DATA SHEET

FortiWLC™ Wireless Controllers

Available in:

Virtual Machine

Dedicated Wireless Controllers for the Enterprise

The FortiWLC controller series optimizes traffic across our controller-based wireless access points and client devices to support high density, high performance and predictability while addressing mission-critical enterprise demands for wireless connectivity. Powered by Fortinet's FWLC operating system, the FortiWLC creates and delivers seamless mobility and superior reliability. FWLC optimizes client distribution and channel utilization in both single- and multi-channel deployments, maximizing efficiency to make the most of available wireless spectrum.

Superior Performance - client steering to 5 GHz radios and Application Control Services all combine to deliver the highest level of performance and user experience.

Resilient - Automatic radio provisioning makes sure that APs are always using the best channels, and multiple FortiWLCs can be configured to allow for hitless failover should the connection to one controller be lost.

Multiple RF Technologies - Allows for traditional channel plan deployments or Fortinet's unique technology that manages spectrum utilization to overcome the interference-related deployment barriers commonly encountered in high density environments.

Product Offerings

Virtual Machines	
FWC-VM-50	50 APs
FWC-VM-200	200 APs
FWC-VM-500	500 APs
FWC-VM-1000	1000 APs
FWC-VM-3000	3000 APs

FEATURE HIGHLIGHTS

Virtual Cell

The Fortinet Wireless LAN Controller offers the ability to deploy a 'Virtual Cell', which differs from the traditional channel deployment approach adopted by all other vendors, while also offering a number of compelling benefits. Virtual Cell minimizes the complex, time-consuming process of channel planning, which can take months for a large campus, through its unique single channel deployment model which avoids the challenges of planning around co-channel interference. In a Virtual Cell, all radios operate on the same channel providing a layer of coverage across your campus, and appear to clients as a single radio wherever they go. In addition, the network, not the client, controls how and when clients roam.

Guest Captive Portal

Browser-based authentication for guest users is supported in FortiWLC via captive portal. The built-in captive portal allows for HTML login page customization by an administrator. FortiWLC also supports universal access method (UAM) for integrating with third-party external captive portal servers as well as OAuth based upon login credentials from social networks.

Automatic Radio Resource Provisioning

FortiWLC can be configured for ARRP (Automatic Radio Resource Provisioning), a technology that ensures the wireless infrastructure is always optimized to deliver maximum performance. When enabled, this advanced feature continuously monitors the RF environment for interference, noise and signals from neighboring APs, enabling the FortiWLC to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, ARRP also ensures that it chooses the optimal channel, without administrator intervention.

Spectrum Scanning

FortiWLC provides the ability to configure deployed APs in spectrum scanning mode, acting as a software-based spectrum monitoring device. It provides a wealth of spectrum data detected in the 2.4 GHz and 5 GHz spectrum, including graphical representations of Channel Availability, Channel Utilization, Spectrogram, Equalizer, and Persistence data.

Time-based ESS

When configuring an ESS within the FortiWLC, you can schedule the availability of that ESS based on pre-defined time intervals. By adding a timer, you can control the availability of an ESS profile based on pre-defined times during a day or across multiple days. A network set up for a specific event can be configured to shut off as soon as the event completes, or for additional security, networks that are not needed during certain times of the day can be shut down to be unavailable.

Hitless Failover/Redundancy

Enterprise WiFi is now a permanent fixture within all organizations, often carrying mission critical data, if the network stops, operations grind to a halt as well. Fortinet's FortiWLC provides for hitless failover with N+1 redundancy. The optional N+1 redundancy software feature, when implemented, allows a standby N+1 controller in the same subnet to monitor and seamlessly failover more than one master controller, and are considered to be an N+1 cluster. The standby monitors the availability of all the master controllers in the cluster by receiving advertisement messages sent by the masters. If advertisements are not received, the standby changes state, assumes the IP address of the failed master, and takes over operations for the failed master. Because the standby already has a copy of the master's latest saved configuration, all configured services continue while the controller switches from standby to active state.

FEATURE 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.

Service Control

Fortinet's Service Control feature is designed to allow clients in the enterprise network to access and communicate with devices that are advertising service via a protocol such as Bonjour. Many Bonjour-enabled devices were largely designed for small-scale use; however, they are growing increasingly prevalent in the enterprise-level environment. The nature of these services makes scaling for larger deployments challenging because the wireless traffic communications for these protocols cannot travel across various subnets. Service Control on Fortinet's FortiWLC addresses this problem by providing a framework by which Fortinet will direct traffic from clients on different subnets over to the Bonjour-capable devices (and vice versa), allowing seamless communication between the two. Users have the flexibility to specify which services should be available to specific users, SSIDs, or VLANs, allowing fine grain control to be exercised over the deployment.

