PULSE SECURE FOR GOOGLE ANDROID

Product Overview

In addition to enabling network and resource access for corporate managed mobile devices, many enterprises are implementing a "Bring Your Own Device" policy that gives authorized users personal device access as well. With a surge in malware developed to attack Google Android mobile devices, enterprises and service providers need a way to secure these devices now more than ever. Pulse Secure for Google Android enables comprehensive network connectivity via SSL VPN, mobile device integrity, secure cloud access, on-device mobile security, secure mobile device management, and identity-based access control, empowering enterprises and service providers to allow secure network, cloud and data access for personal and corporate managed Android-based smartphones and tablets.

Product Description

Pulse Secure enables Google Android devices to be secured, connected, and managed by enterprises within a corporate environment, and allows service providers to offer mobile device security, connectivity, and device and application management as managed services to their consumer, small and medium-sized business and enterprise subscribers. It enables secure, mobile remote network and cloud access via SSL VPN, identity- and role-based application and data access, device integrity, on-device mobile security, and secure mobile device management and control for Google Android devices. Key components of Pulse Secure and the Pulse Secure Mobile Security Suite *connect, protect, and manage* Android devices in any environment.

Connect Securely with Mobile Remote Access

Pulse Secure delivers secure, SSL-based, mobile remote access to web-based internally hosted and cloud-based applications for all Google Android devices, as well as full Layer 3 VPN tunneling for mobile devices running Google Android 4.0 (Ice Cream Sandwich) and other select Android devices[1]. This enables authenticated and authorized mobile device users to access corporate resources such as intranet Web portals and clouds, and applications such as Remote Desktop Protocol (RDP), voice over IP (VoIP), and custom enterprise apps from their Android devices, just as they would from their laptop or other computing device. It also delivers robust protection for sensitive personal and corporate data in transit from the mobile device to the network or cloud, transmitting the data through a tunnel safe from hackers or other threats because it is secured by government-level encryption. Administrators can enforce a consistent range of authentication options for different mobile devices, including username-password and certificate-based authentication for users connecting from Android devices. They can also restrict corporate access based on certain attributes of the Android device—such as specific OS versions, active enablement on the device of the Pulse Secure Mobile Security Suite, or whether the device has been rooted or not.

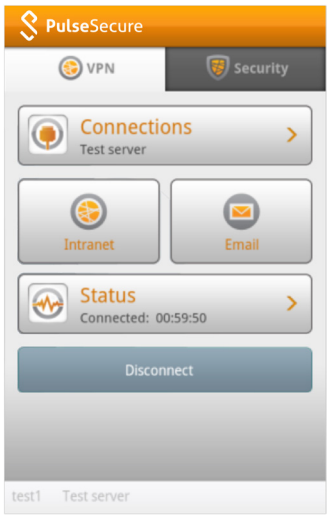

Figure 1: Pulse Secure SSL VPN Connect Screen on a Google Android Device

1 Pulse Secure does not provide full VPN on all Android devices. For a list of supported devices, please refer to the Supported Platforms document at **www.pulsesecure.net**.

Pulse Secure for Android is available as an app from Google Play and other various vendor-specific Android markets. The Pulse Secure for Android app enables secure, mobile remote access through SSL VPN connectivity in conjunction with Pulse Secure's award-winning SSL VPN solutions, Pulse Connect Secure and the MAG Series Pulse Secure Gateways or the SA Series SSL VPN Virtual Appliances.

Protect with On-Device Mobile Security

Pulse Secure for Android and the Pulse Secure Mobile Security Suite deliver comprehensive on-device mobile security for Android devices, protecting users, their devices, and the personal and corporate data residing on their devices against mobile malware, spyware, and trojans. Backed by the sophisticated mobile malware research team at Pulse Secure's Mobile Threat Center, Pulse Secure provides on-device zero-day, heuristics-based malware detection to protect Android devices around the clock, regardless if the device is connected or not, or on- or off premise.

