

# What Secure Mobile Access Solution Is Right for You?

Understand how the SMA 1000 series fits your organization

## ABSTRACT

*The modern workforce is increasingly mobile, which can mean more flexibility, more growth, and more employee satisfaction. But it also means more devices, more policies, and more threats. SonicWall Secure Mobile Access (SMA) supports secure remote access to corporate resources hosted on-premises, in the cloud, and hybrid data centers, empowering your distributed workforce without increasing risk to your enterprise. But which SMA Series solution is right for your organization? This solution brief outlines the parameters of the SMA 1000 Series and how it is best utilized.*

## Introduction

Whether for ensuring business continuity or enhancing workforce retention and productivity, more organizations are embracing mobility, work-at-home, and flextime for their employees. To achieve business goals with a mobile and remote workforce, having a robust, reliable, and secure VPN service has never been more critical. Enter the SonicWall SMA 1000 Series, best for large enterprises and federal establishments (1,000+ employees) where granular access policy configuration, centralized management and reporting, scalability, and FIPS 140-2 compliance make this a successful enterprise-class solution.

## SMA 1000 – An Advanced VPN Solution For Thousands Of Users

The SMA 1000 Series was geared for large, distributed enterprises as well as federal installations where FIPS, Common Criteria, and other certifications are required. Also, the SMA 1000 series facilitates scalability through a Central Management Server (CMS), where clusters of SMA 1000 appliances can be configured and managed to accommodate large deployments. The SMA 1000 series easily handles the inflow of remote users on large, distributed networks by enabling organizations to scale up to a million remote VPN users. Additional enterprise-type features include global load balancing, SIEM support, management APIs, application ID validation, SSL and encryption data acceleration, and more.

## Enterprise-Grade Solution For Large, Distributed Organizations Including Federal Establishments

Consider the following for an SMA 1000 implementation:

- A large enterprise with thousands of users
- The need for a granular access policy engine
- Centralized management and reporting
- Scalability
- Zero downtime
- High availability
- Certification requirements – FIPS, Common Criteria, and DoDIN APL
- A hybrid-IT environment with on-premises assets



## SonicWall Central Management Server (CMS) – A Powerful SMA 1000 Management And Reporting Tool

SonicWall CMS gives organizations a single administrative user interface to manage multiple SMA 1000 deployments regardless of location. CMS does not require dedicated hardware and can be deployed in your private cloud as a virtual appliance, or on a public cloud using Bring Your Own License (BYOL) on AWS and Microsoft Azure. Some Examples of the many benefits of CMS are outlined here:

### Zero Impact Failover

Universal session persistence provides a high-performance, low-latency failover in a global high availability cluster. If an SMA appliance goes offline, users do not need to re-enter their credentials for login, thereby providing a frictionless user experience and improving workforce productivity.

### Dynamic User Licensing

User licenses no longer must be applied to individual SMA appliances. CMS can manage a pool of user licenses and dynamically allocate them among managed appliances based on real-time user demand. Customers that are globally distributed will benefit from the fluctuating demands for user licenses due to time differences as CMS reallocates licenses from geo-locations where usage has fallen due to off-work/night hours.

### Live Monitoring

The CMS dashboard provides a single console view for IT administrators to monitor the health of the entire SMA ecosystem and view useful information like network activity, license, capacity usage, etc. Administrators can customize the dashboard, visualize the data, and generate ad hoc reports with ease using the intuitive interface.

### Automated Maintenance

CMS comes with a built-in scheduler that enables IT administrators to automate maintenance tasks like deploying policies, replicating configuration settings, rolling out firmware patches or upgrades, and restarting services, without manual intervention.

### Conclusion

SonicWall SMA 1000 Series is geared for large, distributed enterprises where scalability, granular policy configuration, zero downtime, and high availability are a must. The SMA 1000 series is also designed for federal installations where regulatory compliance is required. Secure Mobile Access 1000 is an enterprise-grade VPN solution with centralized policy administration that covers reporting and live monitoring and supports thousands of users. To learn how you can be more successful in maintaining a healthy access security environment while achieving zero downtime, visit [www.sonicwall.com/products/secure-mobile-access](http://www.sonicwall.com/products/secure-mobile-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](http://www.sonicwall.com).

---

### SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035

Refer to our website for additional information.

[www.sonicwall.com](http://www.sonicwall.com)

SONICWALL®

#### © 2022 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.