrators can establish and enforce mobile application management policy.

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

Setup wizard — All SMAs are easy to set up and deploy in just minutes. The setup wizard provides an easy, intuitive "out-of-the-box" experience with rapid installation and deployment.

Policy Wizards — Easy-to-use wizards to deploy policies for OWA, ActiveSync, Outlook Anywhere and Autodiscover. This saves IT administrators considerable time for the most commonly created policies, making them more productive and lowering the company's overall TCO.

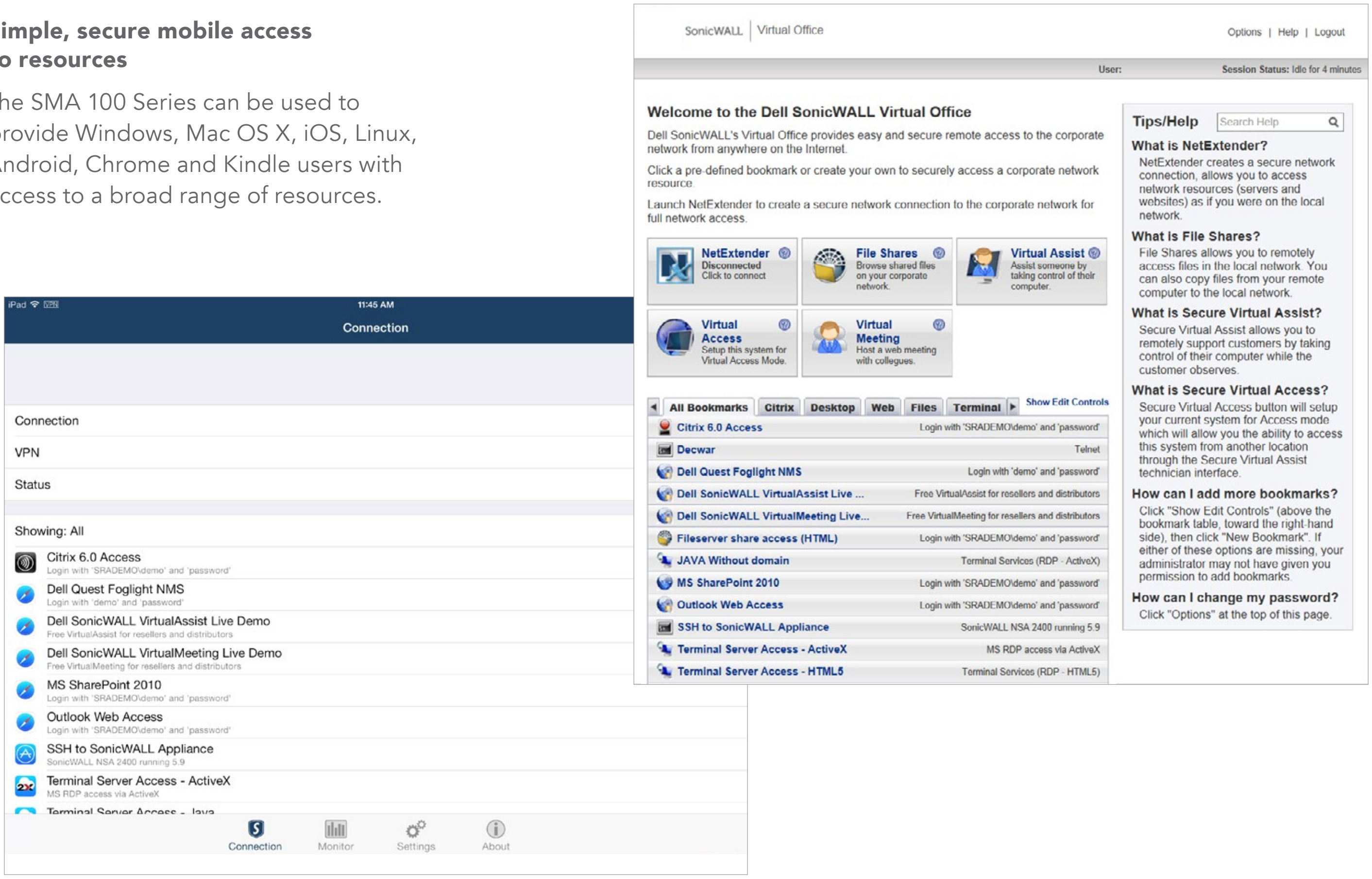
Unified policy — SMA unified policy offers easy, object-based policy management of all users, groups, resources and devices while enforcing granular control based on both user authentication and endpoint interrogation.