Also, Pulse Secure for Android and the Pulse Secure Mobile Security Suite provide comprehensive loss and theft protection capabilities which enable the owner, an IT administrator, or a service provider to quickly and easily pinpoint the exact location of a lost or stolen Android device, and then display its location on an online map. Users and administrators also have the option to remotely lock the lost or stolen device, to remotely set off an alarm on a lost or stolen device, to wipe the data off of the device to ensure that personal and business contacts and calendar data cannot be accessed or exploited, and on specific Android devices, disable the USB if the device is remotely locked[2], protecting the device and its data should it fall into the "wrong hands."

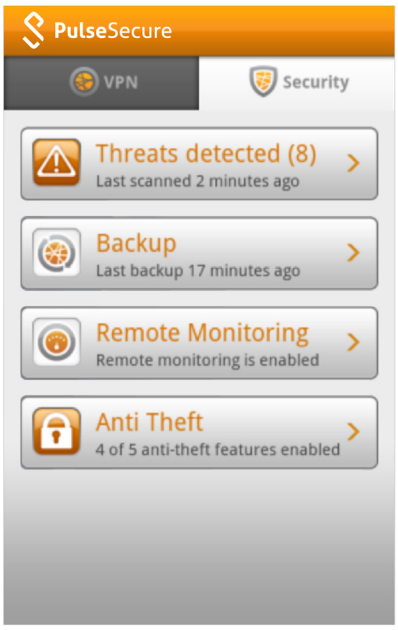

Figure 2: Pulse Secure Mobile Security Suite Dynamic Security Screen on an Android Device

Manage Mobile Devices and Policies

With Pulse Secure for Android and the Pulse Secure Mobile Security Suite, enterprises and service providers can set policies for corporate-issued or personal Android devices that attempt access to their network or cloud - addressing Bring Your Own Device (BYOD) by ensuring that they meet corporate compliance policies. Policies can include the ability to define and enforce strict passcode policies, ensure data-at-rest stored on-device is encrypted, secure data stored on the SD card via encryption[2], set blacklists of apps not to be allowed on the devices, enforcing backup and restore of device data, and remotely locating, tracking, locking, and wiping lost or stolen Android devices. Pulse Secure Mobile Security Suite provides the necessary tools to enforce compliance on Android devices, as well as to take action to prevent the loss of sensitive personal and corporate data if devices are lost or stolen.

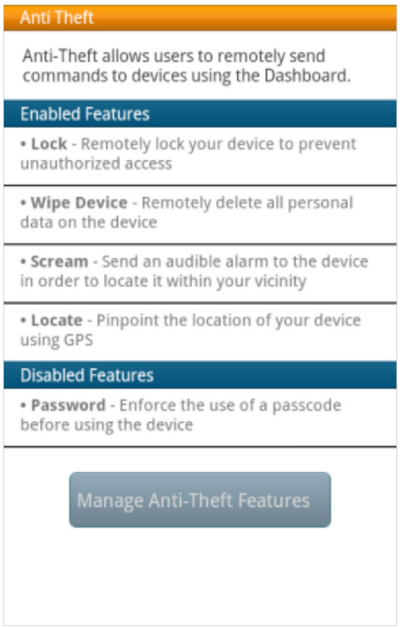

Figure 3: Pulse Secure Mobile Security Suite Anti-Theft Screen on an Android Device

[2] Specific to Samsung smartphones running the Android operating system. For a list of supported Samsung mobile devices, please refer to the Supported Platforms document at **www.pulsesecure.net**.

Architecture and Key Components

Pulse Secure for Android is a multiservice mobile app that can be deployed independently to access Pulse Secure's market-leading SSL VPN gateways and virtual appliances, the Pulse Secure Mobile Security Suite, or both simultaneously. Besides providing SSL VPN access, Pulse Secure for Android can also register an Android mobile device for the hosted, Software-as-a-Service (SaaS) Pulse Mobile Security Suite, as well as apply mobile device and data security and management features enforced by an administrator.

