# Summit WM3000 Series WLAN Controllers

*High-performance wireless LAN controller platforms for advanced wireless services.*

## Enterprise-Class Mobility

- High-speed, cross-subnet roaming
- End-to-end Quality of Service (QoS)
- Large-scale clustering with high availabilty

## Comprehensive Security Features

- Role-based firewall
- IPSec VPN Gateway
- Wireless intrusion detection and prevention

## Value-Add Mobility Services

- Real Time Location Services (RTLS)
- Enhanced guest services

Summit® WM3000 series controllers provide a scalable high-performance Wireless LAN (WLAN) solution that is easy to use and offers robust security features. In today's enterprise environments, dedicated resources are rarely available to build and operate the wireless network. By focusing on ease of installation and management, the Summit wireless mobility solution from Extreme Networks® enables IT organizations to simplify the task of mobilizing their users without compromising security or performance.

Summit WM series controllers enable support of the most advanced wireless LAN applications. With high-speed, cross-subnet roaming and sophisticated multicast support, Summit WM series controllers offer the features needed for IT to meet mobile voice or multimedia networking challenges. Summit WM3000 series controllers can scale to support the largest WLAN installations while providing centralized management for remote office installations.

Summit WM3600 controller can support 2,000 to 20,000 mobile devices and manage up to 256 Access Points (APs). It includes a user accessible ExpressCard™ Slot that can host a broadband card (3G/4G) for a redundant wireless WAN backhaul connection. Summit WM3700 controller is designed for large-scale, high-bandwidth enterprise deployments. It supports 8,000 to 96,000 mobile devices and manages up to 1,024 APs.

## Target Applications

- Enterprise, mission-critical applications
- Multi-site deployments
- Value-add mobility applications

*Summit WM3000 series controllers are purpose built to enable high availability and support for the most advanced wireless applications.*

# Enterprise-Class Mobility

**Summit WM3000 controllers offer scalability in capacity and performance, and help protect user investment.**

## High-Speed, Cross-Subnet Roaming

Summit WM3000 series controllers support Layer 2/Layer 3 inter-controller roaming. Inter-controller Layer 3 roaming allows clients to roam between controllers which are not on the same LAN or IP subnet. This allows controllers to be placed in different locations on the network. Using standards-based 802.11i PMK caching mechanisms, the roaming process is speeded up since it allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. In addition to reusing PMKs on previously visited APs, Opportunistic Key Caching allows multiple APs to share PMKs amongst themselves. This allows a client to roam to an AP that it has not previously visited and reuse a PMK from another AP to skip the 802.1x authentication.

## End-to-End Quality of Service

QoS provides policy enforcement for mission-critical applications and for users that have critical bandwidth requirements when the controller's bandwidth is shared by different users and applications. The Summit WM3000 controllers' architecture offers end-to-end QoS from the wireless client to the packet destination. QoS can be configured for different classes of users through the virtual APs or SSIDs. The wireless QoS solution maintains the traffic priority from client to destination. Over-the-air, latency-sensitive traffic is given priority transmit access using either the SpectraLink Voice Protocol (SVP) or 802.11e Wireless Multimedia (WMM) priority management. Summit WM controllers map the wireless QoS to wired Layer 2 (802.1p) and Layer 3 (DSCP) QoS markings for upstream and downstream traffic.

The Summit WM controllers support Call Admission Control (CAC) as per IEEE 802.11e based Traffic Specifications (TSPEC). CAC is a traffic management technique that regulates the number of calls for better roaming. A client can request a new voice session with specific traffic stream parameters including QoS. These parameters are part of the TSPEC associated with a session request. The Summit WM controller can accept or reject the session request based on the availability of network resources to enable the requested level of service. It also prevents oversubscription of network resources that can result in service degradation and poor voice quality.

