# Secure Mobile Access 1000 Series (SMA 6210, 7210, 8200v)

Empowering global enterprises with a secure and advanced remote workforce solution

The SMA 1000 series is designed as an advanced secure access gateway for medium enterprises, multi-national corporations and managed security service providers (MSSPs). The series, which includes the SMA 6210, 7210 and 8200v, feature built-in multi-layer security to protect high-value corporate assets and enable users to work from anywhere and with any devices securely.

For mission-critical infrastructure, the addition of Central Management Server (CMS) for SMA provides business continuity with global traffic optimization, instant capacity upscaling, and dynamic allocation of pooled licenses.

CMS for SMA is also a powerful system that simplifies the management of global network of SMA 1000 clusters.

**SMA 1000 Series Spec Preview.** **View full specs »**

| 5Gbps | 10,000 | Up to 100 SMA 1000s |
|---|---|---|
| Max SSL/TLS Throughput (SMA 7210) | Max Concurrent User Sessions (SMA 7210) | Per CMS Cluster (physical and/ or virtual appliances) |

## HIGHLIGHTS

- Supports VMWare ESXi, Hyper-V, KVM, AWS and Azure for hybrid-cloud deployments
- User-installable clients are available for macOS, Win 10, Linux, ChromeOS, Android and iOS operating systems
- Every device is interrogated by Advanced Endpoint Control (EPC) to prevent malware from entering the network
- Network access is granted only after EPC has verified that the device has the latest OS patches and free of malware.
- Access is limited to only trusted users and devices, using Context-aware Authorization and Multi-Factor Authentication
- Supports clientless Zero-Trust Access via a web-browser for convenient use with any public device.
- Comes standard with secure clientless (web) access to resources via **HTML5** browser agents
- Helps meet regulatory and federal compliance with FIPS 140-2 Level 2 certification
- Emulates in-office experience and maintains strong security posture with Always-on VPN
- Integrates with the SonicWall Capture ATP, cloud-based multi-engine sandbox, to protect against unknown malware.

**Secure anywhere, anytime access based on user and device identity, context and trust.**

sonicwall.com/products

DATASHEET

SonicWall SMA 1000 series provides anytime, anywhere and any device access to mission-critical corporate resources. It offers a granular access control policy engine, context-aware device authorization, application-level VPN and advanced authentication with single sign-on. The built-in Zero-Trust Access protects both user and high-value data from breaches, even in a multi-cloud environment.

### *EMPOWER REMOTE WORKFORCE AND MOBILITY*

For organizations wishing to embrace BYOD, flexible working and securely enabling third-party access, the SMA 1000 series delivers a critical enforcement point. With best-in-class security, it minimizes threat surface, secures valuable corporate assets and ensures user confidentiality even in public hotspots. SMA empowers productivity in minutes. IT administrators can conveniently provision identity-based privileges to end-users, secure BYOD policies to protect their corporate networks and data from rogue access and malware.

### *INTEGRATED ADVANCED SECURITY WITH END-POINT COMPLIANCE (EPC) AND ADVANCED THREAT PROTECTION (ATP)*

The SMA 1000 series offers centralized, granular, policy-based enforcement of remote and mobile access to corporate apps and data. SMA easily ensures consistent security policies across thousands of unmanaged devices in any locations.

The solution delivers a single web portal to authenticate users in a hybrid IT environment. In addition, support for modern multi-factor authentications comes standard. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless.

The installation of a VPN client comes with the Endpoint Control (EPC) engine. EPC ensures risks originating from users, endpoints or applications are evaluated before granting data access. Remediation actions, such as session quarantining and alerting, are enforced to minimize user frustration and reduce helpdesk calls.

Integration with the SonicWall Capture ATP, a cloud multi-engine sandbox, enables SMA to scan all files that users upload while outside the corporate network. The deep inspection of uploaded files ensures other users have the same level of protection from advanced threats (e.g., ransomware or zero-day malware) regardless of work locations.

## SECURE ACCESS FROM UNMANAGED, PUBLIC AND BYOD DEVICES

The SMA 1000 series supports Zero-Trust Access via HTML5 web agents that are compatible with any browser. No VPN client is needed. Clientless or web-access is convenient because it provides instant support for any unmanaged devices.

It also provides a secure user portal to the most frequently used data types, and applies Least Privilege Access security, which permits users and devices to access only what's necessary and nothing more, like the concept of a "need to know basis." By limiting exposure to sensitive areas of the network, organizations can prevent threats from moving laterally, thereby securing their resources without sacrificing operational flexibility.

