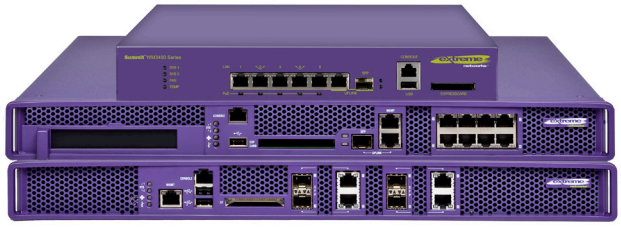
Summit WM3000 Series Wireless Controllers



High-performance Summit® WM3000 series controllers are WLAN controller platforms designed to support advanced wireless services.

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

With high-speed, cross-subnet roaming and sophisticated multicast support, Summit WM3000 series controllers offer IT administrators with the features needed 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.

The Summit WM3700 controller is designed for headquarters enterprise networks that require large-scale, high-bandwidth, multi-site deployments. It offers USB ports and CF slots for file transfers and firmware updates. The Summit WM3600 controller offers comprehensive wireless controller functionality for medium-to-large enterprises. Its ExpressCard™ slot is 3G/4G wireless-ready, for enabling remote site survivability.

The Summit WM3400 controller is ideal for small-to-medium enterprises and branch offices of large enterprises. Its compact form factor integrates wired and wireless networking and security features, for zero-touch installation and easy-to-use manageability. It comes with six AP licenses, a 3G license, Stateful/Role-based Firewall and IPSec VPN Gateway.

Enterprise-Class Mobility

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

Comprehensive Security Features

- Role-based firewall
- IPSec VPN Gateway
- Wireless Intrusion Detection/Prevention System (WIDS/WIPS)[1, 2]

Value-Add Mobility Services

- Supports Real Time Location Services (RTLS)[1, 2]
- Enhanced guest services

[1] Included with Summit WM3000 series version 4.x controllers; Version 5.x controllers do not support RTLS.
[2] Some WIDS/WIPS features require Motorola AirDefense Services Platform, sold separately.

Make Your Network Mobile

Enterprise-Class Mobility

Summit WM3000 series 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. 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, independently of physical topology. Standards-based 802.11i PMK caching mechanisms help speed up the roaming process since they allow a client to reuse 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

When the controller's bandwidth is shared, QoS provides policy enforcement for mission-critical applications and users with critical bandwidth requirements. The Summit WM3000 series controllers architecture offers end-to-end QoS and traffic prioritization from wireless client to packet destination. QoS can be configured for different classes of users through virtual APs or SSIDs. 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. The controllers map the wireless QoS to wired Layer 2 (802.1p) and Layer 3 (DSCP) QoS markings for upstream and downstream traffic.

Summit WM3000 series controllers support Call Admission Control (CAC) 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 TSPEC traffic stream parameters, including QoS. The controller can accept or reject session requests based on the availability of the network resources that 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. A controller using UAPSD power management establishes a downlink flow and requests that the AP deliver buffered frames associated with that flow during an unscheduled service period. Unscheduled service periods are initiated when a controller transmits a trigger frame to an AP. A trigger fame is a data frame associated with a UAPSD-enabled uplink flow. 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

Up to 12 Summit WM3000 series controllers can be clustered to create a redundantly configured mobility domain that supports full mesh connectivity. Clustering can help significantly reduce the chance of WLAN services disruption in the event of failure of a controller or local network.

Cluster-supported network services remain up and running even if a controller fails or is removed for maintenance or a software upgrade. If a controller fails, its associated traffic is redirected to existing members of the cluster. Each redundancy group is capable of supporting an Active/Active configuration responsible for group load sharing. Controllers within the same redundancy group can be deployed across different subnets. APs can be load balanced across controllers within the cluster. AP capacity licenses are aggregated across the cluster. When a new controller joins the cluster, the Smart License Sharing feature leverages the AP license(s) of existing members.

