

ARUBAOS ADVANCED CRYPTOGRAPHY MODULE

Provides Maximum Deployment Flexibility



The ArubaOS™ Advanced Cryptography (ACR) module brings military-grade Suite B cryptography to Aruba Mobility Controllers, enabling user mobility and secure access to networks that handle controlled unclassified, confidential and classified information.

Approved by the U.S. National Security Agency (NSA), Suite B is a set of publicly available algorithms that serve as the cryptographic base for unclassified information and most classified information.

Unlike the previous generation of cryptosystems, known as Suite A or Type I, Suite B improves performance, eliminates unwieldy workflows and strict handling requirements, allows interoperability, and supports commercially available mobile devices – all at a fraction of the cost of Suite A.

The NSA has authorized the use of Suite B to facilitate the sharing of sensitive and classified information among multiple departments as well as to bring secure mobility to commercial laptops, tablets* and smartphones*.

The ArubaOS ACR module is a licensed option on any Aruba Mobility Controller, allowing governments and organizations that handle sensitive or confidential information to securely and cost effectively utilize commercial mobile technology for classified-grade networks.

SUITE B ALGORITHMS

- Advanced Encryption Standard (AES) Block Encryption with key sizes of 128 or 256 bits used with Galois/Counter Mode (GCM)
- Elliptic-Curve Digital Signature Algorithm (ECDSA)
- Elliptic-Curve Diffie-Hellman (ECDH) key agreement
- Secure Hash Algorithm (SHA) using SHA-256 and SHA-384

SUITE B PROTOCOLS

- IPsec using Internet Key Exchange (IKE) or IKEv2 – RFC4869
- Extensible Authentication Protocol (EAP) offload with TLS v1.2 – RFC 5246 and RFC 5430
- bSec – Suite B enhanced version of 802.11i for secure Wi-Fi

DESIGNED FOR COMPATIBILITY

- Based on IEEE 802.1X framework with support for all secure EAP methods
- Supports the use of X.509v3 certificates using ECDSA

FUTURE-PROOF NETWORK ARCHITECTURE

- Elevate unclassified networks to classified status utilizing the same hardware
- Utilize classified-capable solutions when building new unclassified networks

SIMPLIFIED NETWORK DESIGN

- Rapidly deploy secure access locally and remotely using a single architecture
- Support multiple services on the same network infrastructure for both classified and unclassified access

FIPS REVIEWED

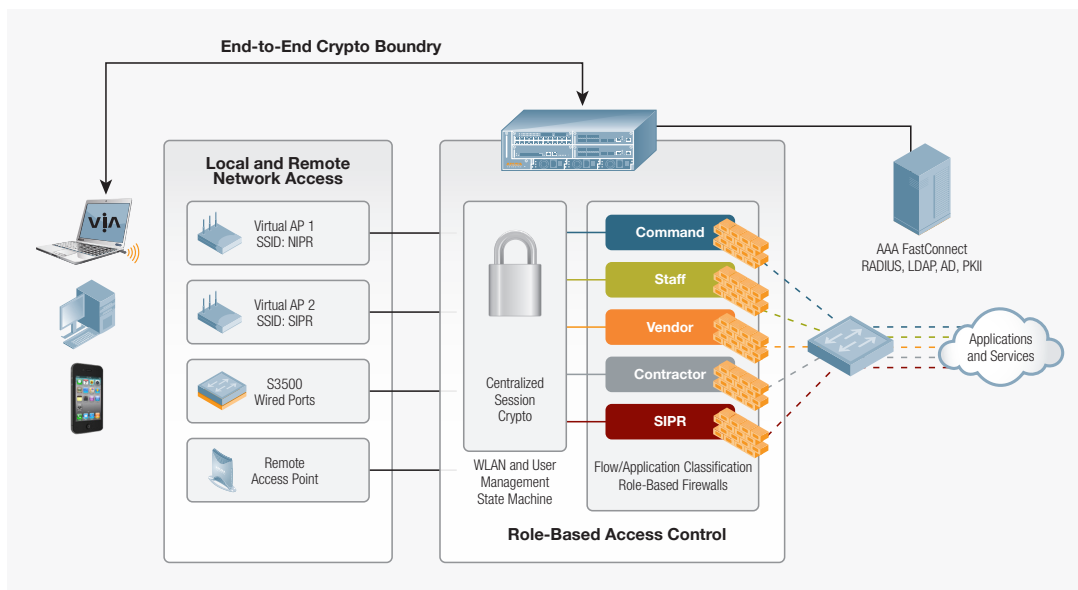
- FIPS 140-2 reviewed (validation in progress)

UNIFIED SECURITY FRAMEWORK

Aruba enables universal authentication and encryption for wired and wireless users, regardless of access method. With the Aruba Virtual Intranet Access (VIA) client and ACR, every client that connects to the network – wireless or wired – can authenticate to an Aruba Mobility Controller.

