

Summit® WM3000 Series Controller System Reference Guide

Software Version 4.4

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
<http://www.extremenetworks.com>

Published: February 2012
Part number: 120761-00 Rev 01



AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrives, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, SentiAnt, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrives logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2012 Extreme Networks, Inc. All Rights Reserved.

Table of Contents

Chapter 1: About This Guide	13
Introduction.....	13
Documentation Set.....	13
Document Conventions.....	14
Notational Conventions.....	14
Chapter 2: Overview	15
Access Port and Access Point.....	15
Hardware Overview.....	16
Physical Specifications.....	17
Power Consumption.....	17
Power Protection.....	18
Cabling Requirements.....	18
Software Overview.....	18
Infrastructure Features.....	19
Installation Feature.....	19
Configuration Management.....	19
Diagnostics.....	20
Serviceability.....	20
Tracing / Logging.....	20
Process Monitor.....	21
Hardware Abstraction Layer and Drivers.....	21
Redundancy.....	21
Secure Network Time Protocol (SNTP).....	21
Wireless Switching.....	22
Adaptive AP.....	22
Physical Layer Features.....	23
Rate Limiting.....	24
Proxy-ARP.....	25
HotSpot / IP Redirect.....	25
IDM (Identity Driven Management).....	25
Voice Prioritization.....	26
Self Healing.....	26
Wireless Capacity.....	27
AP and MU Load Balancing.....	27
Wireless Roaming.....	28
QoS.....	29
WMM-Unscheduled APSD.....	30
Multiple VLANs per WLAN.....	30
Wired Switching.....	32
DHCP Servers.....	32
DHCP User Class Options.....	32
DDNS.....	32
VLAN Enhancements.....	33
Interface Management.....	33
Management Features.....	33
Security Features.....	33
Encryption and Authentication.....	34
MU Authentication.....	35

Secure Beacon	35
MU to MU Disallow	35
802.1x Authentication	36
WIPS	36
Rogue AP Detection	37
ACLs	38
Local RADIUS Server	38
IPSec VPN	38
NAT	39
Certificate Management	39
NAC	39
Supported Access Ports/Points	40
Access Port and Access Point Features	40
IEEE Standards Support	42
Standards Support	46
Chapter 3: Controller Web UI Access and Image Upgrades	49
Accessing the Controller Web UI	49
Web UI Requirements	49
Connecting to the Controller Web UI	49
Upgrading the Controller Image	51
Auto Installation	51
Chapter 4: Controller Information	55
Viewing the Controller Interface	55
Setting the Controller Country Code	56
Viewing the Controller Configuration	56
Controller Dashboard Details	59
Summit WM3400 Controller Dashboard	60
Summit WM3600 Controller Dashboard	62
Summit WM3700 Controller Dashboard	64
Viewing Controller Statistics	66
Viewing Controller Port Information	68
Viewing the Port Configuration	68
Editing the Port Configuration	70
Viewing the Ports Runtime Status	71
Reviewing Port Statistics	72
Detailed Port Statistics	74
Viewing the Port Statistics Graph	75
Power over Ethernet (PoE)	77
Editing Port PoE Settings	78
Configuring WAN Interface Cards	79
Viewing Controller Configurations	81
Viewing the Detailed Contents of a Config File	83
Transferring a Config File	85
Viewing Controller Firmware Information	86
Editing the Controller Firmware	88
Enabling Global Settings for the Image Failover	89
Updating the Controller Firmware	89
Controller File Management	91
Transferring Files	91
Transferring a file from Wireless Controller to Wireless Controller	93
Transferring a File from a Wireless Controller to a Server	94
Transferring a File from a Server to a Wireless Controller	95
Viewing Files	96
Configuring Automatic Updates	98
Viewing the Controller Alarm Log	100

