Mobile Connect

Simple, policy-enforced secure access to mission-critical applications and data for iOS, Android and Windows 8.1 mobile devices

Organizations have reaped significant productivity gains by giving employees easy, fast access to enterprise email and calendar apps from smartphones and tablets. Now, users are increasingly demanding that IT extend support to include access to mission-critical enterprise applications, data and resources. Granting that access offers important 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 or mobile services used by mobile workers.

With the SonicWALL™ Mobile Connect™ application, in combination with Dell SonicWALL Secure Remote Access (SRA) or next-generation firewall appliances, you can give your employees safe, easy access to the data and resources they need to be productive from a range of devices, including iOS, Android™ and Windows 8.1, while ensuring that the corporate network is protected from mobile security threats.

With the Dell solution, mobile workers simply install and launch the Mobile Connect application on their iOS or Android mobile device, or simply launch it from their Windows 8.1 device, to establish a secure connection to an SRA 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 Dell SonicWALL appliances through a single management interface. Plus, the Dell 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.

Benefits:

- Delivers secure SSL VPN connection and granular, policy-enforced access control to resources
- Easy for iOS and Android users to download and install, and already embedded in the Windows 8.1 OS
- Context aware authentication ensures only authorized users and trusted mobile devices are granted access.
- Offers easy mobile access to authorized resources with pre-configured bookmarks
- Centralized policy management reduces administration time from hours to minutes
- Automatically initiates secure SSL VPN sessions when appropriate,
- Decrypts and scans all SSL VPN traffic to block malware before it enters the network when deployed with a next-generation firewall.

Features and benefits

Ease of use—iOS and Android users can easily download and install the Mobile Connect app via the App Store℠ or Google Play; 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 Dell SonicWALL appliances—including control of all web resources, file shares and client-server resources—through a single management interface. Unlike other VPN solutions, the Dell 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 (available only on the E-Class SRA Series) 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.

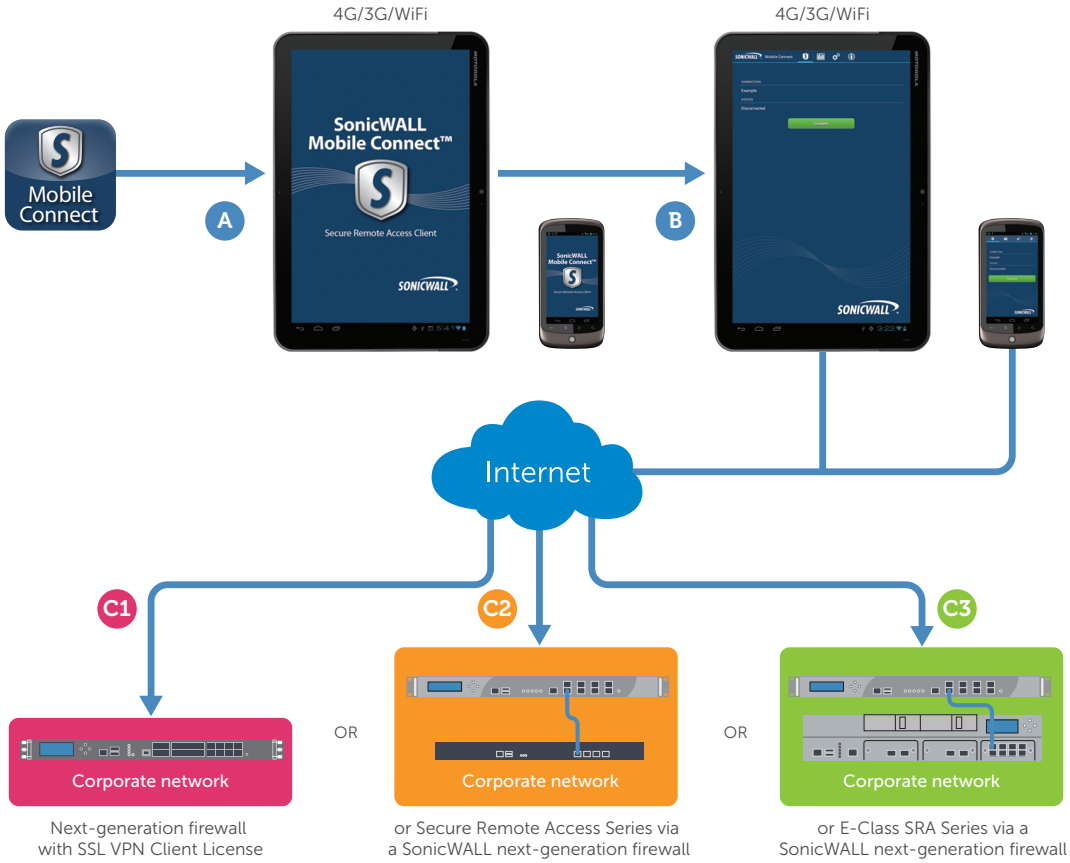
Easy access to appropriate resources—IOS, Android and Windows 8.1 mobile devices can connect to all allowed network resources, including web-based, client/server, server-based, host-based and back-connect applications.
Once a user and device are verified, Mobile Connect offers pre-configured bookmarks for one-click access to corporate applications and resources for which the user and device has privileges.