Web Application Firewall (WAF) Enhancements — Helping to secure internal web applications from remote users, SonicWall's award winning WAF engine has been enhanced to detect against additional exploits and threats. This allows customers to ensure the confidentiality of data, and internal web services remain uncompromised, should there be malicious or rogue authenticated user access.

Geo IP Detection and Botnet Protection — Grants customers with a mechanism to allow or restrict user access from various geographical locations. Also provides additional protection from compromised endpoint participating in a botnet, further verifying the validity of the connecting device.

Simple, secure mobile access to resources

The SMA 100 Series can be used to provide Windows, Mac OS X, iOS, Linux, Android, Chrome and Kindle users with access to a broad range of resources.


SonicWALL | Virtual Office
Options | Help | Logout
User:
Session Status: Idle for 4 minutes

Welcome to the Dell SonicWALL Virtual Office

Dell SonicWALL's Virtual Office provides easy and secure remote access to the corporate network from anywhere on the Internet.

Click a pre-defined bookmark or create your own to securely access a corporate network resource.

Launch NetExtender to create a secure network connection to the corporate network for full network access.

NetExtender Disconnected Click to connect

File Shares Browse shared files on your corporate network.

Virtual Assist Assist someone by taking control of their computer.

Virtual Access Setup this system for Virtual Access Mode.

Virtual Meeting Host a web meeting with collegues.

Citrix 6.0 Access	Login with 'SRADEMO\demo' and 'password'
Decwar	Telnet
Dell Quest Foglight NMS	Login with 'demo' and 'password'
Dell SonicWALL VirtualAssist Live ...	Free VirtualAssist for resellers and distributors
Dell SonicWALL VirtualMeeting Live...	Free VirtualMeeting for resellers and distributors
Fileserver share access (HTML)	Login with 'SRADEMO\demo' and 'password'
JAVA Without domain	Terminal Services (RDP - ActiveX)
MS SharePoint 2010	Login with 'SRADEMO\demo' and 'password'
Outlook Web Access	Login with 'SRADEMO\demo' and 'password'
SSH to SonicWALL Appliance	SonicWALL NSA 2400 running 5.9
Terminal Server Access - ActiveX	MS RDP access via ActiveX
Terminal Server Access - HTML5	Terminal Services (RDP - HTML5)

Tips/Help

What is NetExtender?
NetExtender creates a secure network connection, allows you to access network resources (servers and websites) as if you were on the local network.

What is File Shares?
File Shares allows you to remotely access files in the local network. You can also copy files from your remote computer to the local network.

What is Secure Virtual Assist?
Secure Virtual Assist allows you to remotely support customers by taking control of their computer while the customer observes.

What is Secure Virtual Access?
Secure Virtual Access button will setup your current system for Access mode which will allow you the ability to access this system from another location through the Secure Virtual Assist technician interface.

How can I add more bookmarks?
Click "Show Edit Controls" (above the bookmark table, toward the right-hand side), then click "New Bookmark". If either of these options are missing, your administrator may not have given you permission to add bookmarks.

How can I change my password?
Click "Options" at the top of this page.

