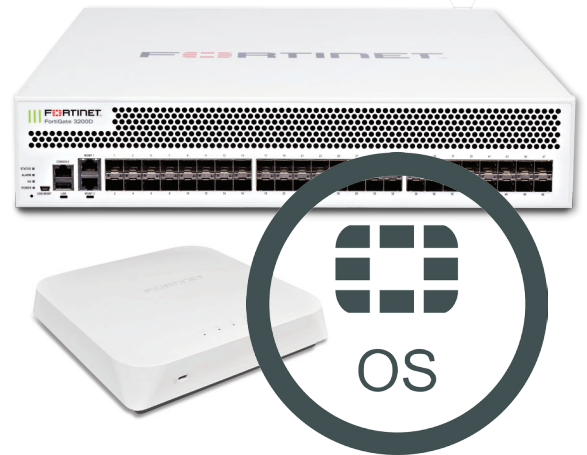


FortiOS® Wireless LAN Controller

Today's organizations are facing numerous challenges as the network environment evolves with the rapid adoption of BYOD, demanding mobile workforce, and evolving security threats. Fortinet's Secure Wireless LAN Controllers are integrated in the FortiOS, a purpose-built network security operating system, which forms the foundation of the FortiGate Network Security Platform.



Security Fabric Integration

Fortinet's Security Fabric extends to our Secure Access solution providing coordinated security policies to the very edge of the wired/wireless network where there are the most vulnerabilities.



Superior Performance

802.11 ac W2, integrated security at the edge, client steering to 5 GHz radios and Application control services all combine to deliver the highest level of performance and user experience.



End-to-End Wireless LAN Security

Integrated UTM services from the controller to the AP provides complete security for the network, the clients and the applications.



Highlights

- Support for 802.11ac Wave 2 FortiAPs
- Scale from 1 to 10,000+ of APs
- Flexible Deployment Models for Distributed Enterprise, Education, Healthcare and Hospitality
- Integrated UTM Security and Management
- PCI Compliance Capabilities for Retail Stores
- Integrated Guest Access Management with Captive Portal
- BYOD Device Finger Printing and Control
- Integrated WIDS and Rogue AP Management



HIGHLIGHTS

Key Features and Benefits

Scalable and Resilient	Highly scalable and centrally managed enterprise WLAN, with integrated radio resource management to reduce co-channel interference and provide consistent WLAN performance.
Integrated UTM Features	Extends wired security features to WLAN, unifying both wired and wireless management into a single console, providing a “Single Pane of Glass” management interface to the network.
Layer-7 Application Visibility	Leverage the market leading UTM features with the power of SPU-based deep packet inspection technology to deliver granular application level visibility and control.

The need for secure wireless networks with intra-SSID privacy, robust third-party certified security and advanced networking capabilities, is now more important than ever. Delivering the industry’s most comprehensive suite of security, wireless and networking services, the FortiOS enterprise class Wireless LAN Controller is purpose-built to leverage hardware acceleration provided by custom Fortinet Security Processing Units (SPUs) while providing an easy to use enterprise wireless solution, in a single unified platform.

Unbeatable flexibility to meet all deployment needs

A wireless infrastructure must be flexible and scalable. By consolidating security and wireless network capabilities, Fortinet Secure Wireless LAN Controllers significantly reduce network complexity and ultimately TCO. Fortinet’s no-VLANs™ approach reduces complex Layer-2 requirements, eliminating the need to propagate VLAN information across the network to simplify and accelerate large, scalable deployments. With a wide range of FortiGate models to choose from, no matter the size of your network, there’s a FortiGate solution right for you.

Single pane of glass management

Integrating wired and wireless security into a single pane of glass lowers operating costs and reduces IT staff workloads by eliminating the complexities of troubleshooting a multivendor network and the need for costly training and certification across multiple vendor products. In addition to reducing operating costs, a single pane of glass provides complete visibility of clients, access points, switches and security services, ensuring consistent security and control policies are applied across the enterprise.

