Fortinet 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. Delivering the industry’s most comprehensive suite of security, wireless and networking services, this enterprise class Wireless LAN Controller is purpose-built to leverage the hardware acceleration provided by custom Fortinet Security Processing Units (SPUs) while providing an easy to use enterprise wireless solution, in a single unified 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.

End-to-End Wireless LAN Security

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. 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. Fortinet Secure Wireless LAN Controllers with FortiAP Access Points meet the demanding needs of enterprise networks, with proven market leading security and management for both wired and wireless networks.

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.

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:

- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- 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

High Density
FortiOS monitors wireless client connections on each AP and ensures the connection load is spread uniformly across the network. This ensures better airtime utilization and provides increased capacity, resulting in a better performing WLAN. Devices can also be distributed across radios (frequencies) on a single AP, by intelligently steering dual band devices to the less crowded and higher performance 5 GHz band.

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.

Strong, Flexible Authentication
FortiOS supports standard WPA2 authentication using pre-shared keys as well as enterprise grade authentication using 802.11i or 802.1x with RADIUS. When 802.1x is enabled, users are authenticated against a backend RADIUS server, either provided by FortiAuthenticator or directly against a Microsoft Active Directory server. FortiOS also supports embedded public certificates for WPA-Enterprise authentication, MAC address authentication and MAC address white/black lists for complete and flexible authentication options based on the network constraints.

Guest 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.

Wireless LAN Planning and Analysis
FortiPlanner is a graphical Wireless LAN Planning and Post-Deployment Site Survey utility, designed to simplify WLAN planning and deployment of Fortinet FortiAP based wireless networks. Sophisticated signal propagation ray tracing algorithms are used to ensure precise pre-deployment planning accuracy, as well as accurate post-deployment visualization via real-time heat-maps.

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

- **VLANs**
  - Dynamic VLAN Support

- **Routing**
  - Static, dynamic and policy routing
    - RFC, OSPF and BGP support

- **Multicast**
  - PM Mode
  - Multicast to unicast conversion

### Data Forwarding
- **Centralized**
  - Tunneld to FortiGate, no VLANs
- **Distributed**
  - Bridged locally
  - Configurable maximum hop count

### Provisioning and Management

#### Management Access
- HTTPS via web browser
- SSH, Telnet and console

#### Monitoring
- Client monitoring – Signal strength, SNR, usernames, 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 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
- Soft 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
- Split Policy Based – Selective forwarding based on resources, policy

### Troubleshooting
- Local FAP diagnostic web portal

#### Mesh and Bridging
- **Toplogy**
  - Multi-hop mesh
- **Path-to-Point bridging**

#### Wireless Access and Authentication
- **Access – Authentication Methods**
  - IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA)
  - PPP, 2710 PPP, EAP-TLS

### Authentication Servers
- **Internal Database**
  - RADIUS, LDAP

### Encryption Protocols
- **IPSec**
  - ESP, AH
- **SSL**
  - DTLS, TLS

### VPN
- **Captive Portal**
  - Fully customizable look and feel including branding, graphics and language
  - AP and Ballonering
  - Redirect to website after authentication

### Guest User Management
- **Integrated receptionist guest user management portal**
  - Configurable start times
  - Configurable expiration time
  - Redirection to website after authentication
  - Forward to external captive portal
  - Multiple-captive portal pages
  - Fully customizable look and feel including branding, graphics and language

### RF and Performance Management
- **DAARP**
  - Distributed Automatic Radio Resource Provisioning
- **DAARP Scheduling**
- **Band Steering**
  - 802.11ac 160 MHz option
  - Automated selection of RF channel to achieve consistent optimal performance
- **Self Healing**
  - Automatic adjustment of power levels to extend coverage to compensate failed APs

### RF Planning
- **Real-time Dynamic Heatmaps**
- **Pre-built**
  - Created for PCI-DSS compliance generated via FortiAnalyzer
  - Integration with e-mail login

### Rogue AP Management
- **Background Scanning**
- **On-Wire Correlation**
- **Rogue Suppression**
  - Detects and logs intrusion attempts on all wireless RF intrusion methods
- **On-Wire Correlation**
  - On-Wire correlation to identify rogue APs that are connected to the local network
- **Auditing**
  - Pre-Drift reported for PCI-DSS compliance generated via FortiAnalyzer

### BYOD and Mobility
- **Device Identity**
  - Distinguish between corporate assets and employee-owned devices
  - Identity and classify device types, vendor information, OS types and OS versions

---

**www.fortinet.com**
### SPECIFICATIONS

<table>
<thead>
<tr>
<th>Application Visibility</th>
<th>End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality of Service</td>
<td>Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
<tr>
<td>Policy Management</td>
<td>Manage and enforce firewall and traffic shaping policies based on device and user identity, Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
<tr>
<td>802.11kvr Support</td>
<td>Enables more intelligent roaming decisions for faster roaming, Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
<tr>
<td>Presence Detection</td>
<td>Presence detection for presence analytics, Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>Support for IPv6 clients, Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
<tr>
<td>Management</td>
<td>Management over IPv6, Support for FortiGate to act as IPv6 router, Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
<tr>
<td>Traffic</td>
<td>Routing protocols, firewall and UTM support, Ability to detect, prioritize or suppress applications, End-to-end QoS, Policy-based retagging of applications, Prioritize transmission of business critical applications over wireless.</td>
</tr>
</tbody>
</table>

### ADDITIONAL REFERENCES

**Resources**

<table>
<thead>
<tr>
<th>Resources</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Datasheets and Matrix</td>
<td><a href="http://www.fortinet.com/resource_center/datasheets.html">http://www.fortinet.com/resource_center/datasheets.html</a></td>
</tr>
</tbody>
</table>

**Certifications**

- **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 firewall certification
- **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/MMM Multimedia Extensions, Block ACK, NoAck, 4 priority queues

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