Comprehensive Security

Comprehensive network security features help secure mission-critical WLAN resources and provide compliance for HIPAA and Payment Card Industry (PCI) data security requirements. The Summit WM3000 series controllers provide a layered approach to protect and secure data at every point in the network, wired or wireless. They offer a wide range of privacy options including unencrypted communication for guests, shared key authentication for phones and PDAs and WPA/WPA2 encryption for enterprise-class applications. For high performance and scalability, all over-the-air encryption connections are hardware accelerated and terminated at the AP. Each defined SSID specifies wireless user or device authentication rules, 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, the controller blocks any Layer 2 communication attempts from MAC addresses associated with the disallowed SSID.

Firewalls

The Summit WM3000 series controllers include a stateful Layer 2 firewall that supports role-based firewalling. Stateful Layer 2 firewalls allow established sessions to continue after a client roams. Role-based firewalls base security policies on user group location, encryption strength, etc. and follow users as they roam across different APs and controllers.

IPSec VPN Gateways

IPSec VPNs can protect enterprise data, voice, and video traffic as it traverses public or insecure networks. IPSec VPNs can be deployed to provide secure point-to-point connectivity between sites, as well as to provide users remote access into the network, eliminating costly dial-up and leased lines. For secure remote access, Summit WM3000 series controllers support IPSec termination for site-to-site VPN and IPSec termination. The controller also supports IPSec traversal of firewall filtering, 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 controller to monitor the RF environment for unauthorized APs. The controller enables an adopted AP to scan all channels within the same frequency band and report unauthorized APs. The controller analyzes the data and determines which APs are unauthorized and creates an alert and a report. APs 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 Services Platform (ADSP)[3] Wireless Intrusion Detection/Prevention System (WIDS/WIPS), enabling an access point radio to be converted into a dedicated sensor. The ADSP server can detect and trust APs managed by the Summit WM3000 controller. ADSP can blacklist suspicious clients by creating wireless filters on the controller. For centrally administered reporting, alarms and correlation, ADSP can enable SNMP traps.

[3] Appliance models 1252, 3652 and 4250 are sold separately and are targeted for future availability.

Value-Add Mobility Services

Real Time Location System[4]

Real Time Location System (RTLS) is a wireless radio frequency solution that continually monitors and reports in real time the location of tracked resources. When combined with a third-party RTLS engine, such as AeroScout, Summit WM3000 series controllers leverages standards-based 802.11a/b/g APs and the Low Level Reader Protocol (LLRP) allowing the controller to provide location services for standard 802.11 devices and tags as well as RFID-enabled devices and tags. This allows Extreme Networks WLAN solutions to provide standard data, video and voice WLAN services to users while simultaneously tracking Wi-Fi and RFID devices for faster deployments, and lower capital and operating expenditures.

Enhanced Guest User Services

Guest authentication offers a simple way to provide secure, authenticated WLAN access for users and devices using a standard web browser. Guest user authentication works by capturing and redirecting 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 in enterprise, hospitality, healthcare, transportation and education environments. Guest authentication is fast becoming a popular means for authenticating users and devices as it provides authentication without requiring administrators to configure 802.1X or distribute shared keys. Visitors and guest users are provided with a temporary username and password during the sign-in process, which permits access to the network for the duration of their visit. Once the alloted time for the guest account expires, the user is denied access to the network.

Web-based guest user authentication offers an elegant way to to provide authenticated access to private networks for unmanaged devices. For example, IT administrators in higher education institutions need to provide network access to personal devices that are owned and maintained by students and faculty. The make, model and OS of these unmanaged wireless devices varies making 802.1X very challenging to deploy, manage and maintain.

The guest user administration tool provides the ability to create guest user accounts on the Summit WM3000 controller database. 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.
- Specify date and time when a guest user account is activated and deactivated.
- Assign the user to a group which that defines policies for WLAN, time of day, day of week and bandwidth.
- Assign a group association to identify users for role-based firewall filtering.
- Print guest user information, such as username, password and alloted time.

[4] Summit WM3000 series version 4.x controllers include integrated RTLS engine and support third-party solutions such as Ekahua or AeroScout; version 5.x controllers do not support RTLS functionality.