Sophisticated Application Control

Wireless bandwidth is a precious shared medium and it is critical that business applications receive priority on the wireless LAN. FortiOS Application Control is built-in to the Wireless LAN controller and uses deep Layer-7 inspection with over 4,000 application

signatures to provide bandwidth guarantees and prioritization of critical applications. This industry leading Application Control capability provides the fine-grained application control required to ensure the Wireless LAN is performing at its best and is being utilized for the intended applications.

Industry Leading Security

FortiOS has its pedigree in Unified Threat Management and Fortinet holds more industry certifications than any other vendor, providing the best-in-class unified protection with an integrated set of security services. From antivirus, web content filtering, application control, network IPS, email filtering and DLP, the same security that is applied to the wired network can now be applied to the wireless LAN. Built-in Wireless Intrusion Detection System capabilities intelligently further protects the wireless LAN by detecting a vast array of RF intrusion techniques including:

- Association/Authentication/EAPOL Flooding
- Broadcast deauthentication
- Spoofed MAC
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- MAC OUI Checking

Automated Rogue AP Detection and Suppression

Rogue access points pose a serious network security threat by creating a leakage point where sensitive data such as credit card information can be siphoned off the network. For this reason, the PCI DSS and other data security standards often mandate proactive monitoring and suppression of rogue APs. The FortiGate Rogue AP on-wire detection engine uses various correlation techniques to determine if a Rogue AP is connected to the network. This automated process continuously monitors for unknown APs and automatically suppress any found to be unauthorized.

HIGHLIGHTS

Band Steering

Band steering makes more efficient use of your available wireless network by sending clients to the bands where they are most efficiently served. The FortiWLC allows the user to assign bands to clients based on their capabilities. Without band steering, a dual band client could associate on either the 2.4 GHz or the 5 GHz channels, leading to overcrowding on one band or the other depending on device preferences. With band steering, you can direct some of this traffic to your band of choice. Another example of using band steering is to separate devices by their importance (or the importance of the types of traffic they will be passing on your network). You can leave all clients with low priority profiles on the 2.4 GHz channels (where bandwidth is not a concern) and move clients to the 5 GHz band to achieve higher data rates.

Automatic Radio Resource Provisioning

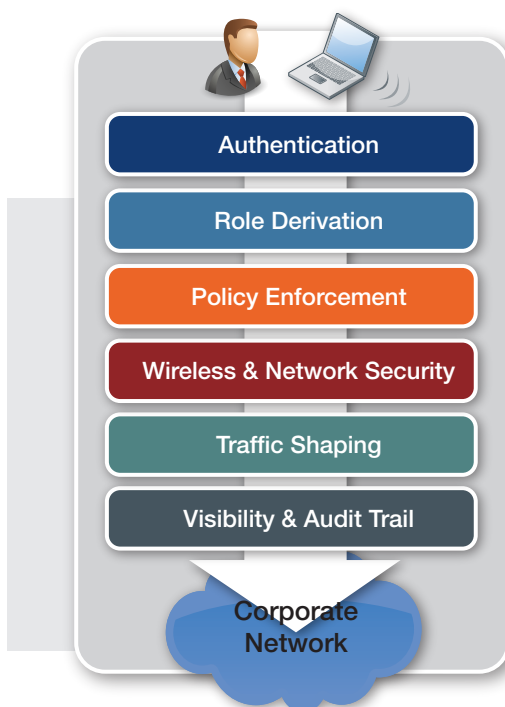
FortiOS DARRP (Distributed Automatic Radio Resource Provisioning) technology ensures the wireless infrastructure is always optimized to deliver maximum performance. Fortinet APs enabled with this advanced feature continuously monitor the RF environment for interference, noise and signals from neighboring APs, enabling the FortiGate WLAN Controller to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, DARRP also ensures that it chooses the optimal channel, without administrator intervention.