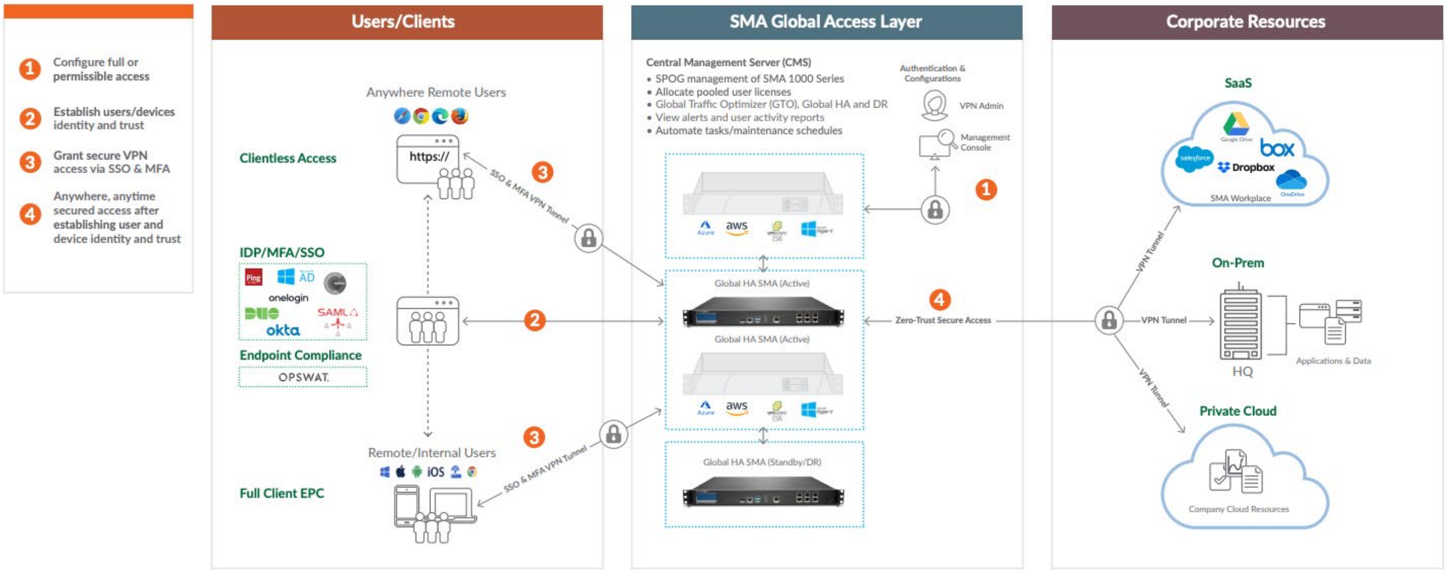
For mobile devices, the SMA 1000 series supports special policies to protect data at rest via SonicWall Mobile Connect. Authenticated users can securely browse, view intranet file shares and collaborate in a completely secure browser environment.

## MANAGE A GLOBAL NETWORK OF SMA 1000 CLUSTERS WITH CMS

SonicWall CMS provides distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy SonicWall SMA 1000 appliances across networks and clouds.

CMS provides a turnkey solution to deliver a high degree of business continuity and scalability with Global High Availability (GHA), and zero downtime during peak hours by dynamically redistributing a pool of user licenses to the managed appliances based on real-time demand.

CMS also acts as a global data store that shares user session state across the mesh network of SMA appliances in an active-active cluster. This allows for session persistence across data centers around the world. In the event of a failover, users do not need to re-enter credentials, so their experience is frictionless, and productivity is not impacted.



## SMA 1000 series feature summary

### Deployment

- Recommended SMA Firmware (v 12.4 onwards)
- Supported Hypervisors (VMware ESXi / Microsoft Hyper-V, KVM)
- Supported Public Clouds (AWS, Azure)

### Client access

- Layer 3 tunnel
- Split-tunnel and redirect-all
- Always On VPN
- Auto ESP encapsulation
- HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)
- Secure Network Detection
- File browser (CIFS/NFS)
- Citrix XenDesktop/XenApp
- VMware View
- On Demand tunnel
- Chrome/Firefox extensions
- CLI tunnel support
- Mobile Connect (iOS, Android, ChromeOS, Win 10, Mac OSX)
- Connect Tunnel (Intel/ ARM-powered Win10, Intel/ ARM-powered macOS, Linux)
- Exchange ActiveSync

### Mobile access

- 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
- TLS 1.3 support
- Suite B ciphers
- Dynamic EPC interrogation
- Role Based Access Control (RBAC)
- Endpoint registration
- Secure File Share (Capture ATP)
- Endpoint quarantine
- OSCP CRL validation
- Cipher selection
- PKI and client certificates
- Forward proxy
- Reverse proxy