Technical Specifications

Summit WM3400

Cluster Capacity

- Version 4.x: Up to 12 controllers; supports Active:Active/Active:Standby configurations
- Version v5.x: Up to 2 controllers; supports Active:Active/Active:Standby configurations

AP Capacity

- Version 4.x: Up to 6 APs; supports any combination of Altitude 3500, 4600 and 4700 APs
- Version v5.x: Up to 36 APs; supports any combination of Altitude 4600 and 4700 APs

SSIDs

- Supports 24 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

Packet Forwarding

802.1D-1999 Ethernet bridging; 802.11-.802.3 bridging; 802.1Q VLAN tagging and trunking; proxy ARP; IP packet steering-redirection

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

Anomaly Analysis

Source Media Access Control (MAC) = Dest MAC; Illegal frame sizes; Source MAC is multicast; TKIP countermeasures; all zero addresses

Authentication

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

Transport Encryption

- WEP 40/128 (RC4), KeyGuard, WPA—TKIP, WPA2-CCMP (AES), WPA2-TKIP

IEEE 802.11w

Provides origin authentication, integrity, confidentiality and replay protection of management frames for 802.11w supported access points

IPSec VPN Gateway

- Supports DES, 3DES, AES-128 and AES-256 encryption, with site-to-site and client-to-site VPN capabilities

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

- Layer 2/Layer 3/Layer 4 ACLs

Geofencing

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

Wireless IDS/IPS

- Some features require Motorola AirDefense Services Platform, available separately
- 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); Suspicious AP, Authorized device in ad-hoc mode, unauthorized AP using authorized SSID, EAP Flood, Fake AP Flood, ID theft, ad-hoc advertising Authorized SSID

Wireless RADIUS Support (Standard and Extreme Networks Vendor Specific Attributes (VSA))

- User Based VLANs (Standard)
- User Based QoS (Extreme Networks VSA)
- Location Based Authentication (Extreme Networks VSA)
- Allowed ESSIDs (Extreme Networks VSA)

NAC Support with third party systems from Microsoft and Symantec

Quality of Service (QoS) Layer 3 Mobility (Inter-Subnet Roaming)

Wireless Priority

- 802.11 traffic prioritization and precedence

Wi-Fi Multimedia Extensions

- WMM
- WMM Power Save (U-APSD)
- TSPEC Admission Control

SIP Call Admission Control

Controls the number of active SIP sessions initiated by a wireless VoIP phone

802.11k

Provides radio resource management to improve client throughput (11k client required)

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, available as demo feature in WM3400 v5.x

IPv6 Client Support

Video Optimization

- Version 5.x supports multicast-to-unicast conversion

Real Time Location System

- Version 4.x controller supports RTLS/RFID/ RSSI, including third-party solutions; version 5.x does not support RTLS functionality
- 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

System Resiliency and Redundancy

- Active:Standby; Active:Active and N+1 redundancy with access point load balancing; Critical resource monitoring
- Dual Firmware bank supports Image Failover capability
- Single virtual IP (per VLAN) for a switch/ contoller cluster to use as the default gateway by mobile devices or wired infrastructure
- SMART RF: Network optimization to ensure user quality of experience at all times by dynamic adjustments to channel and power (on detection of RF interference or loss of RF coverage/neighbor recovery)

System Extensibility

- ExpressCard™ Slot: Driver support for 3G wireless cards for WAN backhaul
- AT&T (NALA) – Option GT Ultra Express
- Verizon (NALA) – Verizon Wireless V740 Express Card
- Vodaphone (EMEA) – Novatel Merlin XU870
- Vodaphone (EMEA) – Vodaphone E3730 3G Expresscard
- Telstra (Australia) – Telstra Turbo 7 series Expresscard (Aircard 880E)
- General Use (NALA/APAC) – Novatel Merlin XU870

Technical Specifications

Summit WM3400 (continued)