Captive Portal

Browser-based authentication for guest users is also supported in using via the SSL enabled captive portal. This built-in captive portal allows for HTML login page customization as well as guest account provisioning and management via an integrated guest management portal. FortiOS also supports universal access method (UAM) for integrating with third-party external captive portal servers as well as two-factor authentication with the FortiToken One Time Password (OTP) solution.

Device Fingerprinting

Device fingerprinting allows collection of various attributes about a device connecting to the network managed by the FortiWLC. The collected attributes can fully or partially identify individual devices, including the client's OS, device type, and browser being used. Device Fingerprinting can provide more information for the station and allows system administrators to be more aware of the types of devices in use and take actions if necessary.



Complete Secure Wireless LAN architecture:

- Captive Portal, 802.1x, Temporary Guest Access
- User & Device Identification, Authorization
- User & Device based policies, Application Control
- Rogue AP Mitigation, Wireless Intrusion Detection
- User & Application Based Wireless QOS
- Detailed Network & Threat Visibility, Compliance Reporting

SPECIFICATIONS

WIRELESS CONTROLLER	
Networking	
Bonjour Gateway	Ability to monitor and control Apple's Bonjour Protocol
DHCP	Integrated DHCP server
VLANs	Interface and trunk SSID to VLAN mapping Dynamic VLAN Support
Routing	Static, dynamic and policy routing RIP, OSPF and BGP support
Multicast	PIM Mode Multicast to unicast conversion
Data Forwarding	Centralized – Tunneled to FortiGate, no VLANs Distributed – Bridged locally Split Policy Based – Selective forwarding based on resources, policy
Provisioning and Management	
Management Access	HTTPS via web browser SSH, Telnet and console SNMP (V1 and V2)
Monitoring	Access Point (radio, channel) – Status, usage, utilization Client monitoring – Signal strength, SNR, username, IP, device type, firewall policy, bandwidth usage, application visibility Rogue AP Mesh connectivity hierarchy Wireless health monitoring, client trends, overloaded APs, excessive RF errors
Centralized Management	Single pane of glass management for wired, wireless and security configuration and monitoring Centralized management of thousands of locations via FortiManager Centralized reporting, network analytics and trends of thousands of locations via FortiAnalyzer
Troubleshooting	Remote wireless packet capture
Remote AP	
Remote AP Support	Supported on all FAP models Enables FAPs to be deployed remotely (over WAN link) to the FortiGate Wireless LAN Controller Option to encrypt data traffic via DTLS Split routing – Selective forwarding based on policy (FortiOS 5.2)
WAN Survivability	Wireless client connectivity is maintained when the wireless controller is unreachable for open and PSK type SSIDs
Troubleshooting	Local FAP diagnostic web portal
Mesh and Bridging	
Topology	Multi-hop mesh Support for multiple mesh instances
Mesh Hops	Configurable maximum hop count
Bridging	Point-to-Point bridging Point-to-Multipoint bridging for wireless ISP applications
Management	Via FortiGate web interface
Wireless Access and Authentication	
Access – Authentication Methods	IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA) RFC 2716 PPP EAP-TLS RFC 2865 RADIUS authentication RFC 3579 RADIUS support for EAP RFC 3580 IEEE 802.1x RADIUS Guidelines RFC 3748 Extensible Authentication Protocol WEP64 – 64-bit Web Equivalent Privacy WEP128 – 128-bit WEP WPA (Wi-Fi Protected Access) Personal and Enterprise, including support for Multiple PreShared Keys (M-PSKs)
Authentication Servers	WPA2 (Personal and Enterprise) – 802.11i standard MAC address authentication MAC address authentication via RADIUS Certificate based authentication for BYOD Internal Database, RADIUS, LDAP, TACACS+ External Authentication Servers – Microsoft Active Directory, Microsoft IAS RADIUS server, Cisco ACS Server, FreeRADIUS, Interlink RADIUS server, Steel Belted Radius
Encryption Protocols	CCMP/AES TKIP TKIP+AES DTLS L2TP/IPSec (RFC 3193) XAUTH/IPSec
VPN	SSL IPSec
Captive Portal	Authentication against internal or external authentication server Fully customizable look and feel including branding, graphics and language Disclaimer page Multiple-captive portal pages Forward to external captive portal Redirect to website after authentication
Guest User Management	Integrated receptionist guest user management portal Configurable expiration time Configurable start times Bulk account creation Integration with FortiAuthenticator for self-service captive portal with e-mail login
RF and Performance Management	
DAARP (Distributed Automatic Radio Resource Provisioning)	Automated selection of RF channel to achieve consistent optimal performance
DAARP Scheduling	Configurable (enable/disable) Enable with the option to exclude time slots
802.11ac 160 MHz option	Supported on 802.11ac Wave 2 models
Band Steering	Intelligently balances stations across radios, steering stations to 5 GHz RF bands for optimal performance and reducing interference
AP Load Balancing	Distribute clients evenly across APs on available channels
Self Healing	Automatically adjust TX power levels to extend coverage to compensate failed APs
RF Planning	Enabled by FortiPlanner software Predictive RF planning Real-time Dynamic Heatmaps Site Survey
Rogue AP Management	
Background Scanning	Background and full-time scanning for rogue APs
On-Wire Correlation	On-Wire correlation to identify malicious APs that are connected to the local network
Rogue Suppression	Configurable options for automatic and/or manual suppression options Over-the-air suppression of offending APs and counter measures to prevent clients attempting to connect to an identified rogue AP
Wireless IDS	Detects and logs multiple RF intrusion methods
Event Logging	Syslog of all Rogue AP events
Auditing	Pre-built reported for PCI-DSS compliance generated via FortiAnalyzer
BYOD and Mobility	
Device Identity	Distinguish between corporate assets and employee owned devices Identify and classify device types, vendor information, OS types and OS versions

