DATA SHEET

ARUBA VIRTUAL INTRANET ACCESS CLIENT

Secure Remote Network Connectivity

The Aruba Virtual Intranet Access (VIA) client is a secure VPN service for users who need corporate connectivity at home, temporary sites, or while they're mobile.

Available as a software download for Google Android, Apple iOS, MacOS, Linux and Windows, VIA is a hybrid IPsec/SSL VPN client that automatically scans and selects the best, secure connection to terminate corporate-bound traffic. Unlike traditional VPNs which require dedicated hardware, Aruba integrates VPN services directly on existing Aruba secure infrastructure to simplify architecture and management.

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

ARUBAOS AND MANAGEMENT INTEGRATION

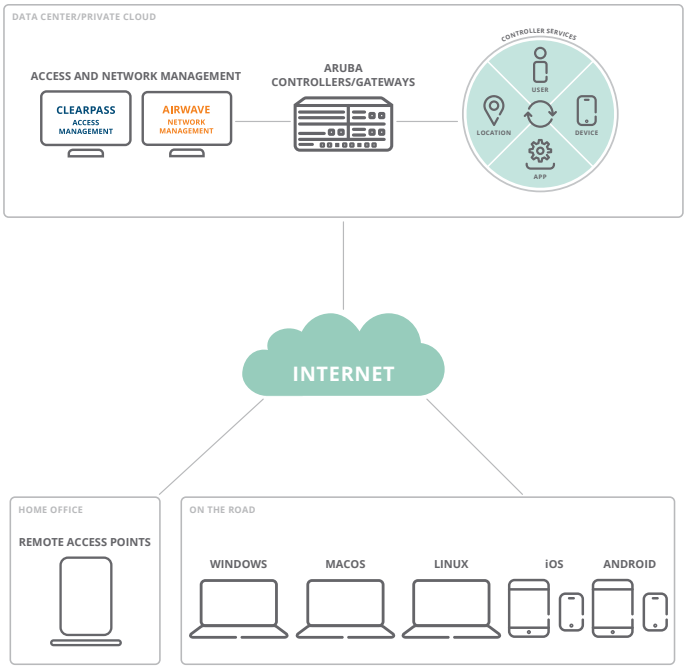
VIA can be downloaded directly from an Aruba Controller, or pushed from an existing software management platform. VIA connects to and receives both software and configuration updates directly from the Controller – no additional hardware or setup required.

AUTOMATIC IPSEC CONNECTIONS

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 login 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



KEY FEATURES

- Simplify VPN services by integrating directly with Aruba Controllers and Gateways
- VPN users can authenticate with the same credentials they use for WLAN
- Dynamically apply and enforce access policies based on the user's role

IPSEC WITH SSL FALLBACK ENCAPSULATION

VIA uses the standard IPsec protocol suite to secure communications between VIA-enabled devices and an Aruba Controller in the data center. This ensures the fastest connections possible where clients 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.

SEAMLESS SINGLE SIGN-ON EXPERIENCE

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.

EXTENDED ROLE-BASED ACCESS

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.

SECURITY PROTOCOLS SUPPORTED

- Encryption: AES-GCM-128, AES-GCM-256, AES256, AES192, AES128, 3DES, DES
- Hash: SHA-256, SHA-384, SHA1-96, MD5, SHA2-256-128, SHA2-384-192
- 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 IKEv1, XAUTH, v2

AUTHENTICATION OPTIONS

- Username/password and certificate multi-factor authentication
- Smart card

FORWARDING MODES

- Tunnel mode: All traffic terminates on an Aruba controller.
- Split-tunnel mode: Non-corporate (e.g. Internet-bound) traffic bypasses the controller directly to its destination.

SUPPORTED CLIENT OPERATING SYSTEMS

- iOS 4.2, 5.0, 6.0, 7.0, 8.0, 9.x and 10.x
- MacOS 10.6, 10.7, 10.8, 10.9, 10.10, 10.11 and 10.12
- Android 4.x, 5x, 6.0, 7.0
- Windows 7, 8, 8.1, 10 (32 and 64 bit variants)
- Windows Vista (32 and 64 bit variants)
- Linux:
  - Ubuntu 12.04, 14.04, 16.04 (32 and 64 bit variants)
  - CentOS 6.3+
  - RHEL 6.3+
  - Debian 7

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 CONTROLLERS/GATEWAYS

- 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 supports 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
Per User licensing transferable from one controller to another	
JZ148AAE	Aruba LIC-VIA per VIA Client License E-LTU This license enables per user/session firewall services for VPN termination from Aruba VIA VPN client[2]
Per Controller licensing must be applied to an Aruba 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
[2] Note: PEFV license can also be used for VIA VPN termination. But PEFV is tied to a particular controller and the license capacity scales to the controller user capacity. On the other hand, LIC-VIA license is per VIA user license and is not tied to any particular controller. It can be transferred from one controller to another. Unlike PEFV, LIC-VIA supports centralized licensing and can be managed by Mobility Master or a Master Controller in AOS 8.x deployment.

DS_VIA_091818