aruba

a Hewlett Packard
Enterprise company

ARUBA VIRTUAL INTRANET ACCESS CLIENT

Provides Secure Remote Network Connectivity

The Virtual Intranet Access (VIA) client from Aruba provides secure remote network connectivity for Android, Apple iOS, Mac OS X, Linux and Windows devices.

A hybrid IPsec/SSL VPN, VIA automatically scans and selects the best secure connection to the corporate network. Unlike traditional VPN software, VIA offers a zero-touch end-user experience and automatically configures wireless LAN (WLAN) settings on client devices.

For military-grade security, VIA supports Suite B cryptography when used with the ArubaOS Advanced Cryptography (ACR) module. With ACR, mobile devices with VIA can securely access networks that handle controlled unclassified, confidential and classified information.

INTEGRATED SOLUTION

Orderable through the Policy Enforcement Firewall (PEF) license, VIA can be downloaded directly from the Mobility Controller, or pushed out from an existing software management platform. VIA connects to and receives both software and configuration updates directly from the Mobility Controller with no additional hardware required.

AUTOMATIC IPSEC CONNECTION

Frequent business travelers often connect through hotels, airports, coffee shops, 4G/LTE and 3G cellular networks, which require secure links to access internal corporate resources. Legacy VPNs often require users to start additional software and undergo a complicated log in process.

However, VIA is completely Wi-Fi-aware. From a non-corporate network – such as a home WLAN, 4G/LTE, 3G or public Wi-Fi network – VIA automatically launches a VPN-on-demand connection to the data center. Connectivity and authentication occur transparently with no complicated logins.
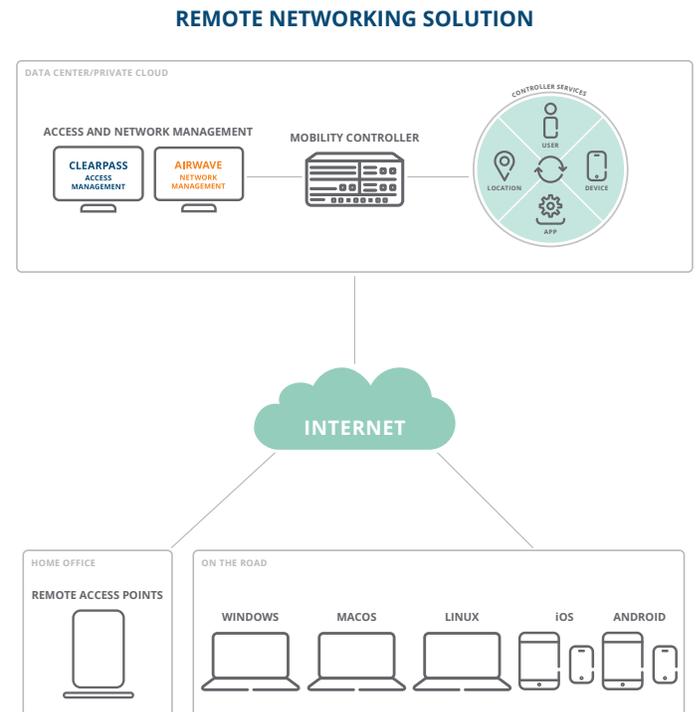
REMOTE NETWORKING SOLUTION

figure 1.0_102214_via-dsa

IPSEC WITH SSL FALLBACK ENCAPSULATION

VIA uses the standard IPsec protocol suite to secure communications between VIA-enabled devices and an Aruba Mobility Controller in the data center. This ensures the fastest connections possible where clients can connect via native IPsec. If a firewall blocks direct IPsec connections, VIA can wrap IPsec packets in an SSL header to allow secure connectivity through corporate firewalls.

LEVERAGING SINGLE SIGN-ON

The same mobile device credentials that authenticate users to wireless LANs (WLANs) can also be used to authenticate VIA users. Leveraging these credentials, VIA automatically connects users in the background without prompting them for a username and password.

When coupled with the automatic connection capability, users get a consistent connection and authentication experience without changing their work habits. Organizations that require additional authentication methods can employ traditional user name and password or token schemes.

USER ROLE SUPPORT

VIA client software leverages the same role-based and stateful firewall policies for local and remote network access to ensure a consistent end-user experience, regardless of location. It can also be configured to allow separate access roles and policies on the same end point, depending on where the user logs into the network.

EXTENSIVE TROUBLESHOOTING SUPPORT

VIA's built-in logging and diagnostic capabilities enable remote troubleshooting of connectivity issues without requiring users to navigate through a complex set of tools. If required, client logs can be emailed to support teams for more detailed troubleshooting. The diagnostic tools include connection logs, system info, detected WLAN networks, and detailed connectivity tests.

CORPORATE, HOME OFFICE AND ROAD ACCESS

VIA operates with Aruba 7200 Series, 7000 Series, 6000, 3000 Series and 600 Series Mobility Controllers. No additional VPN head-end servers or appliances are needed. With VIA, users have the same experience as when they connect to the headquarters or branch office network, creating a seamless end-user experience whether accessing network resources locally or remotely.