The Unscheduled Automatic Power Save Delivery (UAPSD) feature, also known as WMM power save, defines an unscheduled service period, which are contiguous periods of time during which the controller is expected to be awake. If the controller establishes a downlink flow and specifies UAPSD power management, it requests (and the AP delivers) buffered frames associated with that flow during an unscheduled service period. The controller initiates an unscheduled service period by transmitting a trigger frame. A trigger frame is defined as a data frame (e.g. an uplink voice frame) associated with an uplink flow with UAPSD enabled. After the AP acknowledges the trigger frame, it transmits the frames in its UAPSD power save buffer addressed to the triggering controller. UAPSD is well suited to support bi-directional frame exchanges between a Wi-Fi handset and its AP.

## Large-Scale Clustering with High Availability

A set of Summit WM3000 controllers can be clustered to create a mobility domain and a redundancy group. Within the cluster, controllers discover and establish connections to controllers. The cluster has full mesh connectivity. Up to 12 controllers can be configured as members of a cluster to significantly reduce the chance of a disruption in service to WLANs and associated clients in the event of failure of a controller or intermediate network failure.

In the event of a controller failure, an existing cluster member assumes control. Therefore, the controller-supported network remains up and running even if a controller fails or is removed for maintenance or a software upgrade. Each redundancy group is capable of supporting an Active/Active configuration responsible for group load sharing. Members within the same redundancy group can be deployed across different subnets. APs can be load balanced across members of the group. AP capacity licenses are aggregated across the cluster. When a new member joins the cluster, the new member can leverage the AP license(s) of existing members.

# Comprehensive Security

Comprehensive network security features help keep the mission-critical wireless network and resources secure and provide compliance for HIPAA and PCI. The Summit WM3000 controllers provide a layered approach to protect and secure data at every point in the network, wired or wireless. The Summit WM3000 series controllers offer a complete range of privacy options ranging from unencrypted communication for guests, shared key for phones and PDAs, to WPA and WPA2 for enterprise-class applications. For high performance and scalability, all over-the-air encryption connections are terminated at the AP with hardware acceleration. Each defined SSID specifies how the wireless user or device should authenticate, with options for browser-based login, MAC address verification or 802.1x enterprise AAA identity management. MAC address authentication can be combined with other link security types for additional protection.

The Summit WM3000 series controllers can be configured to disallow traffic exchanged between the clients on individual SSIDs. Once enabled on a SSID, the controller will block at Layer 2 any communication attempts made between all client MAC addresses associated to the SSID.

## Firewalls

Firewalls protect networks from unauthorized traffic. The Summit WM3000 controllers' supported firewalls allow authorized traffic while blocking unauthorized traffic. They support Stateful Layer 2 and role-based firewalls. Stateful Layer 2 Firewalls allow established sessions to continue after a client roams. Role-based firewalls base the security policy on user group location, encryption strength, etc. It follows a user as it roams across different APs and controllers.

## IPSec VPN Gateways

IPSec VPN offers the security and encryption features necessary to protect enterprise data, voice, and video traffic as it traverses public or insecure networks. IPSec VPN can be deployed to provide secure point-to-point connectivity between sites as well as provide users remote access into the network eliminating costly dial-up and leased lines. Summit WM3000 controller supports IPSec termination for site-to-site VPN and IPSec termination for remote access VPN. The controller also supports IPSec traversal of firewall filtering, IPSec traversal of NAT and IPSec/L2TP (client to controller).

## Wireless IDS/IPS

Unauthorized AP detection is directly integrated into the Summit WM3000 series controllers – when enabled this allows the Summit WM3000 to monitor the RF environment for unauthorized APs. Unauthorized APs can be reported to the controller from managed radios configured to perform scanning. The controller enables an attached AP to scan the channels for such threats and report them. The AP can scan for threats on its channel or on all channels in that band. The controller analyzes the data and determines which APs are unauthorized and creates an alert and a report. APs that have been categorized as unapproved represent a potential threat to the network. Unauthorized AP containment can be used to provide temporary mitigation against active unauthorized APs operating at a site by attempting to disrupt communications with any associated clients as well as attempting to prevent new clients from associating with the AP.

