

Firetide WLAN Solution FAQ Overview



Firetide WLAN Product FAQ

Can you provide management software and hardware to control, manage, and troubleshoot the wireless LAN in real time and produce reports on utilization?

Yes. We have a software that does policy management, RF management, security control, etc of the WLAN. The UI is able to do all of these in real time. We can even send email alerts if something is wrong and troubleshoot at any time. The graphic tools on the controller can show reports on network utilization.

Do you support enterprise user authentication schemes like 802.1X, EAP, LDAP, RADIUS?

Yes, we have support for all of these and more (including MAC-ACL)

Do you support enterprise encryption TKIP and AES.

Yes, we have support for both of these.

The proposed solution shall NOT require “feature licenses”. Any additional licenses required to comply with technical specifications must be included in pricing.

Yes, unlike ANY other competitor, Firetide includes all features in the price. There are no license fees, up selling or software fees.

Do you support layer 2 and layer 3 roaming, mesh and have no single point of failure?

We can do all of this. The APs also support WDS functionality for “AP Meshing”, in standalone mode as well as controller mode (this is rare). WDS refers to wireless distribution system in which the APs mesh to bridge connectivity from one AP to another. If required, it is possible to use our Mesh Nodes with true mesh capabilities and market leading, unmatched performance.

We have no single point of failure for several reasons:

- For critical networks, customers can enable 1:N redundancy on the controller whereby one controller can serve as a backup for up to 3 controllers with 1:N network redundancy.
- Redundant APs – Firetide Only!
 - Although the APs are working in controller mode, the traffic goes through the controller only when handling L3 roaming traffic. So even if the controller goes down, the APs are able to move traffic.
 - Since the APs are intelligent and have a lot of the functionalities of a Network Authentication server, policy management is still active even if controller goes down.
- An additional bonus is that since the AP and controller have so many authentication features and policy management, smaller enterprises actually don't need to buy a network authentication server that usually costs around \$15,000- \$20,000.

Is your WLAN architecture easily upgradeable and modular to facilitate repairs/upgrades?

Yes. The system is modular and it is very easy to upgrade with more access points and controllers up to 150 APs and 3 controllers. Firmware upgrades are included and can be done remotely.

Do you support intelligent load balancing between radios?

Yes, we support intelligent load balancing between radios AND between Access Points. The controller periodically checks and distributes clients across APs and radios in dense environments making it possible to increase the total capacity of the network. Without our intelligent load balancing, APs do not accept clients if they are overloaded.

Do you have support for Intrusion Detection System (IDS) and self-healing?

Yes. We have high security levels and intrusion detection where we can detect and mitigate rogue APs on the network. We can also differ between actual rogue APs and neighboring APs, which many solutions can't.

The system is self-healing. If an AP goes down, the system automatically covers up for that AP by increasing transmission power on the surrounding APs.

Do you support variable signal and data rate thresholds (similar Dynamic Air Time Scheduling)

Yes. We have an SLA algorithm that provides fairness between different users so that they receive the same bandwidth or according to specification. We set a max rate and a minimum signal quality demand for each client in the profile. This way, we keep away weak or far away clients from coming on board and hogging too much bandwidth. Furthermore, the SLA algorithm periodically estimates the TOTAL network capacity and divides bandwidth among users based on their status for guaranteed bandwidth vs shared bandwidth. This ensures true fairness rather than simply rate limiting. This is all patented by Firetide.

RSSI levels in all areas supporting high-speed video, data, and voice?

Yes, this is included.

Do you support roaming between radios?

We do both L2 and L3 roaming between AP radios on same AND different IPs.

IAPP: Intra access point Protocol. This allows for fast roaming between different APs on the same IP. If desired over different IPs, controller is used for seamless roaming between AP radios.

Does the equipment comply with the FCC's safety standards for RF EMISSION?

Yes, it complies with the FCC's safety standards. Firetide's products are FCC certified.

Does this system support Captive Portal (Guest sign on)

Yes, the system supports captive portal. We have 64 different profile levels that can be used. These can be allocated to different VLANs, making the system very flexible.

Unlike many other solutions, in Firetide's WLAN you can set additional administrator levels with more limited access to the system. For example, this is highly useful for a receptionist at a hotel that may just need to be able to give guest's access to the WLAN by adding them in the authentication scheme – they don't want to see all the other capabilities and options of the WLAN. This interface makes it easy for a clerk to put in the username + password so that the guest will have Wi-Fi access.

Does it offer secure tunneling: natively and inherently provide secure tunneling to segregate “guest”?

Yes, we can associate each profile to one or more VLANs on the APs. This system is extremely flexible. The tunneling is secure and can segregate “guest”.

Does the solution natively and inherently force wireless users (meeting 802.11a specification) to switch between the 2.4GHz and 5GHz wireless bands? Switching being performed to accommodate and mitigate: bandwidth usage, RF noise/interference, and spectrum loading.

Yes. It switches the users to the right AP radio intelligently in order to minimize interference and RF noise, as well as optimize bandwidth usage. This is part of our load-balancing algorithm.

Do the units have built in location tracking? Details: the solution must be able to physically locate wireless users in locations where multiple Access Points (AP) are installed - to an accuracy within 30 feet at those sites having multiple APs delivered as part of this procurement.

Yes we can locate individual clients accurately where multiple access points are installed. We can also blacklist clients them based on location if needed.

ISCA certified firewall with role based policy enforcement - the solution must have an internal firewall with ability to control specific resource access by policy.

We do not support this currently but are evaluating putting this on the roadmap.

Dynamically blacklist malicious users - the solution must provide the ability to control wireless network activity (via native and integral firewall enforced rules/policy). Control parameters must include source/destination IP address, Type of Service, Class of Service, port number, day of week, and time of day.

Yes, this is included.

Spectrum usage scanning - the solution must provide the ability to regularly scan both bands for other devices/usage in proximity to the APs.

Yes, this is included.

Wireless Bridging - the AP's must have the ability to be configured to support AP to AP bridging of connectivity where wire infrastructure is unavailable.

Yes, we also support WDS functionality for “AP Meshing” in our AP & Controller solution, not just in standalone. We have more solutions for situations where wire infrastructure is unavailable than anyone in the industry. You can also use our CPE, Mesh and bridges as well as our APs in WDS mode.

Remote AP Tunneling - the AP's must have the ability to initiate VPN tunneling back to the security controller for AP's installed outside the Agency Network.

This is not currently built into the solution but it is in the road map to do so. However, you can certainly manage the APs remotely through setting up external VPNs.

SLA and QoS for Voice, Video, Data at the AP.

Yes! We have this.

Do the APs have an On-Board state-full inspection Firewall?

We do not currently have this but are evaluating putting this in.

Proposed solution MUST apply QoS marking and queuing at the AP and provide over-the air QoS.

These functionalities are included.

Could you do the following: Proposed solution MUST include network segmentation as follows:

- a) Guest – Internet only access.**
- b) Employee – unlimited access to LAN secured via 802.11i standards including WPA2 Enterprise support.**
- c) Contractor – limited access to LAN secured via 802.11i standards including WPA2 Enterprise support.**
- d) Video – prioritized via 802.11e.**

All of the above are enabled with Firetide's solution. We have support for up to 64 different security and configuration profiles on the network.