

SonicWall Mobile Connect

Simple, policy-enforced secure access to mission-critical applications and data for iOS, OS X, Android, Chrome OS, Kindle Fire and Windows mobile devices.

Give your employees safe, easy access to the data and resources they need to be productive from a range of devices, including iOS, OS X, Android™, Chrome OS, Kindle Fire and Windows. At the same time, ensure that the corporate network is protected from mobile security threats.

The SonicWall™ Mobile Connect™ application works in combination with SonicWall Secure Mobile Access (SMA) or next-generation firewall appliances. Mobile workers simply install and launch the Mobile Connect application on their iOS, OS X, Android, Chrome OS or Windows mobile device to establish a secure connection to an SMA or next-generation firewall appliance. The encrypted SSL VPN connection will protect traffic from being intercepted and keep in-flight data secure. Context-aware authentication ensures only authorized users and trusted devices are granted access.

Behind the scenes, IT can easily provision and manage access policies via SonicWall appliances through a single management interface, including restricting VPN access to a set of trusted mobile apps allowed by the administrator. Plus, the SonicWall solution integrates easily with most back-end authentication systems, including two-factor authentication, so you can efficiently extend your preferred authentication practices to your mobile workers.

Features and benefits

Ease of use

iOS, OS X, Windows 10, Android, Chrome OS and Kindle users can

easily download and install the Mobile Connect app via the App Store™, Google Play, Chrome Web Store, Amazon App Store, or Windows Store. For Windows 8.1 mobile device users, Mobile Connect is embedded in the Windows 8.1 operating system so there is no need to download and install another VPN client app.

Centralized policy management

IT can provision and manage mobile device access via SonicWall appliances — including control of all web resources, file shares and client-server resources — through a single management interface. Unlike other VPN solutions, the SonicWall solution allows you to quickly set role-based policy for mobile and laptop devices and users with a single rule across all objects; as a result, policy management can take only minutes instead of hours.

Verification of both user and device

A Mobile Connect user is granted access to the corporate network only after the user has been authenticated and mobile device integrity has been verified. End Point Control can determine whether an iOS device has been jailbroken or an Android device has been rooted, as well as whether a certificate is present or the OS version is current, and then reject or quarantine the connection as appropriate.

Easy access to appropriate resources

iOS, Android, Chrome OS, Kindle and Windows mobile devices can connect to all allowed network resources, including web-based, client/server, server-based, host-based and back-connect

Benefits:

- Ease of use
- Centralized policy management
- Verification of both user and device
- Easy access to appropriate resources
- Malware protection
- Mobile device registration and authorization management
- Per-application VPN
- One-click secure intranet file browsing and on-device data protection
- Auto-launch VPN
- Easy integration
- Application intelligence and control

Provide fast, secure mobile access through an intuitive, easy-to-use app that is simple to install and launch on both smartphones and tablets.

Specifications compatibility

SonicWall SMA and Next Generation Firewall

TZ, NSA, E-Class NSA or Super Massive 9000 Series appliances running SonicOS 5.9, 6.2 or higher

SMA 100 Series/SRA appliances running 7.5 or higher

SMA 1000 Series/E-Class SRA appliances running 10.7 or higher

SonicWall Mobile Connect

Devices running iOS version 7.0 or higher

Devices running OS X 10.9 or higher

Devices running Android 4.1 or higher

Kindle Fire devices based on Android 4.1 or higher

Devices running ChromeOS 45 or higher

Devices running Windows 8.1

Devices running Windows Phone 8.1

Devices running Windows 10

applications. 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.

Malware protection

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.

Mobile device registration and authorization policy management

With Mobile Connect and Secure Mobile Access OS (versions 11.0 and above) for Secure Mobile Access 1000 Series appliances, prior to granting network access, if a mobile device has not previously registered with the SMA appliance, the user is presented with a 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 policy are customizable by the administrator.

Per-application VPN

Mobile Connect in combination with Secure Mobile Access OS (versions 11.0 and above) for Secure Mobile Access 1000 Series appliances, enables administrators to establish and enforce policies to designate which apps on a mobile device can be granted VPN access to the network. This ensures that only authorized mobile business apps utilize VPN access. Mobile Connect 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.

One-click Secure Intranet File Browse and On-Device Data Protection

Protect company 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 for the Mobile Connect app to control whether files viewed can be opened in other apps, copied to the clipboard, printed or cached securely within the Mobile Connect app. For iOS devices, 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.

