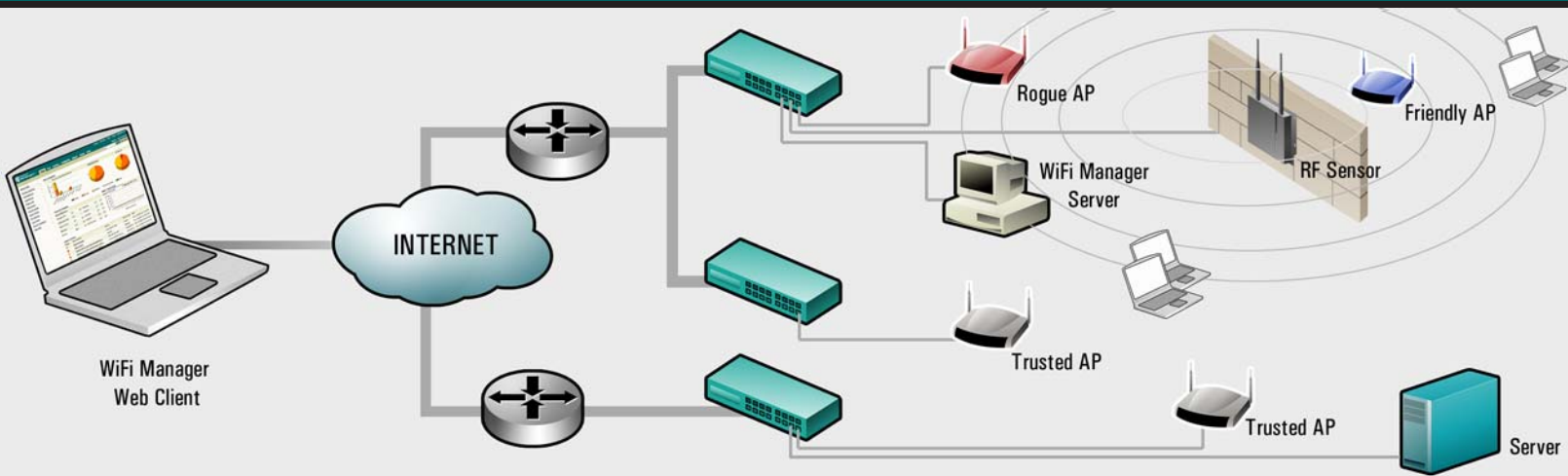


ManageEngine WiFi Manager

Integrated Wireless Security and Management Solution.

Datasheet

ManageEngine WiFi Manager is an integrated wireless security and management solution, offering multi-vendor access point configuration, firmware upgrade, rogue detection, combined wired and wireless network monitoring, and reporting capabilities for enterprise-grade wireless networks. With integrated hardware sensors for analyzing 802.11 packets, the solution protects WLANs from security threats such as intrusions, denial-of-service attacks, and vulnerabilities. It automatically discovers all wireless and wired assets in the distributed network and enables IT to control them from a single console. The Web-based user interface makes it easy to be accessed from anywhere, using a standard HTML browser.



Use WiFi Manager to

- Protect Wireless LANs
- Detect & Block Rogue APs
- Configure Access Points
- Upgrade Firmware
- Troubleshoot WLAN
- Monitor device health

WiFi Manager consists of

- WiFi Manager Software
- RF Sensor

Supports access points from:

- Cisco
- Proxim
- Symbol
- 3Com
- Avaya
- HP
- DELL

and others

Continuous RF Monitoring

Using integrated RF sensors WiFi Manager analyses the RF spectrum for all 802.11 conversations and identifies intrusions, attacks, vulnerabilities, and policy violations. Local analysis and intelligent data forwarding ensures low bandwidth consumption between sensors and the software. These sensors require zero configurations making it truly plug-and-play.

Rogue Detection & Blocking

Multiple techniques involving RF and wired side inputs are employed to detect rogue access points. Once detected, WiFi Manager provides details such as nearest sensor and switch port mapping for the administrators to locate and block the rogue AP from the network.

Attack Mitigation

WiFi Manager reduces the impact of wireless attacks by detecting them before hand. It detects all major attacks including RF jamming attack, AirJack attack, ASLEAP attack, Fata-jack attack, EAPoL logoff Storm, EAPoL Start Storm etc.

Access Point Configuration

Using WiFi Manager administrators can configure access point for basic settings, radio settings, access control settings, security settings, and services settings. Administrators can either fill in pre-defined configuration templates and push the values to select access points or group access points based on model, firmware version etc., and configure them in bulk.

Firmware Upgrade

WiFi Manager facilitates remote firmware upgrade of access points. Upgrades can also be scheduled for later execution.

Wired & Wireless Network Monitoring

WiFi Manager monitors access points and other network devices for availability, SNMP reachability, traffic, and utilization. It generates specific reports for WLANs including radio reports, error reports, association reports, and security reports.