Connection

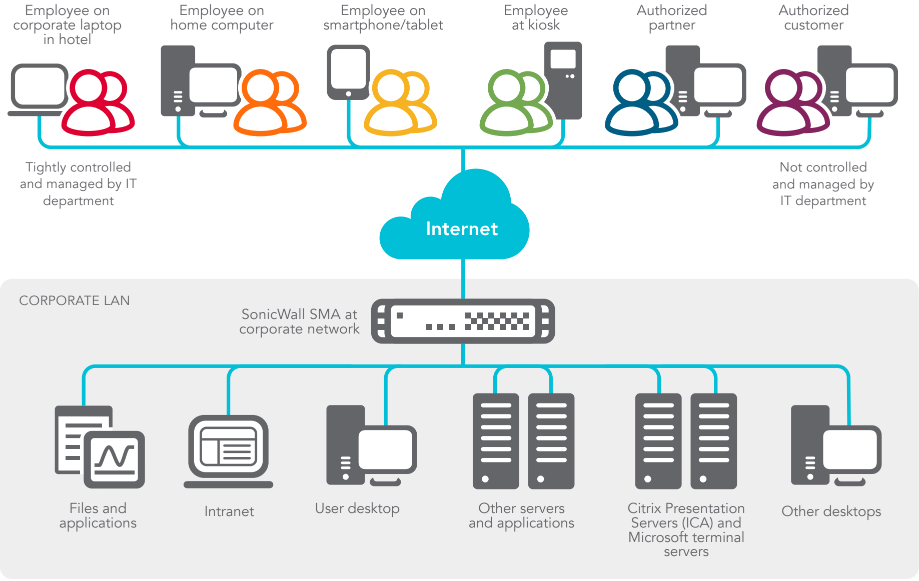
VPN

Status

Showing: All

Citrix 6.0 Access	Login with 'SRADEMO\demo' and 'password'
Dell Quest Foglight NMS	Login with 'demo' and 'password'
Dell SonicWALL VirtualAssist Live Demo	Free VirtualAssist for resellers and distributors
Dell SonicWALL VirtualMeeting Live Demo	Free VirtualMeeting for resellers and distributors
MS SharePoint 2010	Login with 'SRADEMO\demo' and 'password'
Outlook Web Access	Login with 'SRADEMO\demo' and 'password'
SSH to SonicWALL Appliance	SonicWALL NSA 2400 running 5.9
Terminal Server Access - ActiveX	MS RDP access via ActiveX
Terminal Server Access - Java	

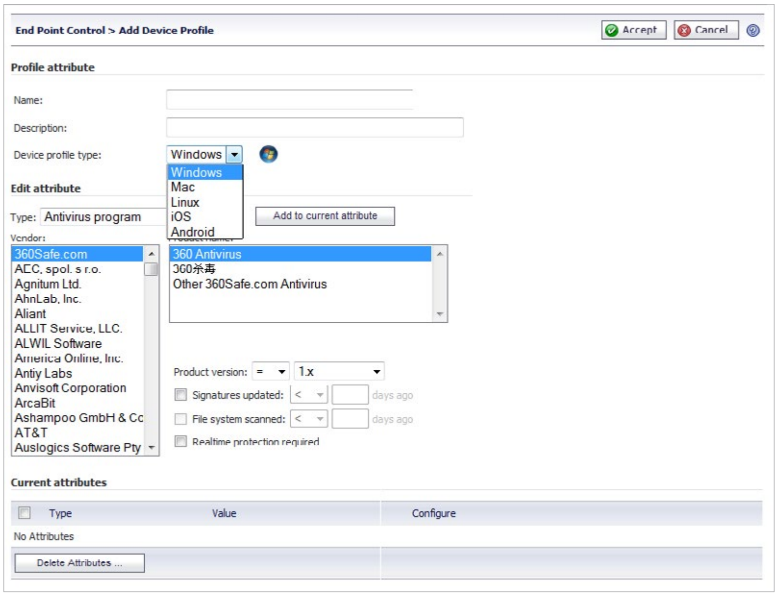
Connection
Monitor
Settings
About


Employee on corporate laptop in hotel
Employee on home computer
Employee on smartphone/tablet
Employee at kiosk
Authorized partner
Authorized customer
Tightly controlled and managed by IT department
Not controlled and managed by IT department
Internet
CORPORATE LAN
SonicWall SMA at corporate network
Files and applications
Intranet
User desktop
Other servers and applications
Citrix Presentation Servers (ICA) and Microsoft terminal servers
Other desktops

Granular access to authorized users

The SMA 100 Series extends secure mobile and remote access beyond managed employees to unmanaged mobile and remote employees, partners and customers by employing policy-enforced fine-grained access controls.