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.

Application Visibility

The FortiWLC allows for application visibility with Deep Packet Inspection. Administrators can set policies to monitor and/or block one or more types of application traffic. Application control can be flexibly implemented based on a number of conditions: All ESS profiles, Per ESS profile, All APs, Per AP, Per AP Group, or ESS and AP Combination. Additionally, users can define custom applications that are not part of the pre-loaded system defined applications.

Highly Scalable

No matter the size of your network, there's a FortiWLC solution right for you, and should you need more than one controller, Fortinet's Wireless Manager platform (FortiWLM) allows you to stack and manage multiple controllers with ease. One of the primary functionalities of FortiWLM is the ability to create a global controller configuration and push it to one or more managed FortiWLCs. If a global controller configuration is changed in the WLM, all controllers using it are automatically updated with those changes. Managing large scale footprints was never so easy.

Rogue AP Detection

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 of rogue APs. The FortiWLC continuously monitors for unknown APs and can suppress connections to any such APs found to prevent information transfer. FortiWLC can also work with the FortiWLM platform to do wired to wireless MAC comparison for enhanced Rogue identification.

SPECIFICATIONS

	FWC-VM-50	FWC-VM-200	FWC-VM-500	FWC-VM-1000	FWC-VM-3000
Application	Small enterprise	Mid enterprise	Large enterprise	Large enterprise	Large enterprise
Capacity					
Maximum Access Points	50	200	500	1,000	3,000
Maximum Clients	1,250	2,500	6,250	10,000	30,000
Virtual Configuration					
vCPU	4	4	8	24	48
RAM	4 GB	8 GB	12 GB	32 GB	64 GB
Security					
Access Control	WEP, WPA-PSK, WPA-TKIP, WPA2-AES, 802.11i, 802.1X (EAP-TLS, EAP-TTLS, PEAP, LEAP, EAP-FAST, EAP-SIM, EAP-AKA, and EAP-MD5) Captive portal authentication against local database on the controller, RADIUS, and Active Directory RADIUS-assisted per-user and per-ESSID access control via MAC filtering				
Policy	Per-user firewall with fine-grained policy management: admission control, packet prioritization, QoS flows, packet drop policy, bandwidth scaling, filter ID, network protocol, and source port filtering. System-configured or per-user, RADIUS-configured firewall policies				
Management & Networking					
Zero Configuration	Access points automatically discover controllers and download configuration settings for zero-touch, plug-and-play deployment				
System Management	Upgrades and management using System Director/Network Manager, support for SNMP, centralized WLAN security policies with multiple ESS profiles, VLAN-specific administrative/security policies				
Intelligent RF Management	Coordination of access points with load balancing for predictable performance				
VLAN Support	IEEE 802.1Q VLAN tagging, GRE Tunneling				
QoS	WMM support, dynamic WMM rate adaptation, configurable QoS rules per user and application				

ORDER INFORMATION

PRODUCT	SKU	DESCRIPTION
FortiWLC Virtual Appliance License	FWC-VM-50	FortiWLC (FWC) WLAN Controller Virtual Appliance perpetual license to support up to 50 APs. Supports VMware and KVM hypervisors.
	FWC-VM-200	FortiWLC (FWC) WLAN Controller Virtual Appliance perpetual license to support up to 200 APs. Supports VMware and KVM hypervisors.
	FWC-VM-500	FortiWLC (FWC) WLAN Controller Virtual Appliance perpetual license to support up to 500 APs. Supports VMware and KVM hypervisors.
	FWC-VM-1000	FortiWLC (FWC) WLAN Controller Virtual Appliance perpetual license to support up to 1000 APs. Supports VMware and KVM hypervisors.
	FWC-VM-3000	FortiWLC (FWC) WLAN Controller Virtual Appliance perpetual license to support up to 3000 APs. Supports VMware and KVM hypervisors.
FortiCare Support	FC-10-WVMC1-248-02-DD	FortiCare for VM-50.
	FC-10-WVMC2-248-02-DD	FortiCare for VM-200.
	FC-10-WVMC3-248-02-DD	FortiCare for VM-500.
	FC-10-WVMC4-248-02-DD	FortiCare for VM-1000.
	FC-10-WVMC5-248-02-DD	FortiCare for VM-3000.

The VM Licenses are not stackable nor can one be upgraded to the next, they are fixed configurations.
A single image is available from the support portal for each of the supported virtual environments. Once installed this image will operate for a limited number of APs for 30 days. A license must then be purchased for the virtual appliance which will lock its configuration permanently. The number of CPUs and memory allocation can then be manually adjusted to match the license purchased.

FORTINET

www.fortinet.com