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 or Tabletop

Dimensions

- 1.75 in H x 12 in W x 10 in D
- 44.45 mm H x 304.8 mm W x 254.0 mm D

Weight

- 4.75 lbs/2.15 kg

Interfaces

- 1x Uplink Port -10/100/1000 Cu/Gigabit SFP interface
- 5x 10/100/1000 Cu Ethernet Ports, 802.3af and 802.3at Draft
- 1x USB port
- 1x ExpressCard Slot
- 1x Serial Port (RJ45 style)

Power Specifications

- AC input voltage: 100 – 240 VAC
- Max AC input current 3A
- Input frequency: 47 Hz to 63 Hz

Environmental Specifications

- Operating temperature: 0° C to 40° C (32° F to 104° F)
- Storage temperature: -40° C to 70° C (-40° F to 158° F)
- Operating humidity: 5% to 85% (w/o condensation)
- Storage humidity: 5% to 85% (w/o condensation)
- Heat dissipation: 95 BTU per hour

Regulatory

Standards Compliance

- RoHS: This product is in Compliance with RoHS Directive 2002/95/EC.

Product Safety Specifications

- IT Equipment:
  - EN 60950-1:2001 + A11:2004
  - UL 60950-1, 1st Edition, 2007-10-31
  - CSA C22.2 No. 60950-1-03, 1st Edition, 2006-07

EMC Specifications

- IT Emissions:
  EN 55022: 2006 + A1: 2007 (Class B)
- IT Immunity:
  EN 55024: 1998 + A1: 2001 + A2: 2003
- Harmonic Current Emissions:
  EN 6100-3-2: 2006 (Class A)
- Voltage Fluctuation & Flicker:
  EN 61000-3-3: 1995 + A1: 2001 + A2: 2005
- Medical Electrical Equipment:
  EN60601-1-2: 2007:
  IEC6060-1-1-2: 2007 (Modified)
- Radio Frequency Devices:
  47 CFR Part 15, Subpart B, Class B
- Digital Apparatus:
  ICES-003 Issue 4, Class B

EMC Compliance

- FCC (USA), Industry Canada (IC), CE (Europe), VCCI (Japan), C-Tick (Australia/New Zealand), ANATEL (Brazil), CCC (China), KCC (Korea)

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

Warranty

- Limited One Year
- For warranty details, visit www.extremenetworks.com/go/warranty

Technical Specifications

Summit WM3600

Cluster Capacity

- Version 4.x: Up to 12 controllers; supports Active:Active/Active:Standby configurations
- Version v5.x: Up to 2 controllers; supports Active:Active/Active:Standby configurations

AP Capacity

- Up to 256 APs; supports a combination of Altitude 3500, 4600 and 4700 with no more than 48 of Altitude 4600 APs

SSIDs

- Supports 24 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

Packet Forwarding

- 802.1D-1999 Ethernet bridging; 802.11-.802.3 bridging; 802.1Q VLAN tagging and trunking; proxy ARP; IP packet steering-redirection
- Layer 2 or Layer 3

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

Anomaly Analysis

Source Media Access Control (MAC) = Dest MAC; Illegal frame sizes; Source MAC is multicast; TKIP countermeasures; all zero addresses

Authentication

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

Transport Encryption

- WEP 40/128 (RC4), KeyGuard, WPA—TKIP, WPA2-CCMP (AES), WPA2-TKIP

IEEE 802.11w

Provides origin authentication, integrity, confidentiality and replay protection of management frames for 802.11w supported access points

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

- Layer 2/Layer 3/Layer 4 ACLs

Geofencing

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

Wireless IDS/IPS

- Some features require Motorola AirDefense Services Platform, available separately
- 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); Suspicious AP, Authorized device in ad-hoc mode, unauthorized AP using authorized SSID, EAP Flood, Fake AP Flood, IDtheft, ad-hoc advertising Authorized SSID

Wireless RADIUS Support (Standard and Extreme Networks Vendor Specific Attributes (VSA))

- User Based VLANs (Standard)
- User Based QoS (Extreme Networks VSA)
- Location Based Authentication (Extreme Networks VSA)
- Allowed ESSIDs (Extreme Networks VSA)