Easy-to-use, cost-effective and secure mobile access that addresses the needs of your increasingly mobile workforce.



End Point Control > Add Device Profile

Profile attribute

Name:

Description:

Device profile type: Windows

Edit attribute

Type: Antivirus program

Vendor: 360Safe.com

Product name: 360 Antivirus

Product version: = 1.x

□ Signatures updated: < days ago

□ File system scanned: < days ago

□ Realtime protection required

Current attributes

□ Type	Value	Configure
No Attributes		

Context-aware authentication

Best-in-class, context-aware authentication grants access only to trusted devices and authorized users. Mobile devices are interrogated for essential security information such as jailbreak or root status, device ID, certificate status and OS versions prior to granting access. Laptops and PCs are also interrogated for the presence or absence of security software, client certificates, and device ID. Devices that do not meet policy requirements are not allowed network access and the user is notified of non-compliance.

Protection of data at rest on mobile devices

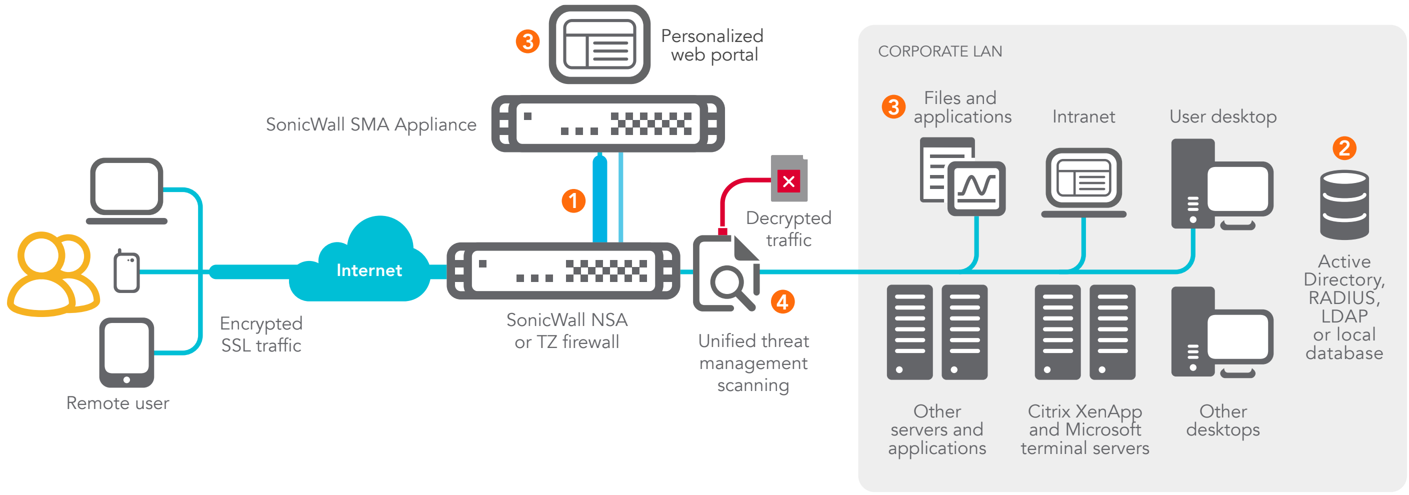
Authenticated Mobile Connect users can securely browse and view allowed intranet file shares and files from within the Mobile Connect app. Administrators can establish and enforce mobile application management policy for the Mobile Connect app to control whether files viewed can be opened in other apps (iOS 7 and newer), copied to the clipboard, printed or cached securely within the Mobile Connect app. For iOS 7 and newer, this allows administrators to isolate business data from personal data stored on the device and reduces the risk of data loss. In addition, if the user's credentials are revoked, content stored in the Mobile Connect app is locked and can no longer be accessed or viewed.

Clean VPN

When deployed with a SonicWall next-generation firewall, Mobile Connect establishes a Clean VPN, an extra layer of protection that decrypts and scans all SSL VPN traffic for malware before it enters the network.