Simply download the Pulse Secure for Android app from Google Play or another Android market, point Pulse Secure to the appropriate URL for SSL VPN support, connect to Pulse Secure's SSL VPN gateway or virtual appliance, and seamlessly access your network and cloud resources from your Android device with the same authentication and network, cloud, application and data authorization enforcements as if you were connecting from a Windows or Mac OS device tethered to your network. MAG Series Pulse Secure Gateways running Pulse Connect Secure, Juniper Networks SA Series SSL VPN Virtual Appliances, or legacy SA Series appliances with Pulse Secure for Android as client, enable secure, purpose-based mobile remote access from Google Android devices, including full Layer 3 VPN access from Android 4.0 enabled devices and specific vendor Android devices[3]. Prior to being granted access to the network or cloud via L3 VPN, Pulse Secure for Android runs device integrity and host checks on the Android device, ensuring that it meets a baseline of access and security policy as set by the enterprise or service provider, which includes checks for the specific Android OS version, if the device has been rooted, and if Pulse Secure Mobile Security Suite is enabled on the device.

The Pulse Secure Mobile Security Suite must be enabled with a license code procured from Pulse Secure at the time of purchase. It includes the Pulse Secure Mobile Security Gateway Web-based management console where administrators can configure device and data security and management features for mobile devices, including Android devices.

Distribution

The Pulse Secure for Android app is available for free download from Google Play. The Android app is also available for specific Android mobile devices from mobile device vendors including Samsung and Lenovo. The Pulse Secure Android apps for these specific mobile devices and vendors are customized to work only with the devices offered and supported by those vendors.

The following Pulse Secure apps are currently available on Android markets worldwide.

- **Pulse Secure**: This application, downloadable from Google Play, enables the delivery of SSL-based secure remote access to networks, clouds, and web-based applications via MAG Series gateways running Pulse Connect Secure, SA Series Virtual Appliances, or legacy SA Series appliances. It also enables and serves as the interface for mobile device and data security and management features with the licensed Pulse Secure Mobile Security Suite. The Pulse Secure app enables full VPN capabilities for all Google Android 4.0-based mobile devices.
- **Pulse Secure for Samsung**: This application enables full L3 VPN–based secure, mobile remote access to networks, clouds and data via Pulse Secure's SSL VPN gateways and virtual appliances for Samsung Galaxy devices[3] running Android version 3.2 or later, as well as serving as the client for mobile device and data security and management features with the licensed Pulse Mobile Security Suite.
- **Pulse Secure for Galaxy Tab 7.0**: This application provides full L3 VPN connectivity via the Pulse Secure SSL VPN gateways and virtual appliances on Android-based Samsung Galaxy S and Tab 7.0 mobile devices[4], as well as serving as the interface for mobile device security and management capabilities with the licensed Pulse Mobile Security Suite.
- **Pulse Secure for Lenovo**: This application delivers full L3 VPN connectivity via the Pulse Secure SSL VPN gateways and virtual appliances for Android-based Lenovo mobile devices, as well as serving as the interface for mobile device and data security and management features with the licensed Pulse Mobile Security Suite. Pulse Secure for Lenovo is available on the Lenovo MobiHand market at **www.mobihand.com/product.asp?id=739637&n=Junos-Pulse**.

Features and Benefits

A simple yet sophisticated mobile device client app, Pulse Secure serves as the intuitive, interactive interface for Pulse Secure's Google Android services, including secure mobile remote access, working in conjunction with Pulse Secure's award-winning, market-leading SSL VPN products, and mobile device and data security and management through the Pulse Secure Mobile Security Suite.