SECURITY PROTOCOLS SUPPORTED

- Encryption: AES-GCM-128, AES-GCM-256, AES256, AES192, AES128, 3DES, DES
- Hash: SHA-256, SHA-384, SHA, MD5
- Authentication: Pre-shared Key, RSA, RSA & ECDSA, Smart Card
- Diffie-Hellman Group: Group 1, Group 2, Group 14, ECDH Group 19, ECDH Group 20
- IPSec IKEv2

AUTHENTICATION OPTIONS

- Username/password and certificate multifactor authentication
- Smart card

FORWARDING MODES

- Tunnel mode
- Split-tunnel mode

SUPPORTED CLIENT OPERATING SYSTEMS

- iOS 4.2, 5.0, 6.0, 7.0 and 8.0
- MacOS 10.6, 10.7, 10.8, 10.9 and 10.10
- Android 4.x
- Windows 7, 8 (32 and 64 bit variants)
- Windows Vista (32 and 64 bit variants)
- Linux:
  - Ubuntu 12.04 LTS, 14.04 LTS (32 and 64 bit variants)
  - CentOS 6.3+
  - RHEL 6.3+

Note: Any device running one of the above operating systems is supported. i.e. Microsoft Surface Pro and Amazon Tablet running Android are supported but Microsoft Surface or Amazon Kindle devices are not.

HARDWARE REQUIREMENTS

- Minimum 900 MHz processor

RAM

- 256 MB
- 100 MB of available hard disk space

SUPPORTED ARUBA MOBILITY CONTROLLERS

- 7200 Series
- 7000 Series
- 6000 with M3 controller module
- 3000 series
- 600 series

VIA WITH SUITE B CRYPTOGRAPHY

For classified or highly sensitive network deployments, VIA has been enhanced to support RFC 4869 (Suite B Cryptographic Suites for IPSec). VIA with Suite B is enabled with the optional ArubaOS ACR module.

ORDERING INFORMATION[1]

Part Number	Description
Must be applied to an Aruba Mobility Controller as listed below	
JW488AAE	Aruba LIC-620-PEFV Controller Policy Enforcement Firewall for Aruba 620 License E-LTU Controller
JW489AAE	Aruba LIC-650-PEFV Controller Policy Enforcement Firewall for Aruba 650 Cntrlr License E-LTU
JW490AAE	Aruba LIC-651 PEFV Controller Policy Enforcement Firewall for Aruba 651 Cntrlr License E-LTU
JW491AAE	Aruba LIC-3200-PEFV Controller Policy Enforcement Firewall for Aruba 3200 Cntrlr License E-LTU
JW492AAE	Aruba LIC-3400-PEFV Controller Policy Enforcement Firewall for Aruba 3400 Cntrlr License E-LTU
JW493AAE	Aruba LIC-3600-PEFV Controller Policy Enforcement Firewall for Aruba 3600 Cntrlr License E-LTU
JW494AAE	Aruba LIC-M3-PEFV Controller Policy Enforcement Firewall for Aruba M3 Cntrlr License E-LTU
JW495AAE	Aruba LIC-7005-PEFV Controller Policy Enforcement Firewall for Aruba 7005 Cntrlr License E-LTU
JW496AAE	Aruba LIC-7010-PEFV Controller Policy Enforcement Firewall for Aruba 7010 Cntrlr License E-LTU
JW497AAE	Aruba LIC-7024-PEFV Controller Policy Enforcement Firewall for Aruba 7024 Cntrlr License E-LTU
JW498AAE	Aruba LIC-7030-PEFV Controller Policy Enforcement Firewall for Aruba 7030 Cntrlr License E-LTU
JW499AAE	Aruba LIC-7205-PEFV Controller Policy Enforcement Firewall for Aruba 7205 Cntrlr License E-LTU
JW500AAE	Aruba LIC-7210-PEFV Controller Policy Enforcement Firewall for Aruba 7210 Cntrlr License E-LTU
JW501AAE	Aruba LIC-7220-PEFV Controller Policy Enforcement Firewall for Aruba 7220 Cntrlr License E-LTU
JW502AAE	Aruba LIC-7240-PEFV Controller Policy Enforcement Firewall for Aruba 7240 Cntrlr License E-LTU
JW538AAE	Aruba LIC-ACR-8 Controller Advanced Cryptography 8 Session License E-LTU
JW539AAE	Aruba LIC-ACR-32 Controller Advanced Cryptography 32 Session E-LTU
JW540AAE	Aruba LIC-ACR-64 Controller Advanced Cryptography 64 Session License E-LTU
JW541AAE	Aruba LIC-ACR-128 Controller Advanced Cryptography 128 Session License E-LTU
JW542AAE	Aruba LIC-ACR-256 Controller Advanced Cryptography 256 Session License E-LTU
JW543AAE	Aruba LIC-ACR-512 Controller Advanced Cryptography 512 Session License E-LTU
JW544AAE	Aruba LIC-ACR-1024 Controller Advanced Cryptography 1024 Session License E-LTU
JW334AAE	Aruba TACT-PEFV Virtual Mobility Controller Policy Enforcement Firewall License E-LTU

[1] Software: 90 days service; can be extended with support contract

1344 CROSSMAN AVE | **SUNNYVALE, CA 94089**
1.844.473.2782 | **T: 1.408.227.4500** | **FAX: 1.408.227.4550** | **INFO@ARUBANETWORKS.COM**

aruba
a Hewlett Packard
Enterprise company

www.arubanetworks.com

DS_VIA_120116