Web Application Firewall and PCI compliance

The SonicWall Web Application Firewall Service offers businesses a complete, affordable, well integrated compliance solution for web-based applications that is easy to manage and deploy. It supports OWASP Top Ten and PCI DSS compliance, providing protection against injection and cross-site scripting attacks (XSS), credit card and Social Security number theft, cookie tampering and cross-site request forgery (CSRF). Dynamic signature updates and custom rules protect against known and unknown vulnerabilities. Web Application Firewall can detect sophisticated web-based attacks and protect web applications (including SSL VPN portals), deny access upon detecting web application malware, and redirect users to an explanatory error page. It provides an easy-to-deploy offering with advanced statistics and reporting options for meeting compliance mandates.


3
Personalized web portal
SonicWall SMA Appliance
1
Decrypted traffic
Remote user
Encrypted SSL traffic
Internet
SonicWall NSA or TZ firewall
4
Unified threat management scanning
CORPORATE LAN
3
Files and applications
Intranet
User desktop
2
Active Directory, RADIUS, LDAP or local database
Other servers and applications
Citrix XenApp and Microsoft terminal servers
Other desktops

1. Incoming traffic is seamlessly forwarded by the SonicWall NSA or TZ Series firewall to the SonicWall SMA appliance, which decrypts and authenticates network traffic.

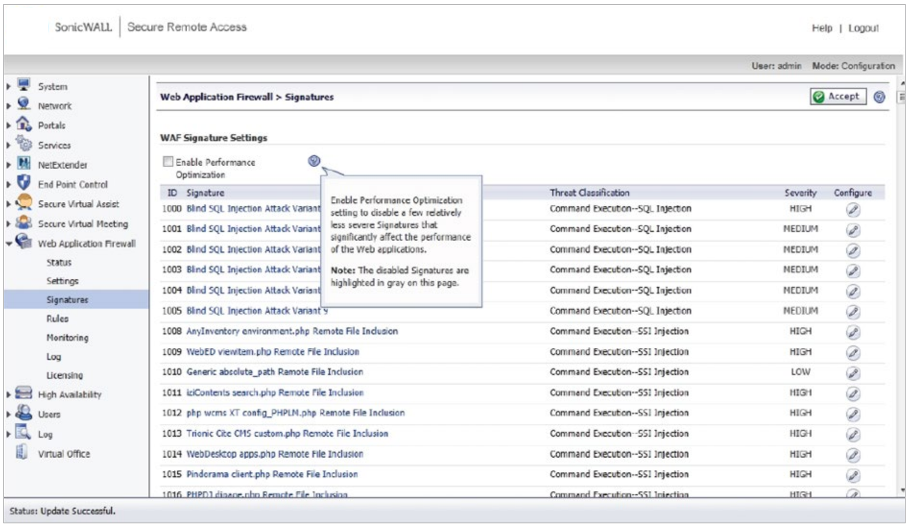
2. Users are authenticated using the onboard database or through third-party authentication methods such as LDAP, Active Directory, Radius, Defender and other two-factor authentication solutions.

3. A personalized web portal provides access to only those resources that the user is authorized to view based on company policies.

4. To create a Clean VPN environment, traffic is passed through to the NSA or TZ Series firewall (running gateway anti-virus, anti-spyware, intrusion prevention, and application intelligence and control), where it is fully inspected for viruses, worms, Trojans, spyware and other sophisticated threats.

Simple to manage

SMA 100 Series solutions feature unified policy and an intuitive web-based management interface that offers context-sensitive help to enhance usability. In addition, multiple products can be centrally managed using the SonicWall Global Management System (GMS 4.0+). Resource access via the products can be effortlessly monitored using the SonicWall Analyzer reporting tool.



Web Application Firewall > Signatures

WAF Signature Settings

☐ Enable Performance Optimization

Enable Performance Optimization setting to disable a few relatively less severe Signatures that significantly affect the performance of the Web applications.

Note: The disabled Signatures are highlighted in gray on this page.