Table 1: Features and Benefits of Pulse Secure for Google Android

Feature	Description	Benefits
Connect securely with mobile remote access	• SSL access to web-based applications • Full L3 VPN tunneling to networks, clouds, web-based applications, and data for Android 4.0 and select vendor devices • Flexible split tunneling options (enabled or disabled) • Authentication via username and password, certificates, and strong authentication (one-time passwords) - which can be the same robust authentication methods used for computing devices • Programmatic APIs to invoke VPN connectivity from third-party applications	• Provides simple, role-based and application specific secure mobile remote access for users of Android mobile devices • Layer 3 VPN access enables all applications on the supported Android device to connect to the corporate network or cloud, as well as enabling users to securely access network and cloud-based apps and data, enhancing user access and increasing productivity
Protect with on-device mobile security	• On-device, advanced malware protection with signature-based detection of trojans, malware, and spyware • Mobile anti-malware solution employs advanced heuristic detection • Scans downloaded files and SD cards upon insertion to prevent device infection • Delivers mobile device and data protection regardless whether the device is network or Internet connected or not, or on-premise or off	• Proactively protects Android-based devices from viruses, spyware, trojans, worms, and other malware day-zero • Ensures that all files and data downloaded to or transmitted by an Android mobile device are malware-free
Manage device usage and apps	• Define and enforce robust passcode protection policies • Ensure data-at-rest, stored on devices, as well as data stored on SD cards for specific vendor Android devices[5], is secure and encrypted, • Device and data loss and theft protection with remote alarm, locate, track, lock, and wipe capabilities • Remote, secure periodic backup and restore of device Personal Information Manager (PIM) data • Automatic removal of disallowed apps, detected malware, and infected apps without user interaction, approval, or notification[5] • Automatically disables USB port when mobile device is remotely locked[6] • Optional monitoring of short message service (SMS), Multimedia Messaging Service (MMS), and e-mail message content	• Minimizes risk of losing sensitive data • Mitigates lost or stolen device risk • Assists in maintaining corporate compliance • Helps with compliance to industry and government regulations, and with associated audits
Programmatic VPN invocation	• Pulse Secure for Android can be programmatically invoked to launch VPN from third-party Android applications using a URL scheme	• Enables third-party Android applications to invoke VPN from within their applications
Fast, easy deployment and scaling	• Simple, secure, cloud-based provisioning and deployment • Rapidly and seamlessly scales to support additional users or new features • No addition or maintenance of new hardware required for mobile device and application security and management • Simply add or remove users and features as needed • Allow users to manage specific mobile security and management functions through the web-based self-service management portal	• Lowers total cost of ownership (TCO) by managing mobile security and device management via SaaS deployment and web-based mobile security self-service management portal • Single “pane of glass” to manage consistent mobile device and apps policies
Ready for international deployment	• Pulse Secure is available in the following languages: - Chinese (Simplified and Traditional) - English - French - German - Italian - Japanese - Korean - Spanish	• Easily and quickly deployed worldwide

[3] Supports Samsung mobile devices running firmware updated later than September 2011.

[4] Supports select Samsung Galaxy mobile devices running firmware updated later than September 2011.

[5] Supports Samsung mobile devices running firmware updated later than September 2011.

[6] Supports select Samsung Galaxy mobile devices running firmware updated later than September 2011.

Ordering Information

- Pulse Secure for Android is available worldwide as a free download from Google Play, and is also available for specific mobile device vendors, including Samsung (Samsung Apps) and Lenovo (Lenovo MobiHand market).
- Pulse Secure Mobile Security Suite must be enabled with a license code procured from Pulse Secure at the time of purchase. Each Pulse Secure Mobile Security Suite SKU includes:
  - License to deploy the Pulse Secure client on as many devices as indicated in the SKU
  - License to deploy the Pulse Secure Mobile Security Suite on as many clients as indicated in the SKU
  - Subscription license for the duration indicated in the SKU
  - Service and support for the duration indicated in the SKU
  - Pulse Secure Mobile Security Gateway as a hosted (SaaS) deployment

Model Number	Description
ACCESS-MSS-AU-BYR	Pulse Mobile Security Suite subscription for "A" number of user devices and "B" number of years duration. A: Number of user devices is available in incremental counts, from 25 to 25,000 devices. B: Number of years duration is available for 1, 2, or 3-year durations.

For detailed information on the Pulse Secure Mobile Security Suite, please go to **www.pulsesecure.net**.

For more information on Pulse Secure's SSL VPN offerings, please go to: **www.pulsesecure.net**.

Pulse Secure Services and Support

Pulse Secure is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Pulse Secure ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability.

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize the company's Pulse virtual private network (VPN), network access control and mobile security products to enable end user mobility securely and seamlessly in their organizations. Pulse Secure's mission is to enable open, integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

DS004 Aug 2014