Viewing Alarm Log Details	102
Viewing Controller Licenses	102
How to use the Filter Option	104
Chapter 5: Network Setup.....	105
Displaying the Network Interface.....	105
Viewing Network IP Information	107
Configuring DNS	107
Adding an IP Address for a DNS Server.....	109
Configuring Global Settings	109
Configuring IP Forwarding	110
Adding a New Static Route	112
Viewing Address Resolution	113
Viewing and Configuring Layer 2 Virtual LANs.....	114
Viewing and Configuring VLANs by Port.....	115
Editing the Details of an Existing VLAN by Port.....	116
Viewing and Configuring Ports by VLAN.....	117
Configuring Controller Virtual Interfaces.....	120
Configuring the Virtual Interface.....	121
Adding a Virtual Interface.....	122
Modifying a Virtual Interface	124
Viewing Virtual Interface Statistics	125
Viewing Virtual Interface Statistics	127
Viewing the Virtual Interface Statistics Graph.....	128
Viewing and Configuring Controller WLANs.....	129
Configuring WLANs.....	130
Editing the WLAN Configuration	134
Assigning Multiple VLANs per WLAN	140
Configuring Authentication Types	142
Configuring Different Encryption Types	163
Viewing WLAN Statistics.....	169
Viewing WLAN Statistics in Detail.....	170
Viewing WLAN Statistics in a Graphical Format	173
Viewing WLAN Controller Statistics	174
Configuring WMM	176
Editing WMM Settings.....	179
Configuring the NAC Inclusion List	180
Adding an Include List to a WLAN	182
Configuring Devices on the Include List.....	182
Mapping Include List Items to WLANs	183
Configuring the NAC Exclusion List	184
Adding an Exclude List to the WLAN	186
Configuring Devices on the Exclude List	186
Mapping Exclude List Items to WLANs.....	187
NAC Configuration Examples Using the Controller CLI	188
Creating an Include List	189
Creating an Exclude List	189
Configuring the WLAN for NAC	189
Viewing Associated MU Details.....	190
Viewing MU Status.....	191
Viewing MU Details	192
Assigning MAC Names	194
Configuring 802.11.k Radio Resource Management	194
Configuring Mobile Units	195
MAC Naming of Mobile Units	196
Viewing MU Statistics.....	196
Viewing MU Statistics in Detail	198

View an MU Statistics Graph	200
Viewing MU Voice Statistics.....	202
Viewing Access Port/Point Information.....	203
Configuring Access Port/Point Radios	204
Configuring an AP Mesh Network	207
Configuring an AP's Global Settings.....	209
Editing AP Settings	212
Adding APs	219
Viewing AP Statistics	221
Viewing AP Statistics in Detail	222
Viewing AP Statistics in Graphical Format.....	224
Configuring WLAN Assignment.....	225
Editing a WLAN Assignment.....	226
Configuring WMM	227
Editing WMM Settings.....	229
Configuring Access Point Radio Bandwidth.....	230
Configuring Radio Groups for MU Load Balancing	231
Viewing Access Point Radio Groups	233
Viewing Active Calls (AC) Statistics	234
Viewing Mesh Statistics	235
Smart RF.....	236
Smart RF Calibration Phase	236
Smart RF Monitoring Phase.....	237
Viewing Smart RF Information	238
Editing Smart RF Radio Settings	241
Viewing Smart RF History	243
Configuring Smart RF Settings	244
Voice Statistics	248
Viewing Access Point Adoption Defaults.....	249
Configuring AP Adoption Defaults.....	250
Editing Default Access Port/Point Adoption Settings	251
Configuring Layer 3 Adoption.....	256
Configuring WLAN Assignment.....	258
Configuring WMM	259
Editing Access Port/Point Adoption WMM Settings	261
Configuring Access Ports/Points	262
Viewing Adopted Access Ports/Points	262
Viewing Unadopted Access Ports/Points	265
Access Port/Point Configuration	266
Editing Access Port/Point Settings.....	268
Configuring a Syslog Server on the AAP from the controller	269
Configuring LLDP Settings for Access Port	270
Viewing Sensor Information	271
Configuring Secure WiSPe	272
Configuring Adaptive AP Firmware	273
Editing an Existing AP Firmware Image.....	275
Updating an existing AAP Image Firmware	276
Updating an AAP Image/Firmware using SFTP	277
Configuring IP Filtering.....	277
Multiple Spanning Tree	280
Configuring a Bridge	281
Viewing and Configuring Bridge Instance Details	285
Creating a Bridge Instance	286
Associating VLANs to a Bridge Instance	286
Configuring a Port	287
Editing an MSTP Port Configuration	290
Viewing and Configuring Port Instance Details	291
Editing a Port Instance Configuration	293

IGMP Snooping	293
IGMP Snoop Configuration	294
IGMP Snoop Querier Configuration	295
Wired Hotspot.....	297
Wired Hotspot Configuration	298
Configuring an Internal Hotspot	298
Configuring an External Hotspot	302
Configuring an Advanced Hotspot	303
Configuring a RADIUS Server	305
Chapter 6: Controller Services.....	309
Displaying the Services Interface	309
DHCP Server Settings.....	311
Configuring the Controller DHCP Server.....	311
Editing the Properties of an Existing DHCP Pool.....	313
Adding a New DHCP Pool	314
Configuring DHCP Global Options.....	317
Configuring DHCP Server DDNS Values.....	317
Viewing the Attributes of Existing Host Pools.....	318
Configuring Excluded IP Address Information.....	320
Configuring the DHCP Server Relay	321
Viewing DDNS Bindings.....	324
Viewing DHCP Bindings.....	325
Reviewing DHCP Dynamic Bindings.....	326
Configuring the DHCP User Class	328
Adding a New DHCP User Class	329
Editing the Properties of an Existing DHCP User Class	330
Configuring DHCP Pool Class.....	331
Editing an Existing DHCP Pool Class	332
Adding a New DHCP Pool Class	332
Configuring Secure NTP	333
Defining the SNTP Configuration	334
Configuring Symmetric Key.....	336
Defining an NTP Neighbor Configuration	338
Adding an NTP Neighbor	340
Viewing NTP Associations	341
Viewing NTP Status	343
Configuring Controller Redundancy and Clustering	345
Configuring Redundancy Settings.....	347
Reviewing Redundancy Status	350
Configuring Redundancy Group Membership.....	353
Displaying Redundancy Member Details	354
Adding a Redundancy Group Member	356
Redundancy Group License Aggregation Rules	357
Managing Clustering Using the Web UI	358
Layer 3 Mobility	359
Configuring Layer 3 Mobility.....	359
Defining the Layer 3 Peer List.....	362
Reviewing Layer 3 Peer List Statistics	363
Reviewing Layer 3 MU Status.....	365
Configuring Self Healing.....	366
Configuring Self Healing Neighbor Details	368
Editing the Properties of a Neighbor	369
Configuring Controller Discovery.....	370
Configuring Discovery Profiles	372
Adding a New Discovery Profile.....	374
Viewing Discovered Controllers	374