ID	Signature	Threat Classification	Severity	Configure
1000	Blind SQL Injection Attack Variant	Command Execution--SQL Injection	HIGH	✎
1001	Blind SQL Injection Attack Variant	Command Execution--SQL Injection	MEDIUM	✎
1002	Blind SQL Injection Attack Variant	Command Execution--SQL Injection	MEDIUM	✎
1003	Blind SQL Injection Attack Variant	Command Execution--SQL Injection	MEDIUM	✎
1004	Blind SQL Injection Attack Variant	Command Execution--SQL Injection	MEDIUM	✎
1005	Blind SQL Injection Attack Variant 9	Command Execution--SQL Injection	MEDIUM	✎
1008	AnyInventory environment.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1009	WebED viewitem.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1010	Generic absoluta_path Ramote File Inclusion	Command Execution--SSI Injection	LOW	✎
1011	iciContents search.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1012	php wcms XT config_PHPLM.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1013	Trionic Cite CMS custom.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1014	WebDesktop apps.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1015	Pindorama client.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎
1016	PHPD1 dinene.php Remote File Inclusion	Command Execution--SSI Injection	HIGH	✎

Status: Update Successful.

Specifications

SonicWall SMA 100 Series

Performance			
	SMA 200	SMA 400	SMA 500v (virtual)
	Recommended for organizations with 50 or fewer employees	Recommended for organizations with 250 or fewer employees	Recommended for SMB companies with 250 or fewer employees
Concurrent user license	Starts with 5 concurrent users. Additional user licenses available in 5 and 10 user increments	Starts with 25 users. Additional user licences are available in 10, 25 and 100 user increments	User licenses available in 5, 10, and 25 user increments
User capacity[1]	5-included/50-licensable	25-included/250-licensable	5-included/250-licensable
Secure Virtual Assist technicians	30-day trial-included/10-concurrent technicians maximum	30-day trial-included/25-concurrent technicians maximum	30-day trial-included/25-concurrent technicians maximum
Maximum allowable Meeting participants	–	75	75
Unified policy	Yes. Also supports policies which have multiple AD groups		
Logging	Detailed logging in an easy-to-read format, Syslog supported email alerts		
Single-arm mode	Yes	Yes	Yes
SonicWall Secure Virtual Assist or Secure Virtual Access (licensed together)	Connection to remote PC, chat, FTP, session recording and diagnostic tools		
Secure Virtual Meeting[2]	Instantly brings meeting participants together securely and cost-effectively		
IPv6 support	Basic	Basic	Basic
Load balancing	HTTP/HTTPS load balancing with failover. Mechanisms include weighted requests, weighted traffic, least requests		
High Availability	–	Yes	Yes
Application offloading	Yes	Yes	Yes
Web Application Firewall	Yes	Yes	Yes
End Point Control (EPC)	Yes	Yes	Yes
Geolocation-based policies[4]	Yes	Yes	Yes
Botnet filtering[4]	Yes	Yes	Yes
Key features			
Applications supported[3]	• **Web portal access:** Supports HTML5, proxy and application offloading • **Web services:** HTTP, HTTPS, FTP, SSH, Telnet, VNC, Windows® file sharing (Windows SMB/CIFS), OWA 2003/2007/2010 • **Virtual Desktop Infrastructure (VDI):** Citrix (ICA), RDP • **Mobile Connect and NetExtender:** Any TCP/IP based application: ICMP, VoIP, IMAP, POP, SMTP, etc.		
Encryption	ARC4 (128), MD5, SHA-1, SHA-256, SHA-384, SSLv3, TLSv1, TLS 1.1, TLS 1.2, 3DES (168, 256), AES (256), RSA, DHE		
Authentication	Quest Defender, other two-factor authentication solutions, One-time Passwords, Internal user database, RADIUS, LDAP, Microsoft Active Directory and Single Sign On (SSO) for most web based apps, RDP and VNC3		
Multiple domain support	Yes		
Multiple portal support	Yes		
Fine grain access control	At the user, user group and network resource level		
Session security	Inactivity timeouts prevent unauthorized use of inactive sessions		
Certificates	• **Server:** Self-signed with editable common name and imported from third parties • **Client:** Optional client certificates supported		
Cache cleaner	Configurable. Upon logout all cached downloads, cookies and URLs downloaded through the SSL tunnel are erased from the remote computer		
Client support[3]	• **Web portal access:** Internet Explorer, Mozilla, Chrome, Opera, and Safari browsers • **NetExtender:** Windows 2003, 2008, XP/Vista (32-bit and 64-bit), 7 (32-bit and 64-bit), 8 (32-bit and 64-bit), Mac OS X 10.4+, Linux Fedora Core 3+ / Ubuntu 7+ / OpenSUSE, Linux 64-bit • **Mobile Connect:** iOS 4.2 and higher, OS X 10.9 and higher, Android 4.0 and higher, Chrome 43 and higher, Kindle Fire running Android 4.0 and higher and Windows 8.1		
Personalized portal	The remote user sees only those resources that the administrator has granted access to based on company policy		
Management	Web GUI (HTTP, HTTPS), Send syslog and heartbeat messages to GMS (4.0 and higher) SNMP Support		
Usage monitoring	Graphical monitoring of memory, CPU, users and bandwidth usage		