The Summit WM3000 series controllers and Altitude™ 3500 series access points seamlessly integrate with Motorola AirDefense WIPS. One of the radios on the access point can be converted into dedicated AirDefense sensors. The AirDefense Enterprise server can detect and trust APs managed by the Summit WM3000 controller. The AirDefense Enterprise server can blacklist suspicious clients by creating wireless filters on the controller. Administrators can launch the AirDefense GUI from within Extreme Networks Wireless Management Suite (WMS). The AirDefense Enterprise server can forward SNMP traps to WMS to provide centralized alarm reporting and correlation.

# Value Add Mobility Services

## Real Time Location System

Real Time Location System (RTLS) is a wireless radio frequency solution that continually monitors and reports in real time the location of tracked resources. The Extreme Networks RTLS solution leverages standards-based 802.11a/b/g APs and the Low Level Reader Protocol (LLRP) allowing the Summit WM3000 controller to provide location services for standard 802.11 devices and tags as well as RFID enabled devices and tags. By eliminating the need to purchase overlay location engines, the Extreme Networks WLAN system can provide standard data, video and voice WLAN services to users while simultaneously tracking Wi-Fi and RFID devices providing faster deployments and lowering capital and operating expenditure. An RTLS feature license for the Summit WM3000 controller enables API for 3rd party RTLS applications. In addition Extreme Networks provides support for 3rd party RTLS solutions from industry leaders AeroScout and Ekahau.

## Enhanced Guest User Services

Guest authentication offers a simple way to provide secure authenticated access on a WLAN for users and devices using a standard web browser. Guest user authentication allows enterprises to offer authenticated access to the network by capturing and re-directing a web browser session to a captive portal login page where the user must enter valid credentials to be granted access to the network.

This service can be utilized for multiple applications including guest and visitor access or private user access and can be found in enterprise, hospitality, healthcare, transportation and education environments. Guest authentication is fast becoming a popular means for authenticating users and devices as it provides administrators with the means for performing authentication without deploying 802.1X or distributing shared keys. Visitors and guest users at a site would be provided with a temporary username and password from front desk personnel during the sign-in process which would permit access to the network for the duration of their visit. Once the alloted time for the guest account expires, the user would be denied access to the network.

Another common application for the guest access feature is to provide authenticated access to private networks for unmanaged devices. In certain vertical markets, such as education, administrators need to provide access to unmanaged devices that are owned and maintained by end users like students and faculty. In environments such as education, the make, model and OS of the end-user devices varies making 802.1X very challenging to deploy, manage and maintain. Web-based guest user authentication provides an elegant way to solve these administrative challenges.

The web-based guest user administrator tool provides the ability to create guest user accounts on the local database on the Summit WM controller. The guest user provisioning tool is designed for non-administrative users such as front desk personnel and provides:

- The ability to create guest user accounts with user defined or random usernames and password.
- Ability to specify date and time when the account is active and deactivated.
- Ability to assign the user to a group which determines WLAN, time of day, day of week and bandwidth policies. The group can also be utilized to assign a role to the users when the role-based firewall is employed.
- Ability to print a card which contains the username, password and alloted time information.

# Technical Specifications

## Summit WM3600

### AP Capacity
- Up to 256 APs

### SSIDs
- Supports 32 SSIDs
- Multi-ESS/BSSID traffic segmentation
- VLAN to ESSID mapping
- Auto Assignment of VLANs (on RADIUS authentication)
- Power Save Protocol Polling
- Pre-emptive roaming
- Congestion control with Bandwidth Management
- Multiple SSIDs per VLAN

### Network Security

**Firewall**
- Role-based wired/wireless firewall ( L2-L7) with stateful inspection for wired and wireless traffic; Active firewall sessions; protects against IP Spoofing and ARP Cache Poisoning

**Authentication**
- Pre-shared keys (PSK)
- 802.1x/EAP – transport layer security (TLS), tunneled transport layer security (TTLS), protected
- EAP(PEAP)
- Kerberos Integrated AAA/RADIUS Server with native support for EAP-TTLS, EAP-PEAP (includes a built-in user name/password database
- Supports LDAP and EAP-SIM