Authentication is achieved using standard the 802.1X EAP or IKE, with credential validation through RADIUS or Online Certificate Status Protocol (OSCP).

VIA supports authentication using passwords, certificates, smart cards, token cards and other credentials that are supported by the chosen EAP type.



Centralized Security Architecture for Classified Networks

NSA CERTIFIED

Suite B has been certified by the NSA as part of its Cryptographic Modernization Program, and includes a common set of cryptographic algorithms for use in protecting unclassified information and most classified information up to the secret level.

More details on Suite B may be found at http://www.nsa.gov/ia/programs/suiteb_cryptography/.

ACR DEPLOYMENT SCENARIOS

ACR is deployed by activating the ACR module license on an Aruba Mobility Controller and by installing VIA on a wired or wireless device, smartphone* or tablet*.

ACR can be used to secure traffic between an Aruba Mobility Controller and local or remote wired and wireless clients, as well as between two Mobility Controllers on the same VLAN.

DESIGNED FOR COMPATIBILITY

The Aruba ACR module is built on public security standards such as 802.1X and IPsec. Secure EAP methods supported include EAP-TLS, TTLS, and PEAP, making ACR compatible with existing security mechanisms such as Smart Cards and PKI certificates.

ACR is designed to work seamlessly on top of existing Layer 2 and Layer 3 network infrastructures.

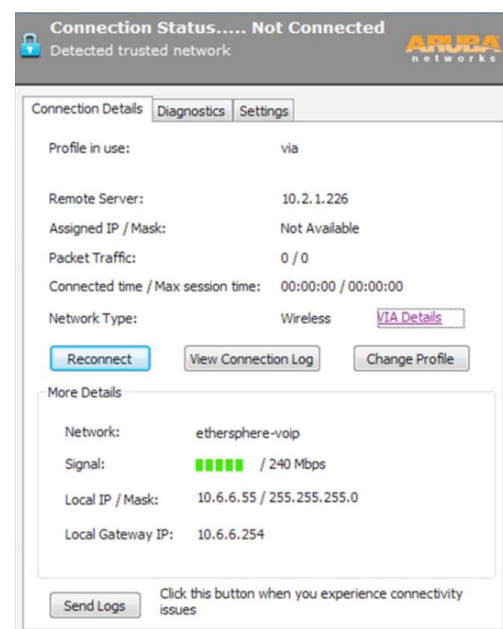
VIA WITH SUITE B

VIA is a licensed option available on any Aruba Mobility Controller that enables secure connectivity to an enterprise data center for popular device operating systems.

Combining the best of IPsec and SSL VPN technology, VIA automatically establishes a secure connection whenever it is needed, and automatically negotiates transport protocols to use SSL when other protocols fail.

To enable Suite B connectivity, VIA has been enhanced to support RFC 4869 (Suite B Cryptographic Suites for IPsec) and bSec, a Suite B enhanced version of IEEE 802.11i for secure wireless connectivity.

VIA with Suite B is enabled with the ArubaOS ACR module and supported on Windows Vista/7 devices as well as popular smartphone* and tablet* operating systems.



VIA Client Connection Status

* Roadmap items

VIA Connection Profile > default Hide Reference Save As Reset

Profile Type	Instances	Parameter
None found		

Basic Advanced

VIA Servers	Hostname / IP Address: <input type="text"/> Internal IP Address: <input type="text"/> Description: <input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>
Client Auto-Login	<input checked="" type="checkbox"/>	
VIA tunneled networks	IP Address: <input type="text"/> Network mask: <input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Delete"/>
Enable split tunneling	<input type="checkbox"/>	
Allow client side logging	<input checked="" type="checkbox"/>	
Enable IKEV2	<input checked="" type="checkbox"/>	
Use Suite B Cryptography	<input checked="" type="checkbox"/>	
IKEV2 Authentication method	eap-tls	
VIA Client DNS Suffix List	eap-mschapv2	
VIA Support E-Mail Address	user-cert	

Enabling Suite B Cryptography on VIA

ORDERING INFORMATION

The ACR module is available as a license for Aruba Mobility Controllers and is ordered based on the number of concurrent Suite B sessions supported by the controller.

Part Number	Description
LIC-ACR-8	Advanced Cryptography (8 Sessions)
LIC-ACR-32	Advanced Cryptography (32 Sessions)
LIC-ACR-64	Advanced Cryptography (64 Sessions)
LIC-ACR-128	Advanced Cryptography (128 Sessions)
LIC-ACR-256	Advanced Cryptography (256 Sessions)
LIC-ACR-512	Advanced Cryptography (512 Sessions)
LIC-ACR-1024	Advanced Cryptography (1024 Sessions)



www.arubanetworks.com

1344 Crossman Avenue, Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com