[1] *The recommended number of users supported is based on factors such as access mechanisms, applications accessed and application traffic being sent.*

[2] *Available in conjunction with Secure Virtual Assist for SMA 400 and SRA Virtual Appliances only.*

[3] *Refer to the latest SMA 100 Series release notes and admin guide for supported configurations.*

[4] *Botnet filtering and Geolocation-based policies require an active support contract to be in place on the hardware or virtual appliance.*

SonicWall SMA 100 Series

Hardware		
	SMA 200	SMA 400
Hardened security appliance	Yes	Yes
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console
Processors	x86 main processor	x86 main processor
Memory (RAM)	2 GB	4 GB
Flash memory	2 GB	2 GB
Power supply/input	Internal, 100-240VAC, 50-60MHz	Internal, 100-240VAC, 50-60MHz
Max power consumption	26.9 W	31.9 W
Total heat dissipation	92 BTU	109 BTU
Dimensions	16.92 x 10.23 x 1.75 in 43x26x4.5cm	16.92 x 10.23 x 1.75 in 43x26x4.5cm
Appliance weight	11 lbs 5 kg	11 lbs 5 kgs
WEEE weight	11 lbs 5.3 kg	11 lbs 5.3 kgs
Major regulatory compliance	FCC Class A, ICES Class A, CE, RCM, VCCI Class A, ANATEL, BSMI, UL, cUL, UL Mexico CoC, TUV/GS, CB, MSIP Class A	
Regulatory Model	1RK33-0BB	1RK33-0BC
Environment	32-105° F, 0-40° C Humidity 5-95% RH, non-condensing	
MTBF	7.06 years	6.87 years
	SMA 500v (virtual)	
SMA 500v virtualized environment requirements (Minimum)	Hypervisor: VMWare ESXi and ESX (version 4.0 and newer) Appliance size (on disk): 2 GB Allocated memory: 2 GB	

SMA 200	
5 User	01-SCC-2231
SMA 200 additional users (50 user maximum)	
Add 5 concurrent users	01-SSC-2232
Add 10 concurrent users	01-SSC-2233
SMA 200 support	
SonicWall Dynamic Support	
24x7 for up to 25 users (1-year)	01-SSC-2234

SMA 400	
5 User	01-SSC-2243
SMA 400 additional users (250 user maximum)	
Add 10 concurrent users	01-SSC-2244
Add 25 concurrent users	01-SSC-2245
Add 100 concurrent users	01-SSC-2246
SMA 400 support	
SonicWall Dynamic Support	
24x7 for up to 100 users (1-year)	01-SSC-2247
24x7 for up to 250 users (1-year)	01-SSC-2248

SonicWall SMA 500v (virtual)	
5 User	01-SSC-8469
SMA 500v (virtual) additional users (250 user maximum)	
Add 5 concurrent users	01-SSC-9182
Add 10 concurrent users	01-SSC-9183
Add 25 concurrent users	01-SSC-9184
SMA 500v (virtual) support	
SonicWall Dynamic Support	
24x7 for up to 25 users (1-year)	01-SSC-9191
24x7 for up to 50 users (1-year)	01-SSC-9197

For more information on SonicWall Secure Mobile Access solutions, visit www.sonicwall.com.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

SONICWALL™