NETSCOUT

| DATASHEET |

AirMagnet Enterprise

AirMagnet Enterprise is a comprehensive 24x7 Performance Monitoring & Wireless Intrusion Detection system (WIDS) / Prevention System (WIPS), that enables organizations to meet security, performance and compliance demands of today's mobile workforce.

- *Complete Insight into Wi-Fi network Performance & Security status to proactively achieve the best quality of end-user experience*
- *SmartEdge Wi-Fi (802.11n and 802.11ac) & Wi-Fi/Cellular Spectrum sensors*
- *Automated Health Check for the WLAN AP Infrastructure pinpoints and diagnoses problems impacting Wi-Fi connectivity, performance, and WLAN network security*
- *Centralized WIPS solution with comprehensive threat detection, threat location & remediation vs unauthorized rogue devices or any internal/external policy violator*
- *Dynamic Threat Update technology for immediate wireless intrusion prevention of new threats*
- *Forensic analysis and event triangulation for rapid response*
- *Auditor-ready regulatory compliance reporting*

AirMagnet Enterprise

AirMagnet Enterprise centralized wireless intrusion detection/prevention system (WIDS/WIPS) defends your wireless environment by automatically detecting, blocking, tracing and locating any threat on all Wi-Fi channels. It contains an unmatched suite of event alerting, escalation, remote troubleshooting, forensic analysis, network health check, and professional PCI and other policy compliance reporting. The end result is a unified system that scans your environment 100% of the time to ensure your WLAN is performing safely and securely and is meeting the needs of your users and applications.

In addition to rich security features, AirMagnet Enterprise constantly monitors the health and performance of the WLAN and RF environment to proactively detect evolving problems that can lead to network interruption. The system detects issues, gives users remediation advice and includes active remote tools to troubleshoot the issue. This allows staff to avoid network downtime and vastly reduces the time-to-fix for any outage, leading to greater uptime, better performance and overall higher end-user satisfaction.

AirMagnet Enterprise is vendor agnostic and provides an independent view into the security and performance of the wireless Access Point (AP) infrastructure (controller and cloud-based).

AirMagnet Enterprise — Complete Cellular and Wi-Fi Security

AirMagnet Enterprise protects against every wireless threat by combining the industry's most thorough wireless monitoring with leading research, analysis and threat remediation.

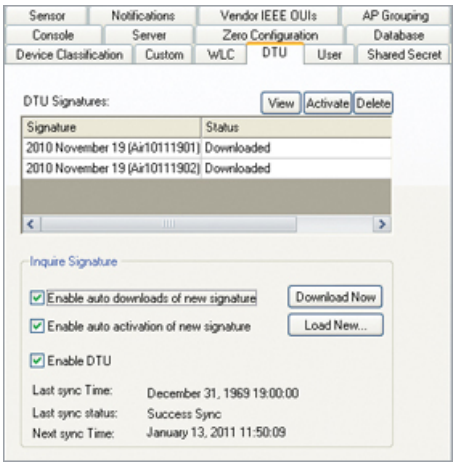
Full Visibility

AirMagnet Enterprise scans all possible 802.11 wireless network channels (including the 200 extended channels for certain sensor models), ensuring there are no blind spots where rogue devices may be hiding. AirMagnet Enterprise goes beyond Wi-Fi analysis with optional spectrum analysis that detects and classifies RF jamming attacks, Bluetooth devices and many other non-802.11 transmitter types, such as unapproved wireless cameras.

Industry Leading Threat Detection

The AirMagnet Security Research Team constantly investigates the latest hacking techniques, trends and potential vulnerabilities to keep organizations ahead of evolving threats. Our Dynamic Threat Update (DTU) technology speeds the creation, automation and immediate deployment of new threat signatures. New DTU signatures can be deployed immediately with no impact to system operation, providing a unique framework for maintaining the most up-to-date WLAN security posture.