### Authentication and identity services

- SAML 2.0
- LDAP, RADIUS
- Kerberos (KDC)
- NTLM
- SAML Identity Provider (IdP)
- Biometric device support
- Face ID support for iOS
- Two-factor authentication (2FA)
- Multi-factor authentication (MFA)
- Chained authentication
- One Time Passcode (OTP) via email or SMS
- Common Access Card (CAC) support
- X.509 certificate support
- Captcha integration
- Remote password change
- Form-based SSO
- Federated SSO
- Session persistence
- Auto logon

### Zero-Trust Security

- User verification (with 2FA, TOTP )
- Devices verification (with VPN per device, pre-login EPC)
- Context verification (with time-based access, continuous user and device monitoring via EPC)
- Least-Access Privilege Policy enforcement (with advanced ACL)
- Segmented App Access  (with HTML5 bookmarks for RDP, HTTPS)

### Access control

- Group AD
- LDAP attributes
- Continual endpoint monitoring

### Management

- Management interface (ethernet)
- Management interface (console)
- HTTPS administration
- SSH administration
- SNMP MIBS
- Syslog and NTP
- Usage monitoring
- Configuration rollback
- Centralized management
- Centralized reporting
- Management REST APIs
- Authentication REST APIs
- RADIUS accounting
- Scheduled tasks
- Centralized session licensing
- Event-driven auditing

### Networking

- IPv6
- Global load balancing
- Server load balancing
- TCP state replication
- Cluster state failover
- Active/passive high availability
- Active/active high availability
- Horizontal scalability
- Single or multiple FQDNs
- L3-7 smart tunnel proxy
- L7 application proxy

### Integration

- 2FA TOTP support (Google Authenticator, MS Authenticator, DUO Security)
- EMM and MDM product support
- SIEM product support
- TPAM password vault
- Microsoft InTune support
- Let's Encrypt support

### Licensing options

- Subscription based license
- Perpetual license with support
- Spike licensing
- Tiered licensing

## Specifications - Physical appliance

| Performance | SMA 6210 | SMA 7210 |
|---|---|---|
| Recommended firmware | Rev 12.4 onwards | Rev 12.4 onwards |
| Concurrent sessions/Users | Up to 2,000 | Up to 10,000 |
| SSL VPN Throughput* (at max CCU) | Up to 1.3 Gbps | Up to 5.0 Gbps |
| Form factor | 1U | 1U |
| 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) |
| Appliance weight | 17.7 lbs (8 kgs) | 18.3 lbs (8.3 kgs) |
| Encryption data acceleration (AES-NI) | Yes | Yes |
| Dedicated management port | Yes | Yes |
| SSL acceleration | Yes | Yes |
| Storage | 2 x 1TB SATA; RAID 1 | 2 x 1TB SATA; RAID 1 |
| Interfaces | (6)-port 1GE, (2) USB, (1) console | (6)-port 1GE, (2)-port 10Gb SFP+, (2) USB, (1) console |
| Memory | 8GB DDR4 | 16GB DDR4 |
| TPM chip | Yes | Yes |
| Processor | 4 cores | 4 cores |
| MTBF (@ 25°C or 77°F) in hours | 70,127 | 129,601 |

| Operations and Compliance | SMA 6210 | SMA 7210 |
|---|---|---|
| Power | Fixed power supply | Dual power supply, hot swappable |
| Input rating | 100-240 VAC, 1.1 A | 100-240 VAC, 1.79 A |
| Power consumption | 77 W | 114 W |
| Total heat dissipation | 264 BTU | 389 BTU |
| 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) | |
| FIPS certification | FIPS 140-2 Level 2 with anti-tamper protection | |

## Specifications - Virtual appliance

| | SMA 8200v (ESX/ ESXi/ Hyper-V/ KVM) |
|---|---|
| Recommended firmware | Rev 12.4 onwards |
| Concurrent sessions | Up to 5000 |
| SSL-VPN throughput* | Up to 1.58 Gbps |
| Allocated memory | 8 GB |
| Processor | 4 cores |
| SSL acceleration | Yes |
| Recommended disk size | 240 GB |
| Operating system installed | Hardened Linux |
| Dedicated management port | Yes |

* Throughput performance may vary based on deployment and connectivity. Published numbers are based on internal lab conditions. SMA 8200v on Hyper-V scales up to 5000 concurrent sessions and provides up to 1.58 Gbps SSL-VPN throughput when running SMA OS 12.1/ 12.4 with Windows Server 2016/ 2019

## PARTNER ENABLED SERVICES

**Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at:**

www.sonicwall.com/PES

**To learn how you can be more successful in maintaining a healthy access security environment while achieving zero downtime, visit:**

sonicwall.com/products/remote-access

## About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

**SonicWall, Inc.**
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
**www.sonicwall.com**

**© 2021 SonicWall Inc. ALL RIGHTS RESERVED.**

*SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.*