Malware protection—When deployed with a Dell 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.

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 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, web sites or hosts.

Integration with existing authentication solutions—The Dell 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.



A Download and install SonicWALL Mobile Connect onto smartphone or tablet.

B Create a connection profile to connect to your corporate network.

C1 Connect to a Dell SonicWALL next-generation firewall.
Benefits: Provides DPI scanning for malware as well as application intelligence and control.

C2 Connect to a Dell SonicWALL Secure Remote Access appliance via a Dell SonicWALL next-generation firewall.
Benefits: Provides DPI scanning for malware.

C3 Connect to a Dell SonicWALL E-Class Secure Remote Access appliance via a Dell 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.

.

Features

	iOS	Android	Windows 8.1
App distribution	App Store	Google Play	In box
Layer-3 VPN connectivity (SSL VPN)	Yes	Yes	Yes[5]
Connect on demand	Yes[1]	No	Yes
Configurable trusted networks	Yes[1]	No	Yes
URL control	Yes	Yes	No
Basic authentication (Username\Password)	Yes	Yes	Yes
Two-Factor Authentication (Dell Defender\OTP\RADIUS)	Yes	Yes	Yes
Client certificate authentication	Yes[1]	Yes[1]	Yes
Password change	Yes	Yes	Yes
Windows domain SSO for VPN	No	No	Yes
Split-tunnel\Tunnel-all routing	Yes	Yes	Yes
IPv6 support	Yes[4]	Yes[4]	Yes[4]
SSLv3.0\TLS 1.0, 1.1, 1.2	Yes[3]	Yes[3]	Yes[3]
Compression of data over VPN	Yes[1]	Yes[1]	Yes[1]
ESP Mode (UDP transport)	Yes[1]	Yes[1]	No
Network conflict resolution	Yes[1]	Yes[1]	Yes[1]
End Point Control[1]	Jailbreak, Certificate, OS version, DeviceID	Root, Certificate, OS version, DeviceID, Anti-Virus software	Limited
RDP bookmarks	Dell Wyse Pocket Cloud Pro, 2X RDP	Dell Wyse Pocket Cloud Pro, 2X RDP, Remote RDP Lite/Enterprise	No
Citrix receiver bookmarks	Yes[2]	Yes[2]	No
VNC bookmarks	Remoter VNC	Dell Wyse Pocket Cloud Pro, Android-vnc-viewer	No
Web bookmarks	Safari, Chrome	Any browser—configured in Android system settings	No
Terminal bookmarks	iSSH	ConnectBot	No
MDM management of VPN connection profiles	Yes	No	Yes

[1] This feature is supported on the E-Class SRA appliances only. Please refer to the product release notes for the specific software version required to support this feature. [2] This feature is supported on the SMB SRA appliances only. [3] This feature is supported on the SMB SRA and E-Class SRA appliances only. Please refer to the product release notes for the specific software version required to support this feature. [4] This feature is supported on the SMB SRA, E-Class SRA and next-generation firewall appliances. Please refer to the product release notes for the software-specific version required to support this feature. [5] For the E-Class SRA appliances please refer to the product release notes for the specific software version required to support this feature.

Specifications

Dell SonicWALL SRA and next-generation firewall specifications compatibility:

TZ, NSA or E-Class NSA appliance running SonicOS 5.8.1.0 or higher

SRA appliances running 5.5 or higher

E-Class SRA appliances running Aventail 10.5.4 or higher

SonicWALL Mobile Connect specifications compatibility:

Devices running iOS version 6.0 or higher

Devices running Android 4.0 and higher

Devices running Windows 8.1

Software access

Available for download from from Google Play

ANDROID APP ON Google play

Available for download from the App Store

Available on the App Store

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

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.

DSW 561-09/13