The AirWISE engine constantly analyzes all wireless devices and traffic using a combination of frame inspection, stateful pattern analysis, statistical modeling, RF analysis and anomaly detection. This enables detection of hundreds of specific threats, attacks and vulnerabilities such as rogue devices, spoofed devices, DoS attacks, man-in-the-middle attacks, evil twins, as well as the most recent hacking tools and techniques such as MDK3, Karmetasploit and 802.11n DoS attacks.



Dynamic threat update

Automated Response and Network Protection

AirMagnet Enterprise provides a full arsenal of remediation and investigation options that can be triggered by policy to ensure that WLAN problems are quickly and accurately detected and that appropriate automated protection mechanisms are activated.

Threat Tracing, Blocking/Suppression and Mapping

All devices are traced using a suite of wired and wireless tracing methods to quickly and reliably determine if a device is connected to the network. The system uses a newly enhanced set of sophisticated techniques, including use of SNMP, automated switch discovery, and hardware and traffic analysis, to ensure accurate, fast tracing in any network topology.

Threats can be manually or automatically remediated with a combination of both wired and wireless threat suppression. Wireless blocking targets a threat at the source and specifically blocks the targeted wireless device from making any wireless connections. Wired blocking automatically closes the wired switch port where a threat has been traced.

All threats and devices can be located on a map or floor plan and be set to trigger rogue alarms based on the device's location.

Event Forensics

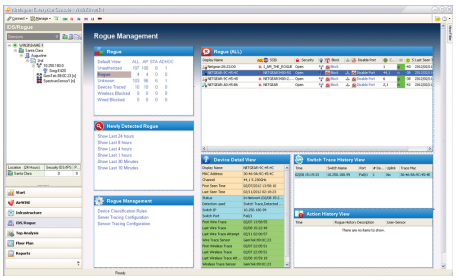
AirMagnet Enterprise captures a complete packet or RF forensic record of any network event, allowing appropriate staff to investigate the issue in depth, at any time.

Notification and Integration

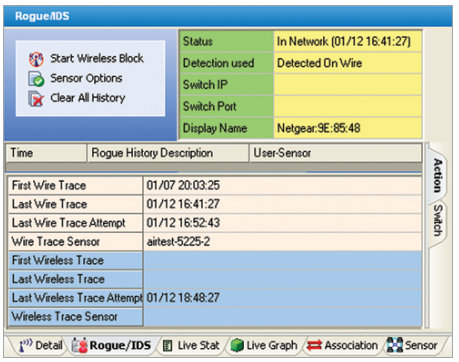
Managers have access to more than a dozen notification and escalation mechanisms, making it easy to alert specific staff members of issues or integrate wireless event data into larger enterprise management systems and operations.

Flexible Sensor Architecture

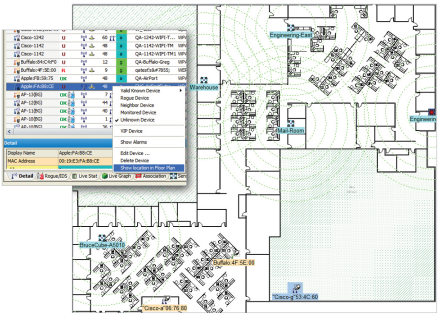
The SmartEdge Sensors support one or two Wi-Fi radios and dedicated Wi-Fi or cellular spectrum analysis. This design also enables a wireless connection from the sensor, eliminating the need for costly Ethernet cabling, or simultaneous security monitoring and performance testing.