**IPSec VPN Gateway**
- Supports DES, 3DES, AES-128 and AES-256 encryption, with site-to-site and client-to-site VPN capabilities
- Supports 1,024 concurrent IPSEC tunnels per controller, 12,288 per cluster

**Secure Guest Access**
- URL redirection for user login
- Local web-based authentication
- Customizable login/welcome pages
- Support for external authentication/billing systems
- Web interface for Guest Account setup by non-IT personnel

**Access Control Lists**
- L2/L3/L4 ACLs

**Geofencing**
- Add location of users as a parameter that defines access control to the network

**Wireless IDS/IPS/AirDefense WIPS**
- Multi-mode rogue AP detection,
- 802.11n Rogue Detection,
- Ad-Hoc; Network Detection,
- Denial of Service protection against wireless attacks, client blacklisting, excessive authentication/association; excessive probes; excessive disassociation/deauthentication; excessive decryption errors; excessive authentication failures; excessive 802.11 replay; excessive crypto IV failures (TKIP/CCMP replay)

**Wireless RADIUS Support (Standard and Extreme Vendor specific attributes)**
- User Based VLANs (Standard)
- User Based QoS (Extreme VSA)
- Location Based Authentication (Extreme VSA)
- Allowed ESSIDs (Extreme VSA)

### Quality of Service (QoS)

**Wireless Priority**
- 802.11 traffic prioritization and precedence

**Wi-Fi Multimedia Extensions**
- WMM
- WMM Power Save

**Classification and Markings**
- Layer 1-4 packet classification; 802.1p VLAN priority; and marking: DiffServ/TOS

**IGMP Snooping**
- Optimizes network performance by preventing flooding of the broadcast domain

### Real Time Location System
- RSSI based triangulation for Wi-Fi assets
- Tags supported: Ekahau, Aeroscout, Newbury, Gen 2 Tags
- RFID support: Compliant with LLRP protocol. Built-in support for the following Motorola RFID readers: fixed (XR440, XR450, XR480; mobile (RD5000) and handheld (MC9090-G RFID)

### Availability
- Active:Standby; Active:Active and N+1 redundancy with access point load balancing; Critical resource monitoring
- Dual Firmware bank supports Image Failover capability

### Management
- Command line interface (serial, telnet, SSH);
- Secure Web-based GUI (SSL) for the wireless switch and the cluster
- SNMP v1/v2/v3; SNMP traps—40+ user configurable options; Syslog; TFTP Client
- Secure network time protocol (SNTP)
- Text-based switch configuration files
- DHCP (client/server/relay), switch auto-configuration and firmware updates with DHCP options; multiple user roles (for switch access)
- MIBs (MIB-II, Etherstats, wireless controller specific monitoring and configuration)
- Email notifications for critical alarms
- Client naming capability

### Physical Specifications

**Form Factor**
- 1U Rack Mount

**Dimensions**
- 1.75 in. H x 17.32 in. W x 15.39 in. D
- 44.45 mm H x 440 mm W x 390.8 mm D

**Weight**
- 14 lbs./6.35 kg

**Package Dimensions**
- 24.5 in H x 21.5 in W x 6.25 in D
- 622.3 mm H x 546.1 mm W x 158.8 D

**Package Weight**
- 17.55 lbs/7.96 kg

**Interfaces**
- 1x Uplink Port -10/100/1000 Cu/ Gigabit SFP interface
- 8x 10/100/1000 Cu Ethernet Ports with 29.7 Watts PoE, 802.3af and 802.3at Draft
- 1x 10/100 Management port
- 1x USB port
- 1x ExpressCard™ Slot (in USB mode)
- 1x PCI-X Interface
- 1x Serial Port (RJ45 style)

### Power Specifications
- AC input voltage: 90 – 264 VAC 50/60 Hz
- Max AC input current 6A@115 VAC, 3A@230 VAC current
- Input frequency: 47 Hz to 63 Hz