Auto-launch VPN

URL control allows apps that require a VPN connection for business (including Safari) to create a VPN profile and automatically initiate or disconnect Mobile Connect on launch (requires compatible server firmware). In addition, for iOS or OS X devices, to simplify use when a secure connection is required, VPN on Demand automatically initiates a secure SSL VPN session when a user requests internal data, applications, websites or hosts.

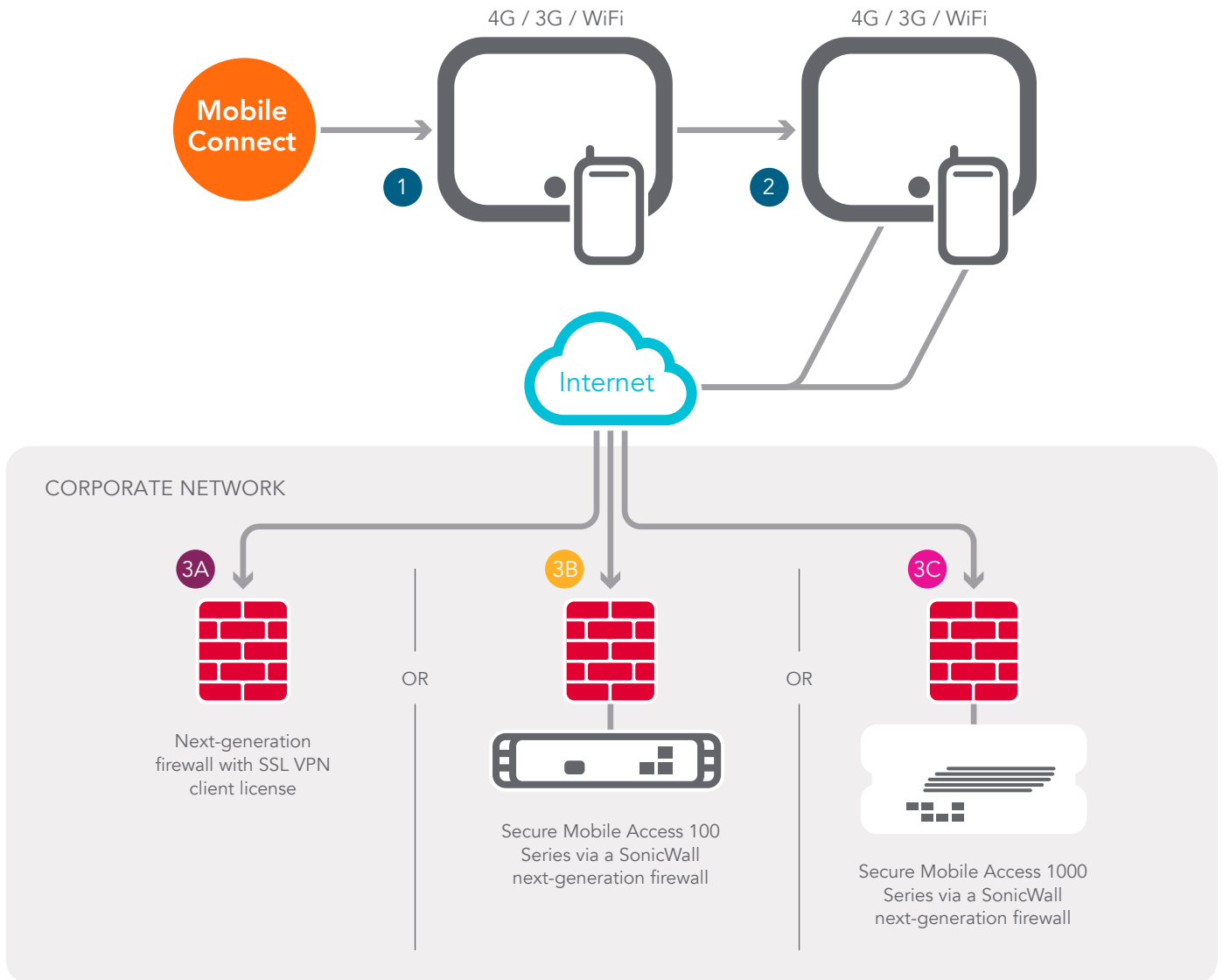
Integration with existing authentication solutions

The SonicWall solution supports easy integration with most back-end authentication systems, such as LDAP, Active Directory and Radius, so you can efficiently extend your preferred authentication practices to your mobile workers. For increased security, you can enable one-time password generation and easily integrate with two-factor authentication technologies.

Application intelligence and control

When deployed with a next-generation firewall, IT can easily define and enforce how application and bandwidth assets are used.