NAC Support with third party systems from Microsoft and Symantec

Quality of Service (QoS) Layer 3 Mobility (Inter-Subnet Roaming)

Wireless Priority

- 802.11 traffic prioritization and precedence

Wi-Fi Multimedia Extensions

- WMM
- WMM Power Save
- TSPEC Admission Control

SIP Call Admission Control

Controls the number of active SIP sessions initiated by a wireless VoIP phone

802.11k

Provides radio resource management to improve client throughput (11k client required)

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, available as demo feature in WM3400 v5.x

IPv6 Client Support

Video Optimization

- Version 5.x supports multicast-to-unicast conversion

Real Time Location System

- Version 4.x controller supports RTLS/RFID/RSSI, including third-party solutions; version 5.x does not support RTLS functionality
- 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

System Resiliency and Redundancy

- Active:Standby; Active:Active and N+1 redundancy with access point load balancing; Critical resource monitoring
- Dual Firmware bank supports Image Failover capability
- Single virtual IP (per VLAN) for a switch/contoller cluster to use as the default gateway by mobile devices or wired infrastructure
- SMART RF: Network optimization to ensure user quality of experience at all times by dynamic adjustments to channel and power (on detection of RF interference or loss of RF coverage/neighbor recovery)

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

Technical Specifications

Summit WM3600 (continued)

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

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 (RJ-45 style)

Power Specifications

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

Environmental Specifications

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

Regulatory

Standards Compliance

- RoHS: This product is in Compliance with RoHS Directive 2002/95/EEC.
- WEEE

Product Safety Specifications

- IT Equipment:
  - EN 60950-1: 2001 + A11: 2004
  - IEC 60950-1, 2001
  - UL 60950-1, first edition; CSA 60950-1, first edition
- Laser Products*:
  (*When Fiber Transceiver module fitted)
  - IEC Class 1 Laser Product
  - EN 60825-1: 1994 + A1: 2002 + A2: 2001
  - IEC 60825-1: 1993 + A1: 1997 + A2: 2001
  - 21CFR1040.10 Class IIa or II

EMC Specifications

- IT Emissions:
  EN 55022: 2006 (Class A)
- IT Immunity:
  EN 55024: 1998 + A1: 2001 + A2: 2003
- Harmonic Current Emissions:
  EN 6100-3-2: 2006 (Class D)
- Voltage Fluctuation & Flicker:
  EN 61000-3-3: 1995 + A2: 2005
- Radio Frequency Devices:
  47CFR Part 15: 1998 (FCC Part 15 Class A)
- Digital Apparatus:
  ICES 003 Class A

EMC Compliance

- FCC (USA), Industry Canada (IC), CE (Europe), VCCI (Japan), C-Tick (Australia/New Zealand), ANATEL (Brazil), CCC (China), KCC (Korea)

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

Warranty

- Limited One Year
- For warranty details, visit www.extremenetworks.com/go/warranty

Technical Specifications

Summit WM3700

Cluster Capacity

- Version 4.x: Up to 12 controllers; supports Active:Active/Active:Standby configurations
- Version v5.x: Up to 2 controllers; supports Active:Active/Active:Standby configurations

AP Capacity

- Up to 1,024 APs; supports a combination of Altitude 3500, 4600 and 4700 with no more than 256 of Altitude 4600 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

Packet Forwarding

- 802.1D-1999 Ethernet bridging; 802.11-.802.3 bridging; 802.1Q VLAN tagging and trunking; proxy ARP; IP packet steering-redirection

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

Anomaly Analysis

Source Media Access Control (MAC) = Dest MAC; Illegal frame sizes; Source MAC is multicast; TKIP countermeasures; all zero addresses

Authentication

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

Transport Encryption

- WEP 40/128 (RC4), KeyGuard, WPA—TKIP, WPA2-CCMP (AES), WPA2-TKIP

IEEE 802.11w

Provides origin authentication, integrity, confidentiality and replay protection of management frames for 802.11w supported access points

