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
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 via FortiManager.
- **VLANs**: Supports VLAN tagging for multiple VLANs, including 802.1Q and Port-Mode VLANs.
- **Dynamic VLAN Support**: Supports dynamic VLAN creation and deletion.
- **QoS**: Supports QoS to VLAN mapping.
- **Routing**: Supports static, dynamic, and policy routing.
- **RF, U8, and Dual Support**: Supports both 802.11a and 802.11n.
- **Multicast**: Provides PIM Mode support.
- **Multicast to unicast conversion**: Supports multicast to unicast conversion.

### Provisioning and Management

- **Management Access**: Management via HTTPS, SSH, and Telnet.
- **Monitoring**: Monitors RF, topology, troubleshooting, and logging.
- **Centralized Management**: Provides single pane of glass management for wired, wireless, and security configuration.
- **Troubleshooting**: Provides remote wireless packet capture.
- **Remote AP Support**: Supports management and monitoring of remote APs from a central location.

### Mesh and Bridging

- **Mesh Hops**: Supports multiple mesh instances.
- **Site Survey**: Provides real-time dynamic heatmaps and failed APs.
- **Band Steering**: Automatically balances stations across radios, steering stations to 5 GHz RF bands.
- **2.4 GHz**: Supports 802.11ac 160 MHz option.
- **802.11a/b/g/n/ac**: Supports multiple radio bands for optimal performance and reducing interference.

### Wireless Access and Authentication

- **802.1x** (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA): Supports all EAP methods.
- **RADIUS**: Supports RADIUS protocol.
- **DHCP**: Supports DHCPv6 and DHCPv4.
- **802.11w**: Supports 802.11w EAP.
- **802.11i**: Supports 802.11i EAP.
- **WPA**: Supports WPA (Personal and Enterprise).
- **WPA2**: Supports WPA2 (Personal and Enterprise).
- **CCM/AES**: Supports CCM/AES encryption.
- **TKIP+AES**: Supports TKIP and AES encryption.
- **TKIP**: Supports TKIP encryption.
- **WEP**: Supports 64-bit and 128-bit WEP.
- **IDV**: Supports Internal Database, RADIUS, LDAP, and TACACS+ for authentication.
- **BYOD and Mobility**: Supports BYOD and mobility, including captive portal and BYOD account management.

### Troubleshooting

- **Remote AP Support**: Supports management and monitoring of remote APs from a central location.
- **RF Planning**: Supports RF planning and site survey.
- **Background Scanning**: Provides background and full-time scanning for rogue APs.
- **On-Wire Correlation**: Provides on-wire correlation to identify malicious APs that are connected to the local network.
- **Rogue AP Suppression**: Provides automated selection of RF channel to achieve consistent optimal performance.
- **Remote AP Support**: Provides management and monitoring of remote APs from a central location.
- **BYOD and Mobility**: Supports BYOD and mobility, including captive portal and BYOD account management.
- **VLAN**: Supports VLAN tagging for multiple VLANs, including 802.1Q and Port-Mode VLANs.
- **QoS**: Supports QoS to VLAN mapping.
- **Routing**: Supports static, dynamic, and policy routing.
- **RF, U8, and Dual Support**: Supports both 802.11a and 802.11n.
- **Multicast**: Provides PIM Mode support.
- **Multicast to unicast conversion**: Supports multicast to unicast conversion.

### Wireless Access and Authentication

- **Access – Authentication Methods**: Supports IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA), RADIUS, and 802.1x RADIUS with certificates.
- **WPA2**: Supports WPA2 (Personal and Enterprise).
- **WPA**: Supports WPA (Personal and Enterprise).
- **Device Identity**: Distinguishes between corporate assets and employee-owned devices.
- **Certificate**: Supports certificate-based authentication for BYOD.
- **MAC address authentication**: Supports MAC address authentication via FortiGate.
- **FortiGate as RADIUS Server**: Supports FortiGate as RADIUS server and FortiGate as RADIUS client.

### Encryption Protocols

- **SSL/TLS**: Supports SSL/TLS encryption.
- **IPSec**: Supports IPSec encryption.
- **XAUTH/IPSec**: Supports XAUTH/IPSec encryption.
- **L2TP/IPSec (RFC 3193)**: Supports L2TP/IPSec encryption.

### Wireless LAN Controller

- **WIRELESS CONTROLLER**: Provides centralized management for thousands of locations via FortiManager.
- **Remote AP Support**: Supports management and monitoring of remote APs from a central location.
- **RF Planning**: Provides automated selection of RF channel to achieve consistent optimal performance.
- **Background Scanning**: Provides background and full-time scanning for rogue APs.
- **On-Wire Correlation**: Provides on-wire correlation to identify malicious APs that are connected to the local network.
- **Rogue AP Suppression**: Provides automated selection of RF channel to achieve consistent optimal performance.
- **Remote AP Support**: Supports management and monitoring of remote APs from a central location.
- **BYOD and Mobility**: Supports BYOD and mobility, including captive portal and BYOD account management.

### Troubleshooting

- **Remote AP Support**: Supports management and monitoring of remote APs from a central location.
- **RF Planning**: Provides automated selection of RF channel to achieve consistent optimal performance.
- **Background Scanning**: Provides background and full-time scanning for rogue APs.
- **On-Wire Correlation**: Provides on-wire correlation to identify malicious APs that are connected to the local network.
- **Rogue AP Suppression**: Provides automated selection of RF channel to achieve consistent optimal performance.
- **Remote AP Support**: Supports management and monitoring of remote APs from a central location.
- **BYOD and Mobility**: Supports BYOD and mobility, including captive portal and BYOD account management.
# SPECIFICATIONS

**Application Visibility**
- Layer 7 application detection with support for over 3,000 signatures
- Ability to detect, prioritize or suppress applications

**Quality of Service**
- Policy-based QoS tagging 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** certified (802.11ac, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Saver).
- **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 HT-40 support, (4x4 MIMO)
  - 802.11e and WME/WMM Multimedia Extensions, Block ACK, NoACK, 4 priority queues
  - 802.11i (WPA/WPA2), 802.1x

**NOTE:** Feature set based on FortiOS Version 5.6.

---

# ADDITIONAL REFERENCES

<table>
<thead>
<tr>
<th>Resources</th>
<th>URL</th>
</tr>
</thead>
</table>

Copyright © 2018 Fortinet, Inc. All rights reserved. FortiGate® and FortiGuard® are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant herein, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.