Software Access



- 1 Download and install SonicWall Mobile Connect onto mobile device.
- 2 Create a connection profile to connect to your corporate network.
- 3A Connect to a SonicWall next-generation firewall.
Benefits: Provides DPI scanning for malware as well as application intelligence and control.
- 3B Connect to a SonicWall Secure Mobile Access 100 Series appliance via a SonicWall next-generation firewall.
Benefits: Provides DPI scanning for malware plus end point control to quarantine or reject connections from jailbroken or rooted mobile devices.
- 3C Connect to a SonicWall Secure Mobile Access 1000 Series appliance via a SonicWall next-generation firewall.
Benefits: Provides DPI scanning for malware, end point control to quarantine or reject connections from jailbroken or rooted mobile devices. Also, enables administrators to restrict VPN access to an allowed set of trusted mobile apps, and manage enforced BYOD security policy terms.

Features	iOS	OS X/ Mac	Android	Kindle Fire	Windows 8.1	Windows Phone 8.1	Windows 10	Chrome OS
App distribution	App Store	Mac App Store	Google Play	Amazon App Store	In box	Windows Phone Store	Windows Store	Chrome Web Store
Layer-3 VPN connectivity (SSL VPN)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connect on demand	Yes ¹	Yes ¹	—	—	Yes	MDM Only	MDM/ PowerShell	Yes
Configurable trusted networks	Yes ¹	Yes ¹	—	—	Yes	Yes	Yes	—
Network awareness	Yes ¹	Yes ¹	Yes ¹	Yes ¹	—	—	—	—
Credential caching	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Touch ID/Fingerprint support	Yes ²	—	Yes ²	—	—	—	—	—
URL control	Yes	Yes	Yes	Yes	—	—	—	—
Basic authentication (Username>Password)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two-Factor Authentication (Dell Defender\OTP\RADIUS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Client certificate authentication	Yes ³	Yes ³	Yes ³	Yes ³	Yes	Yes	Yes	—
Password change	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows domain SSO for VPN	—	—	—	—	Yes	Yes	Yes	—
Split-tunnel/Tunnel-all routing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPv6 support	Yes ⁴	Yes ⁴	Yes ⁴	Yes ⁴	Yes ⁴	Yes ⁴	Yes ⁴	—
Compression of data over VPN	Yes ³	Yes ³	Yes ³	Yes ³	Yes ³	Yes ³	Yes ³	Yes ³
ESP Mode (UDP transport)	Yes ¹	Yes ¹	Yes ¹	Yes ¹	—	—	—	—
Network conflict resolution	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹	Yes ¹
End Point Control	Jailbreak, Certificate, OS version, DeviceID ³	DeviceID, OS version, Client certificate ¹	Root, Certificate, OS version, DeviceID, Anti-Virus software ³	Root, Certificate, OS version, DeviceID, Anti-Virus software	DeviceID, OS version ¹	DeviceID, OS version ¹	DeviceID, OS version ¹	DeviceID, Chrome OS version ¹
File Reader/ Bookmarks	Yes ²	—	Yes ²	Yes ²	—	—	—	—
RDP bookmarks	2X RDP, Microsoft Remote Desktop for RDP	—	2X RDP, Remote RDP Lite/ Enterprise, Microsoft Remote Desktop for RDP	2X RDP, Microsoft Remote Desktop for RDP	—	—	—	—
Citrix receiver bookmarks	Yes ²	—	Yes ²	Yes ²	—	—	—	—
VNC bookmarks	Remoter VNC	—	android-vnc-viewer	—	—	—	—	—
Web bookmarks	Safari, Chrome	—	Any browser—configured in Android system settings	Silk Browser	—	—	—	—
Terminal bookmarks	iSSH, Server Auditor for SSH	—	ConnectBot, JuiceSSH	JuiceSSH	—	—	—	—
Native HTML5 Bookmarks	RDP, VNC, SSH, Telnet ²	—	RDP, VNC, SSH, Telnet ²	—	—	—	—	—
MDM management of VPN connection profiles	Yes	—	—	—	Yes	Yes	Yes	Google Mgmt Console

¹This feature is supported on the E-Class SRA/SMA 1000 series appliances only. Please refer to the product release notes for the specific software version required to support this feature.

²This feature is supported on the SRA/SMA 100 series appliances only.

³This feature is supported on the SRA/SMA 100 series and E-Class SRA/SMA 1000 series appliances only. Please refer to the product release notes for the specific software version required to support this feature.

⁴This feature is supported on the SRA/SMA 100 series, E-Class SRA/SMA 1000 series and Next-Generation Firewall appliances. Please refer to the product release notes for the software specific version required to support this feature.

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

© 2017 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.
DataSheet-MobileConnectSMA200_400-US-VG-26866