Rogue management



Rogue device detected and traced



Locate rogue device on a floor map

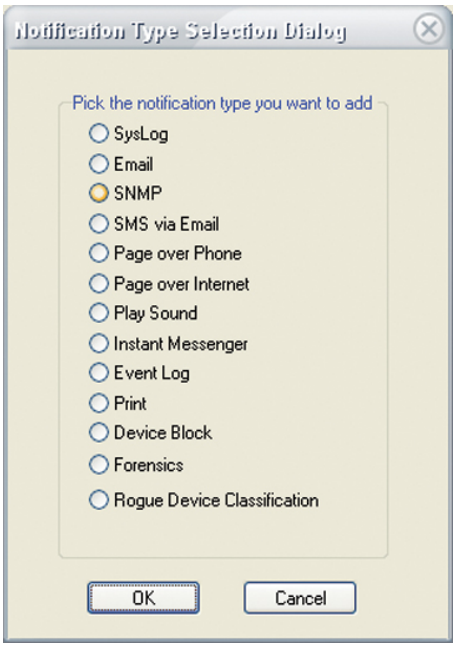
Best of Breed Security Architecture

AirMagnet Enterprise offers the only solution in the industry to meet the established standards of a mission-critical security application. It is the only system to build fault-tolerance into each component, with fail-over boot images in every sensor and automatic server fail-over licenses that come standard with the system. Additionally, AirMagnet Enterprise sensors can operate as fully independent IDS/IPS nodes detecting and remediating threats without losing information, even if the network connection to the server is lost for days. Additional unique benefits of the AirMagnet Enterprise architecture include:

Massive Scalability
With intelligent sensors that locally analyze Wi-Fi, cellular and RF conditions, more than 1,000 sensors can be supported through a single centralized server in the data center, requiring minimal network bandwidth.

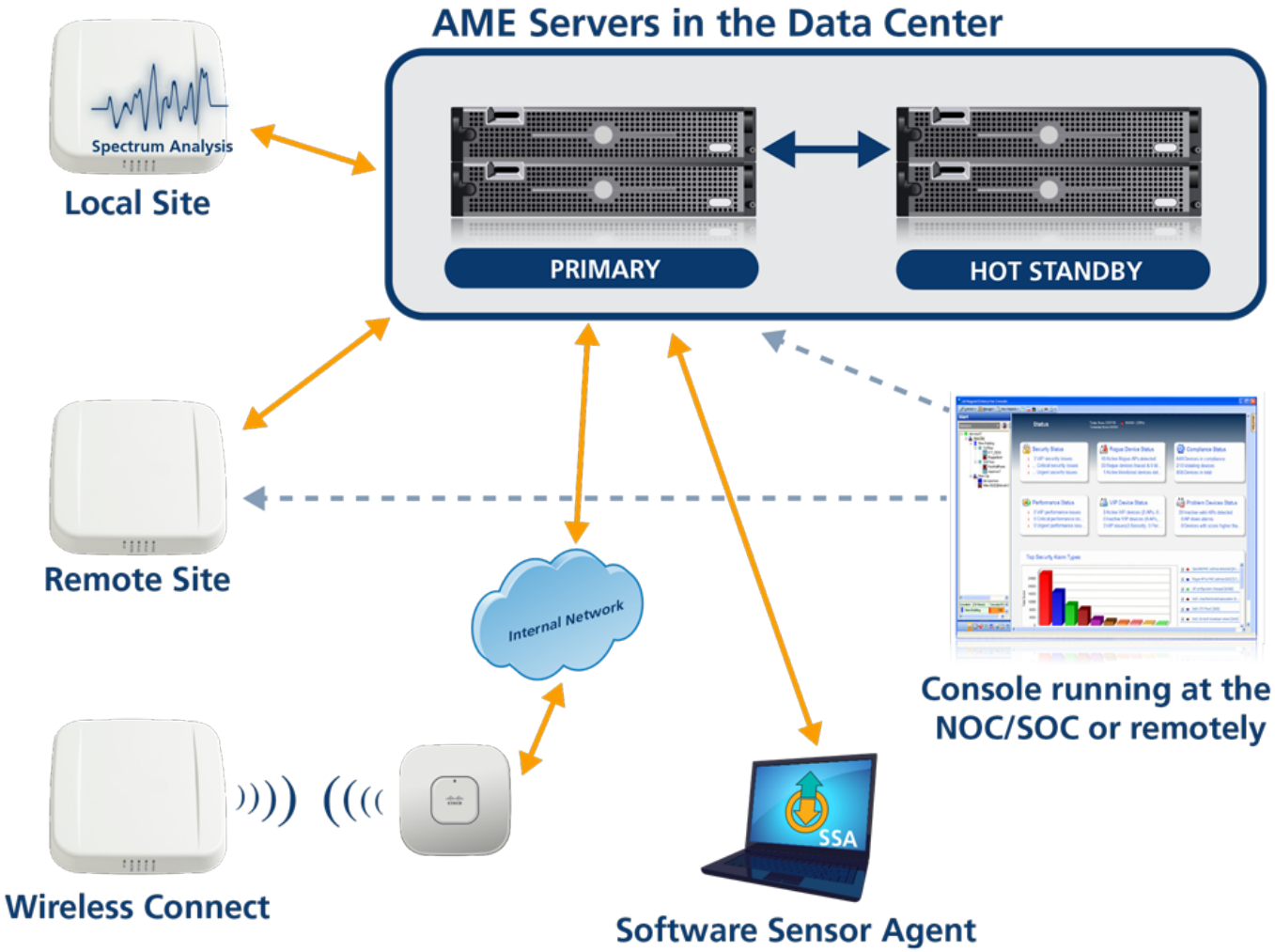
Highest System Resilience
Processing at the sensor level means that each sensor continues to enforce the security policy even if connection to the server is lost for more than 24 hours. Hot standby server software (included) enables fully redundant datacenter operations for maximum wireless security protection.

