# MESA VPN

## Protecting the DoD and Intelligence Communities' Most Sensitive Data

Apriva technology has been protecting data for the US and international governments for over 15 years, enabling the transmission of classified and unclassified communication from locations around the world with confidence.

Since 2012, Apriva's MESA VPN has been protecting DoD's most sensitive information on a global scale. As part of the DoD Mobility Classified Capability (DMCC), MESA VPN has provided the secure connectivity for hundreds of thousands of classified phone calls and data transfers between classified mobile devices and SIPRnet. Listed as an approved product on the National Security Agency's Commercial Solutions for Classified (CSfC) Components List, the MESA VPN is approved to handle up to Top Secret traffic as part of a CSfC solution.

The need for our leaders to access sensitive or classified data on-the-go to make timely decisions has never been greater and Apriva's technology makes that possible.

## Robust Protection for Your Data in Transit

The Apriva MESA VPN is an extremely robust IPsec VPN that provides data-in-transit protection through the implementation of validated encryption algorithms and commercial standard protocols free of burdensome, proprietary modes of operation.

### MESA VPN BENEFITS

- Implemented with strict adherence to commercial standards protocols
- No proprietary modes of operation
- Interoperable with most native IPsec clients, including Windows-10, Android, and iOS.
- Supports RSA and ECC encryption algorithms
- NIAP Certified/Listed on NSA's CSfC Components List

### Robust, Validated Security

The MESA VPN has been certified under the National Information Assurance Partnership (NIAP) and listed on the NSA CSfC Components List as an approved product.

### IETF Standards - The Cornerstone of MESA VPN Flexibility

Unlike our competitors, the MESA VPN is designed and developed with strict adherence to IETF standards, without the implementation of proprietary licensing or policy files. This means that the MESA VPN supports most native device VPN clients out of the box and alleviates the need for costly client integration. MESA provides out-of-the-box support for Samsung, WIN 10, Apple and a variety of CSfC, commercial, and open-source clients.

## Standalone Appliance, Enterprise Gateway or Tactical Applications

No matter your implementation requirements, the MESA VPN is equipped to provide the necessary security, connectivity and flexibility so that your solution can grow as your requirements change. Whether trying to provide a classified voice solution for an entire enterprise, streaming tactical video to a small community of interest, or transmitting sensitive commercial business secrets, Apriva MESA VPN is ready for the challenge.

# MESA VPN

## Protecting the DoD and Intelligence Communities' Most Sensitive Data

## Apriva MESA VPN Technical Characteristics

- The Apriva® MESA VPN server Version 2.0 is delivered in two configurations:
    1. MESA VPN Appliance -- 1 RU rack mountable form factor
        - Dual CPU Intel® Xeon® Silver 4109T 2.0GHz processors
    2. MESA VPN Virtual – VMWare OVA Image
- Administration through Command Line or GUI-based Interfaces (with Optional MESA CCS)
- Remote Access Support

## NSA Commercial Solutions for Classified (CSfC) compliant

- NIST validated Entropy Sources
- NIST FIPS validated Cryptographic Algorithms (FIPS Certs: #2657, #3016, #3063, #3067, #3145)
- Complies with NIAP Protection Profiles:
    - Collaborative Protection Profile for Network Devices V2 (CPP_ND_V2.0E)
    - VPN Extended Package for VPN Gateways Version 2.1 (EP_VPN_GW_V2.1)
    - Collaborative PP for Stateful Traffic Filter Firewalls Version 2.0 (CPP_FW_V2.0E)
    - CSfC Selections for VPN Gateways v1.5
- IPsec Cryptography – Suite B and Legacy non-Suite B digital certificates can be supported to enable an orderly transition to Suite B certificates.
- SHA-256, 384, and 512 secure hash algorithms.
- ECDSA (P-256, P-384, P-521) and RSA (2048, 3072, 4096) certificates/signatures during user/device authentication.
- Simultaneous support for RSA and ECC certs/trust chains (one each)
- ECDH (Groups 19 and 20) and MODP DH (Groups 14, 15, and 24) for key exchange.
- AES-128-GCM and AES-256-GCM for Suite B symmetric cryptography.
- AES-128-CBC, AES-128-CCMP legacy modes.
- IKEv2/MOBIKE
- Enterprise PKI integration with OCSP and CRL support
- Supports internal or external DHCP server for two step Security Association (SA) authentication and authorization – PKI + DHCP before SA is established.
- Built-in IP address allocation Supports Tunnel Mode.  Does not support Transport mode.
- NAT and NAT Traversal (NAT-T)

## To Learn More

Please contact your Apriva sales representative at Apriva.com, email iss-sales@apriva.com or telephone (480) 421-7074.

Apriva | 8501 North Scottsdale Road, Suite 110 | Scottsdale, AZ 85253 | P 480-421-1210 | **apriva.com**
**Our new address effective July 2019:** 7600 N. 16th St., Suite 240 | Phoenix, AZ 85020
Apriva ISS Sales 480-421-7074 | International +1-480-421-1210 | iss-sales@apriva.com