Troubleshooting

Web-based GUI enables quick access to alarms, reports, configuration history etc., facilitating easy troubleshooting.

WiFi Manager Technical Specifications

GENERAL

- Heterogeneous access point management.
- RF monitoring using sensors. No dependency on cards.
- Works in Windows and Linux.
- Robust BE-FE-Client tiered architecture with inbuilt data base and web server.
- Highly scalable solution.

DISCOVERY

- Discovery using ICMP, SNMP, Telnet, CLI, APScan, RF Scan, CDP, and Manual entry.
- Automated periodic discovery.

AP CONFIGURATION

- Template-based configuration.
- Group configuration.
- Configuration audit.
- Basic settings: name, syslocation, syscontact, IP, subnet mask, SSID, broadcast SSID, Channel.
- 802.11 radio settings: enable radio, allow auto channel selection, channel, SSID, allow broadcast SSID, radio preamble, data rate, fragmentation threshold, RTS threshold, max RTS/CTS retries, max data retries, beacon period, data beacon period, receive antenna, transmit antenna.
- Access control settings: Enable MAC based access control, block MAC, passthrough MAC.
- Security settings: Create SSID, create VLAN, enable/disable security mode, WEP, 802.1x, WPA, WPA-PSK, RADIUS server.
- Services settings: Enable or disable services running in access points such as HTTP, Telnet, NTP etc.

EVENT MANAGEMENT

- Intelligent alarm correlation.
- Configurable alarm generation.
- E-mail based notification.
- Intelligent alarm de-duplication

FIRMWARE UPGRADE

- Group firmware upgrade.
- Scheduled upgrade.
- Firmware upgrade audit.

DEVICE MONITORING

- Wired and Wireless device monitoring.

SECURITY

- Integrated IDS sensors.
- Intrusions: Rogue AP, Rogue Client, Rogue Adhoc Client, AirJack, Airsnarf, WEPWedgie attack, MAC address spoofing, Hotspotter attack.
- DoS Attacks: Fata-jack attack, Deauthentication attack, Disassociation storm, Association storm, Authentication storm, RF jamming, EAPoL start storm, EAPoL logoff storm, Duration attack, Broadcast disassociation packet, Broadcast deauthentication packet, Improper broadcast packet.
- Vulnerabilities: Default SSID in use, AP broadcasts SSID, Adhoc network operating, AP not using encryption, Weak WEP IV used, AP using hot spot SSID, HTTP enabled for AP, Telnet enabled for AP, EAP disabled, Netbios traffic detected.

REPORTING

- Access point radio and ethernet interface availability report.
- Access point radio and ethernet interface utilization report.
- Mobile client availability report.
- Mobile client utilization report.
- Radio signal reports.
- Radio channel utilization report.
- Association report: Live associations, association history per client, association history per access point, associations sorted by duration.
- Access point traffic reports by frame speed.
- Access point traffic reports by frame type.
- Access point inventory report.
- Router availability report.
- Router traffic & utilization report.
- Router CPU utilization report.
- Router memory utilization report.
- Router interface Rx errors.
- Router interface Tx errors.
- Switch traffic and utilization report.
- Switch port Rx errors.
- Switch port Tx errors.
- Server availability report.
- Server traffic and utilization report.

- Server CPU utilization report.
- Server memory utilization report.
- AAA server availability report.
- Service response time report.

SENSOR SPECIFICATIONS

- *Standards Compliance:* IEEE 802.11a/b/g, 802.3, 802.3u, 802.3af
- *Ethernet Interface:* 1 x 10/100Mbps Auto-sensing, Auto-MDIX, 802.3af power over Ethernet
- *Antenna:* Dual external dipole with diversity, 4dBi gain at 2.45GHz, 3.5dBi gain at 5.25GHz
- *Power Input:* DC adapter 5V 1A, or 802.3af power over Ethernet
- *Receive Sensitivity:* 802.11a - 84dBm @ 6Mbps to -68dBm @ 54Mbps, 802.11b/g -91dBm @ 1Mbps to -68dBm @ 54Mbps
- *Data Rates Supported:* 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps
- *Operating Frequencies:* 802.11a 5.15-5.25GHz, 5.25-5.35GHz, 5.725-5.825GHz; 802.11b/g 2.412-2.484GHz
- *Supported Protocols:* TCP/IP, DHCP, TFTP, SNMP (v1), T ZSP
- *Dimensions:* 6.460" x 4.00" x 1.3"
- *Low bandwidth consumption:* Intelligent forwarding mechanism enables sensors utilize low bandwidth for sensor-management software communication.

SUPPORTED OS

- Windows 2000
- Windows NT
- Windows XP
- RedHat Linux 8.0
- RedHat Linux 9.0

HARDWARE REQUIREMENTS

- 512 MB RAM
- 200 MB disk space
- PENTIUM III 800 MHz

SUPPORTED BROWSERS

- IE 5.5 & above, Opera 7.2 & above, Netscape 7.0 & above