Designed for Correlation
The AirMagnet Enterprise server continuously correlates analysis from all sensors, ensuring that intelligence is always coordinated across the entire enterprise.



Notification options

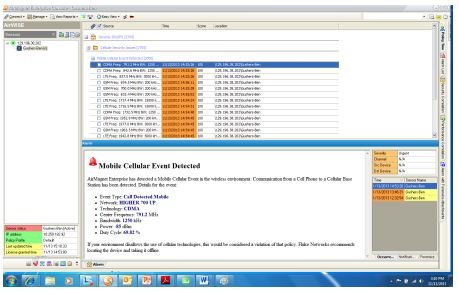
AirMagnet Sensor



AirMagnet Enterprise System

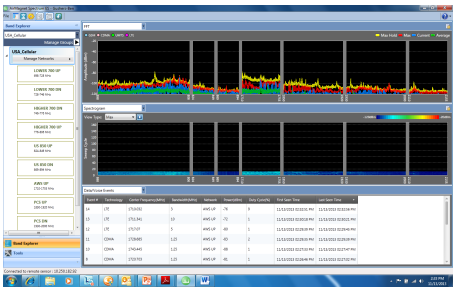
Performance Optimization and Troubleshooting

Performance and reliability of a WLAN are often directly tied to the value a wireless network delivers to an organization. AirMagnet Enterprise technology has consistently been at the forefront of innovation, developing into wireless network monitoring solutions that help IT professionals identify and mitigate WLAN problems before they impact users. By digging into the root-cause of any issue and arming users with the critical tools needed to resolve problems when they happen, AirMagnet Enterprise ensures wireless networks can reliably support business-critical applications.



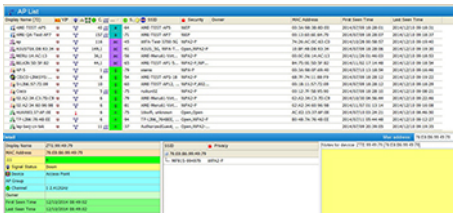
AirWISE alarm with cellular security events

AirMagnet Enterprise provides a 24x7 spectrum security solution empowering customers to enforce unified no wireless (cellular and Wi-Fi) zones. It offers detection, monitoring, and remediation of spectrum activity in a broad frequency range that includes 3G, 4G LTE, and CDMA. Activity by cellular devices like cell phones and jammers is tracked and reported. In addition, AirMagnet Enterprise monitors and reports on 4 types of cellular security violation events:



Cellular spectrum analyzer with security events

- Mobile cellular events, e.g., calls made from a specific cellular network
- Cellular interference events, e.g., cellular jammers
- Non-cellular energy events, e.g., events taking place outside of the country's allocated cellular bandwidth
- Base station cellular events, e.g., base station beacons
- Location of cellular event
- Provide cellular operator information



Access Point Listing

For further analysis, users can access sensor's built-in cellular spectrum analyzer. This avoids costly truck-rolls and reduce time to resolution.