### Environmental Specifications
- Operating temperature: 32° F to 104° F/0° C to 40° C
- Storage temperature: -40° F to 158° F/-40° C to 70° C
- Operating humidity: 5% to 85% (w/o condensation)
- Storage humidity: 5% to 85% (w/o condensation)
- Heat dissipation: 665 BTU per hour

### Regulatory
- Product safety: UL/cUL 60950-1, IEC/EN60950-1
- EMC compliance: FCC (USA), Industry Canada (IC), CE (Europe), VCCI (Japan), C-Tick (Australia/New Zealand), ANATEL (Brazil), CCC (China), KCC (Korea)
- RoHS, WEEE

For additional country certifications see: http://www.extremenetworks.com/go/wirelesscertification

### Warranty
- Limited One Year

# Technical Specifications

## Summit WM3700

### AP Capacity
- Up to 1,024 APs

### SSIDs
- Supports 256 SSIDs
- Multi-ESS/BSSID traffic segmentation
- VLAN to ESSID mapping
- Auto Assignment of VLANs (on RADIUS authentication)
- Power Save Protocol Polling
- Pre-emptive roaming
- Congestion control with Bandwidth Management
- Multiple SSIDs per VLAN

### Network Security

**Firewall**
- Role-based wired/wireless firewall ( L2-L7) with stateful inspection for wired and wireless traffic; Active firewall sessions; protects against IP Spoofing and ARP Cache Poisoning

**Authentication**
- Pre-shared keys (PSK)
- 802.1x/EAP – transport layer security (TLS), tunneled transport layer security (TTLS), protected
- EAP(PEAP)
- Kerberos Integrated AAA/RADIUS Server with native support for EAP-TTLS, EAP-PEAP (includes a built-in user name/password database
- Supports LDAP and EAP-SIM

**IPSec VPN Gateway**
- Supports DES, 3DES, AES-128 and AES-256 encryption, with site-to-site and client-to-site VPN capabilities
- Supports 2,048 concurrent IPSEC tunnels per controller, 24,576 per cluster

**Secure Guest Access**
- URL redirection for user login
- Local web-based authentication
- Customizable login/welcome pages
- Support for external authentication/billing systems
- Web interface for Guest Account setup by non-IT personnel

**Access Control Lists**
- L2/L3/L4 ACLs

**Geofencing**
- Add location of users as a parameter that defines access control to the network

**Wireless IDS/IPS/AIrDefense WIPS**
- Multi-mode rogue AP detection,
- Rogue AP Containment,
- 802.11n Rogue Detection,
- Ad-Hoc; Network Detection,
- Denial of Service protection against wireless attacks, client blacklisting, excessive authentication/association; excessive probes; excessive disassociation/deauthentication; excessive decryption errors; excessive authentication failures; excessive 802.11 replay; excessive crypto IV failures (TKIP/CCMP replay)

**Wireless RADIUS Support (Standard and Extreme Vendor specific attributes)**
- User Based VLANs (Standard)
- User Based QoS (Extreme VSA)
- Location Based Authentication (Extreme VSA)
- Allowed ESSIDs (Extreme VSA)

### Quality of Service (QoS)

**Wireless Priority**
- 802.11 traffic prioritization and precedence

**Wi-Fi Multimedia Extensions**
- WMM
- WMM Power Save

**Classification and Markings**
- Layer 1-4 packet classification; 802.1p VLAN priority; and marking: DiffServ/TOS

**IGMP Snooping**
- Optimizes network performance by preventing flooding of the broadcast domain

### Real Time Location System
- RSSI based triangulation for Wi-Fi assets
- Tags supported: Ekahau, Aeroscout, Newbury, Gen 2 Tags
- RFID support: Compliant with LLRP protocol. Built-in support for the following Motorola RFID readers: fixed (XR440, XR450, XR480; mobile (RD5000) and handheld (MC9090-G RFID)

### Availability
- Active:Standby; Active:Active and N+1 redundancy with access point load balancing; Critical resource monitoring
- Dual Firmware bank supports Image Failover capability