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

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

Access Control Lists

- Layer 2/Layer 3/Layer 4 ACLs

Geofencing

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

Wireless IDS/IPS

- Some features require Motorola AirDefense Services Platform, available separately
- Multi-mode rogue AP detection
- Rogue AP Containment
- 802.11n Rogue Detection
- Ad-Hoc; Network Detection

Wireless RADIUS Support (Standard and Extreme Networks Vendor Specific Attributes (VSA))

- User Based VLANs (Standard)
- User Based QoS (Extreme Networks VSA)
- Location Based Authentication (Extreme Networks VSA)
- Allowed ESSIDs (Extreme Networks VSA)

NAC Support with third party systems from Microsoft and Symantec

Quality of Service (QoS) Layer 3 Mobility (Inter-Subnet Roaming)

Wireless Priority

- 802.11 traffic prioritization and precedence

Wi-Fi Multimedia Extensions

- WMM
- WMM Power Save
- TSPEC Admission Control

SIP Call Admission Control

Controls the number of active SIP sessions initiated by a wireless VoIP phone

802.11k

Provides radio resource management to improve client throughput (11k client required)

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, available as demo feature in WM3400 v5.x

IPv6 Client Support

Video Optimization

- Version 5.x supports multicast-to-unicast conversion

Real Time Location System

- Version 4.x controller supports RTLS/RFID/ RSSI, including third-party solutions; version 5.x does not support RTLS functionality
- 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

System Resiliency and Redundancy

- Active:Standby; Active:Active and N+1 redundancy with access point load balancing; Critical resource monitoring
- Dual Firmware bank supports Image Failover capability
- Single virtual IP (per VLAN) for a switch/ contoller cluster to use as the default gateway by mobile devices or wired infrastructure
- SMART RF: Network optimization to ensure user quality of experience at all times by dynamic adjustments to channel and power (on detection of RF interference or loss of RF coverage/neighbor recovery)

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

Interfaces

- 4x 10/100/1000 Cu/SFP Ethernet
- 1x 10/100 Management port
- 1x CF card slot
- 2x USB ports
- 1x serial port (RJ-45 style)

Technical Specifications

Summit WM3700 (continued)

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

Regulatory

Standards Compliance

- RoHS: This product is in Compliance with RoHS Directive 2002/95/EEC.
- WEEE

Safety Specifications

- IT Equipment:
  - EN 60950-1:2001 + A11: 2004
  - IEC 60950-1: 2001:
  - UL 60950-1, first edition; CSA 60950-1, first edition
- Laser Products*:
  (*When Fiber Transceiver module fitted)
  - EN 60825-1: 1994 + A1: 2002 + A2: 2001
  - IEC 60825-1: 1993 + A1: 1997 + A2: 2001
  - 21CFR1040.10 Class IIa or II

EMC Specifications

- IT Emissions:
  EN 55022: 1998 + A2: 2003 (Class A)
- IT Immunity:
  EN 55024: 1998 + A2: 2003
- Harmonic Current Emissions:
  EN 6100-3-2: 2000 + A1: 2001
- Voltage Fluctuation & Flicker:
  EN 61000-3-3: 1995 + A1: 2001
- Radio Frequency Devices:
  47CFR15: 1998 (FCC Part 15 Class A)
- Interface Equipment:
  ICES 003 Class A

EMC Compliance

- FCC (USA), Industry Canada (IC), CE (Europe), VCCI (Japan), C-Tick (Australia/New Zealand), ANATEL (Brazil), CCC (China), KCC (Korea)

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

Warranty

- Limited One Year
- For warranty details, visit www.extremenetworks.com/go/warranty

Ordering Information

Part Number	Description
Summit WM3400	
15717	Summit WM3400 WLAN controller with 6 AP support. Includes IPSEC VPN/firewall/WIPS security, location engine and 3G failover.
10051	SFP-SX optical module for use with Summit WM3000 series controller.
15738	Rack mount kit for mounting Summit WM3400 controller and the power module to a 19' rack. Optional accessory.
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.

Make Your Network Mobile

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 +65 6836 5437

Japan
Phone +81 3 5842 4011

extremenetworks.com