Find Outages and Emerging Problems Before Users are Affected
Powered by the Automated Health Check (AHC), AirMagnet Enterprise sensors and Software Sensor Agents actively test and verify complete WLAN connectivity from the wireless link all the way through to application servers or the internet, automatically detecting critical outages or network degradation while pinpointing the exact source of trouble. Sensors running AHC tests provide a true client perspective, as they fully authenticate to the network and proactively probe for problems, which can be related to WLAN issues or other network resources. This provides network staff with immediate and specific information on the root cause, so they can respond often before users are impacted.

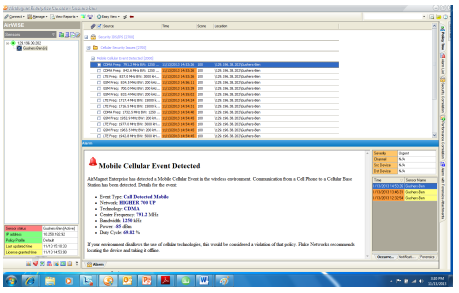
Comprehensive Wireless Analysis
AirMagnet Enterprise identifies and generates AirWISE alarms for performance issues such as traffic congestion, overloaded devices and channels, device misconfigurations, collisions, roaming problems and QoS issues. Tools for optimization enable network staff to ensure that their WLAN investment is delivering the expected real-world performance to users.

Extensive RF Interference Analysis
AirMagnet Enterprise is the only WLAN monitoring system supporting dedicated spectrum analysis hardware in the sensor for the most accurate and complete RF interference detection and remote real-time analysis. The environment is scanned 100 percent of the time over both 2.4 GHz and 5 GHz Wi-Fi bands, and specifically classifies interference sources like video cameras, cordless phones and microwave ovens, which can seriously impact the performance of the WLAN.

Real-time Remote Troubleshooting
AirMagnet Enterprise allows IT professionals to troubleshoot wireless problems remotely to fix problems faster and without costly "truck rolls". AirMagnet Enterprise sensors contain a real-time analysis interface based on AirMagnet Wi-Fi Analyzer and Spectrum XT, enabling staff to track utilization and bandwidth, view real-time decodes, as well as troubleshoot user connectivity and RF interference problems without leaving their desks.

Simple Policy-Driven Management

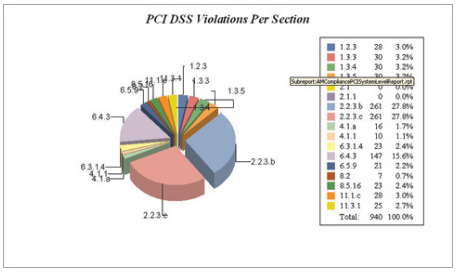
As Wi-Fi adoption continues to expand, it is increasingly important for network managers and wireless professionals to leverage tools that allow them to easily cut through the flood of Wi-Fi data and devices, revealing the information that matters most. AirMagnet Enterprise does this with tools that easily classify new Wi-Fi devices, score and prioritize issues in the network and share timely information with network staff and management systems.