SPECIFICATIONS

Application Visibility	Layer-7 application detection with support for over 3,000 signatures Ability to detect, prioritize or suppress applications
Quality of Service	End-to-end QoS Policy based retagging of applications Preserve QoS tags across the wired and wireless network Prioritize transmission of business critical applications over wireless
Policy Management	Manage and enforce firewall and traffic shaping policies based on device and user identity
802.11kvr Support	Enables more intelligent roaming decisions for faster roaming 802.11i fast-roam back 802.11i fast-associate in advance PMK caching
Presence Detection	Presence detection for presence analytics
IPv6 Support	
Client Support	Support for IPv6 clients
Management	Management over IPv6 — Support for FortiGate to act as IPv6 node
Traffic	Routing protocols, firewall and UTM support

Certifications

Wi-Fi Alliance	Wi-Fi Alliance certified (802.11ac, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Save).
Firewall	ICSA firewall enterprise certification ICSA IPv6 certified firewall USGv6 certified firewall
IEEE Standard Compliance	802.11a, 802.11b, 802.11g, 802.11n (2x2 MIMO), 802.11n (3x3 MIMO), 802.11n with Automatic Power Save Delivery (UAPSD), 802.11n with HT40 support, (4x4 MIMO) 802.11e and WME/WMM Multimedia Extensions, Block ACK, NoAck, 4 priority queues 802.11h, 802.11j 802.11i (TKIP/AES), 802.1x

NOTE: Feature set based on FortiOS Version 5.6.

ADDITIONAL REFERENCES

Resources	URL
The FortiOS Handbook — The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
FortiAP Website	http://www.fortinet.com/products/fortiap/index.html
Product Datasheets and Matrix	http://www.fortinet.com/resource_center/datasheets.html
Secure WLAN Solution Page	http://www.fortinet.com/solutions/wireless.html



GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990