### Management
- Command line interface (serial, telnet, SSH);
- Secure Web-based GUI (SSL) for the wireless switch and the cluster
- SNMP v1/v2/v3; SNMP traps—40+ user configurable options; Syslog; TFTP Client
- Secure network time protocol (SNTP)
- Text-based switch configuration files
- DHCP (client/server/relay), switch auto-configuration and firmware updates with DHCP options; multiple user roles (for switch access)
- MIBs (MIB-II, Etherstats, wireless controller specific monitoring and configuration)
- Email notifications for critical alarms
- Client naming capability

### Physical Specifications

**Form Factor**
- 1U Rack Mount

**Dimensions**
- 1.75 in. H x 17.32 in. W x 15.39 in. D
- 44.45 mm H x 440 mm W x 390.8 mm D

**Weight**
- 13.5 lbs./6.12 kg

**Package Dimensions**
- 24.5 in H x 21.5 in W x 6.25 in D
- 622.3 mm H x 546.1 mm W x 158.8 D

**Package Weight**
- 18.1 pounds/8.21 kg

**Interfaces**
- 4x 10/100/1000 Cu/SFP Ethernet
- 1x 10/100 Management port
- 1x CF card slot
- 2x USB ports
- 1x serial port (RJ45 style)

### Power Specifications
- AC input voltage: 90 – 264 VAC 50/60Hz
- Max AC input current: 6A@115 VAC, 3A@230 VAC
- Input frequency: 47 Hz to 63 Hz

### Environmental Specifications
- Operating temperature: 32° F to 104° F/0° C to 40° C
- Storage temperature: -40° F to 158° F/-40° C to 70° C
- Operating humidity: 5% to 85% (w/o condensation)
- Storage humidity: 5% to 85% (w/o condensation)

### Regulatory
- Product safety: UL / cUL 60950-1, IEC / EN60950-1
- EMC compliance: FCC (USA), Industry Canada (IC), CE (Europe), VCCI (Japan), C-Tick (Australia/New Zealand), ANATEL (Brazil), CCC (China), KCC (Korea)
- RoHS, WEEE

For additional country certifications see: http://www.extremenetworks.com/go/wirelesscertification

### Warranty
- Limited One Year

# Ordering Information

| Part Number | Description |
|---|---|
| ***Summit WM3600*** | |
| 15714 | Summit WM3600 WLAN controller. AP capacity and feature licenses sold separately. Power cord sold separately. |
| 15715 | 16 AP capacity upgrade license for Summit WM3600 controller. |
| 15719 | 64 AP capacity upgrade license for Summit WM3600 controller. |
| 15716 | Real Time Location System (RTLS) feature upgrade license for Summit WM3600 controller. Enables API for 3rd party RTLS applications. |
| 15736 | Advanced Security feature upgrade license for Summit WM3600 controller. Enables role-based firewall configuration and increases number of IPSEC VPN tunnels from 100 to 1024. |
| 10051 | SFP-SX optical module for use with Summit WM3000 series controller. |
| ***Summit WM3700*** | |
| 15710 | Summit WM3700 WLAN controller. AP capacity and feature licenses sold separately. Power cord sold separately. |
| 15711 | 16 AP capacity upgrade license for Summit WM3700 controller. |
| 15712 | 64 AP capacity upgrade license for Summit WM3700 controller. |
| 15718 | 256 AP capacity upgrade license for Summit WM3700 controller. |
| 15713 | Real Time Location System (RTLS) feature upgrade license for Summit WM3700 controller. Enables API for 3rd party RTLS applications. |
| 15737 | Advanced Security feature upgrade license for Summit WM3700 controller. Enables role-based firewall configuration and increases number of IPSEC VPN tunnels from 600 to 2048. |
| 10051 | SFP-SX optical module for use with Summit WM3000 series controller. |

www.extremenetworks.com

**Corporate and North America**
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

**Europe, Middle East, Africa and South America**
Phone +31 30 800 5100

**Asia Pacific**
Phone +852 2517 1123

**Japan**
Phone +81 3 5842 4011