Dashboard view of top WLAN issues

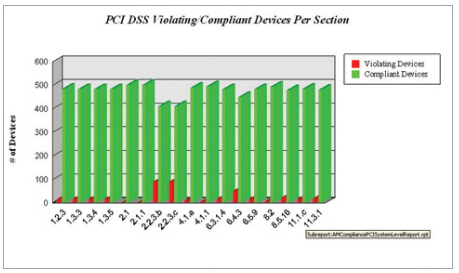
Automatic Device Classification

The AirMagnet Enterprise device classification engine allows a user to easily and accurately identify Wi-Fi devices as rogue, neighbors, monitored or approved devices. Classification rules are built using simple straightforward sentences and Boolean rules to classify devices based on their wired traced status, the device vendor, security settings, signal level, association history and variety of other factors. The system also allows managers to preview new rules so they can see what devices will be reclassified and catch any problems before the policy is pushed live.



Finding the Information that Matters

The AirMagnet Enterprise dashboard shows key headline information for all major job roles including the top security issues, performance issues, problem devices and compliance issues. All threats are correlated and scored according to user-controlled policies. This allows staff to quickly see and prioritize important events, and see devices that are at the root of multiple problems.



PCI compliance summary

Focus on Users

The system also includes a concept of VIP users or devices, allowing staff to prioritize alarms affecting key resources. Similarly, events are scored on their impact to the network, letting staff prioritize issues that are affecting many users versus lower-impact issues.

Compliance Reports

AirMagnet Enterprise outputs detailed compliance reports covering a variety of regulatory standards including Sarbanes-Oxley, HIPAA, PCI, DSS GLBA, DoD 8100.2, ISO 27001, BASEL 2 and CAD3. Reports provide a step-by-step pass/fail assessment of each section of the standard. As a result, IT staff can take the guesswork out of compliance audits and complete work in a fraction of the time.

Integrated Reporting

AirMagnet Enterprise's integrated reporting engine makes it easy to generate professional customized reports for any location or date range. Reports cover all areas of management including cellular security events, RF statistics, device reports, security and performance reports. Reports can be scheduled to run at regular intervals and delivered to key managers by email.

Ordering Information

Model	Description
AM/A5505G-ENT	AirMagnet Enterprise Server plus Add-On License, no sensors included, sw
AM/A5311G	AirMagnet Enterprise Server License for Software Sensor Agent (100)
SENSOR4-R1S1W1-E	AirMagnet Sensor, cellular spectrum, 4th Gen, 1 X 11n Radio, External Ant. [802.11n sensor]
SENSOR4-R2S1-I	AirMagnet Spectrum, 4th Gen, 2 X 11n Radio, Internal Ant. [802.11n sensor]
SENSOR4-R2S1-E	AirMagnet Spectrum, 4th Gen, 2 X 11n Radio, External Ant. [802.11n sensor]
SENSOR6-R2S1-I	SmartEdge Sensor, 2 X 11AC WI-FI Radio with Spectrum, Internal ANT [802.11ac sensor]
SENSOR6-R2S1-E	SmartEdge Sensor, 2 X 11AC WI-FI Radio with Spectrum, External ANT [802.11ac sensor]
SENSOR6-R1S0W1-E	SmartEdge Sensor, 1 X 11AC WI-FI Radio and Cellular, External ANT [802.11ac sensor]
AM/A5032	Power Injector for AirMagnet Sensors
ABLEKIT-SENSOR4	Console Cable Kit for Sensor 4 Series

Note: The AirMagnet Enterprise system requires a server/database. Users can purchase a server from NetScout or use their own server that meets the minimum requirements below.

System Requirements

IMPORTANT NOTES

- Deployments over 100 sensors require that the AirMagnet Enterprise server software and database are installed on separate physical machines
- Drive partition for AirMagnet Enterprise server must have at least 50 GB free disk space

AirMagnet Enterprise STANDALONE HARDWARE SPECIFICATIONS

Recommended Hardware (Small - Support 1 to 100 Sensors)

AirMagnet Enterprise Primary / Failover Server	AirMagnet Enterprise Database Server *
(1) 2.4 GHz, 4 core, 8 threads, 10 M Cache	(1) 2.4 GHz, 4 core, 8 threads, 10 M Cache
16 GB Memory RDIMM	16 GB Memory RDIMM
(2) 200 GB 10 K Near Line SAS (Raid 1)	(2) 200 GB 10 K Near Line SAS (Raid 1)
Microsoft® Windows Server 2012 R2 64-bit	Microsoft® SQL Server 2012/2014 or PostgreSQL version 9.1.x **
1 Gbps or faster Ethernet connection	1 Gbps or faster Ethernet connection

Notes:
** Presumes DB Server is **dedicated** to AirMagnet Enterprise Services only*
*** AirMagnet Enterprise DB Instance can reside in existing MS-SQL or PostgreSQL farm*

Recommended Hardware (Medium - Support 101 to 500 Sensors)

AirMagnet Enterprise Primary / Failover Server	**AirMagnet Enterprise Database Server ***
(1) 2.4 GHz, 8 core, 16 threads, 20 M Cache	(1) 2.4 GHz, 8 core, 16 threads, 20 M Cache
32 GB Memory RDIMM	16 GB Memory RDIMM
(2) 300 GB 15 K RPM SAS (Raid 1)	(2) 300 GB 15 K RPM SAS (Raid 1)
Microsoft® Windows Server 2012 R2 64-bit	Microsoft® SQL Server 2012/2014 or PostgreSQL version 9.1.x **
1 Gbps or faster Ethernet connection	1 Gbps or faster Ethernet connection

Notes:
** Presumes DB Server is **dedicated** to AirMagnet Enterprise Services only*
*** AirMagnet Enterprise DB Instance can reside in existing MS-SQL or PostgreSQL farm*

Recommended Hardware (Large - Support 501 to 1000 Sensors)

AirMagnet Enterprise Primary / Failover Server	**AirMagnet Enterprise Database Server ***
(2) 2.4 GHz, 8 core, 16 threads, 20 M Cache	(2) 2.4 GHz, 8 core, 16 threads, 20 M Cache
64 GB Memory, RDIMM	32 GB Memory, RDIMM
(2) 500 GB 15 K RPM SAS (Raid 1)	(2) 500 GB 15 K RPM SAS (Raid 1)
Microsoft® Windows Server 2012 R2 64-bit	Microsoft® SQL Server 2012/2014 or PostgreSQL version 9.1.x **
1 Gbps or faster Ethernet connection	1 Gbps or faster Ethernet connection

Notes:
** Presumes DB Server is **dedicated** to AirMagnet Enterprise Services only*
*** AirMagnet Enterprise DB Instance can reside in existing MS-SQL or PostgreSQL farm*

AirMagnet Enterprise Server Virtual Machine Specifications

Recommended Configuration

Deployment	vCPUs	Clock Speed (GHz)	Memory	Allocated Disk Space	Sensor Limit*	Database Size
Small	8	2.4	16 GB	200 GB	1 - 100	40
Medium	16	2.4	32 GB	300 GB	101 - 500	50

Notes:
**** Dependant on Wi-Fi and RF environment, number of Wi-Fi devices monitored and policy complexity***
Recommendation:
Operating System: Microsoft® Windows Server 2012 R2 64-bit
Recommended Database software: Microsoft® SQL 2012/2014 or PostgreSQL 9.1.x

AirMagnet Enterprise Console

Recommended Configuration

Intel Core i5 or greater

Microsoft® Windows 7 Enterprise/Professional (Service Pack 1) 64-bit
Microsoft® Windows Pro/Enterprise 8.1 64-bit

8 GB RAM or greater

Ethernet connection

AirMagnet Software Sensor Agent

Recommended Configuration

Microsoft® Windows 7 Enterprise/Professional (Service Pack 1) 64-bit

Microsoft® Windows 7 Enterprise/Professional (Service Pack 1) 64-bit
Microsoft® Windows Pro/Enterprise 8.1 64-bit

Enabled 802.11a/b/g/n/ac wireless adapter

Since SSA client is run as Window services, the user needs to have administrative rights on the machine in order for the SSA client to be installed successfully