Locating	376
RTLS Overview	377
SOLE—Smart Opportunistic Location Engine.....	377
Defining Site Parameters	378
Adding AP Location Information	380
Configuring SOLE Parameters.....	381
Configuring Aeroscout Parameters	383
Configuring Ekahau Parameters	385
Chapter 7: Controller Security	387
Displaying the Main Security Interface	387
Access Point Detection	389
Enabling and Configuring AP Detection.....	389
Adding or Editing an Allowed AP	392
Authorized / Ignored APs	393
Unauthorized APs (AP Reported)	395
Unauthorized APs (MU Reported).....	396
AP Containment	398
Wireless IDS/IPS.....	399
Configuring Wireless IDS/IPS	400
Viewing Filtered MUs	402
Configuring Firewalls and Access Control Lists	403
ACL Overview	404
Router ACLs	405
Port ACLs.....	406
Wireless LAN ACLs	407
ACL Actions	407
Precedence Order.....	407
Attaching an ACL on a WLAN Interface/Port	408
Adding or Editing a New ACL WLAN Configuration.....	409
Attaching an ACL Layer 2/Layer 3 Configuration.....	410
Adding a New ACL Layer 2/Layer 3 Configuration	412
Configuring the Role Based Firewall.....	412
Configuring the Role Based Firewall.....	414
Configuring Wireless Filters	414
Editing an Existing Wireless Filter	416
Adding a new Wireless Filter.....	417
Associating an ACL with WLAN	419
Configuring the Firewall	420
Adding a New ACL.....	421
Adding a New ACL Rule	422
Editing an Existing Rule	424
Configuring Layer 2 Firewall	425
Adding Layer 2 Firewall Configurations	427
Configuring WLAN Firewall rules	428
Adding a new WLAN Firewall Rule	430
Configuring Denial of Service (DoS) Attack Firewall Rules.....	432
Configuring the Role	434
Creating a new Role	436
Configuring Firewall Logging Options	439
Reviewing Firewall and ACL Statistics	441
Reviewing ACL Statistics	441
Viewing DHCP Snoop Entry Statistics	443
Viewing Role Based Firewall Statistics	445
Configuring NAT Information.....	445
Defining Dynamic NAT Translations	446
Adding a New Dynamic NAT Configuration	448
Defining Static NAT Translations	449

Adding a New Static NAT Configuration	451
Configuring NAT Interfaces	453
Viewing NAT Status	455
Configuring IKE Settings	457
Defining the IKE Configuration	457
Setting IKE Policies	459
Viewing SA Statistics	463
Configuring IPsec VPN	465
Defining the IPsec Configuration	467
Editing an Existing Transform Set	468
Adding a New Transform Set	470
Defining the IPsec VPN Remote Configuration	471
Configuring IPsec VPN Authentication	473
Configuring Crypto Maps	476
Crypto Map Entries	478
Crypto Map Peers	481
Crypto Map Manual SAs	483
Crypto Map Transform Sets	485
Crypto Map Interfaces	487
Viewing IPsec Security Associations	488
Configuring the RADIUS Server	489
RADIUS Overview	490
User Database	491
Authentication of Terminal/Management User(s)	492
Access Policy	492
Proxy to External RADIUS Server	492
LDAP	492
Accounting	492
Using the Controller's RADIUS Server Versus an External RADIUS	492
Defining the RADIUS Configuration	493
RADIUS Client Configuration	494
RADIUS Proxy Server Configuration	495
Configuring RADIUS Authentication and Accounting	496
Configuring RADIUS Users	499
Configuring RADIUS User Groups	503
Viewing RADIUS Accounting Logs	508
Creating Server Certificates	509
Using Trustpoints to Configure Certificates	509
Creating a Server / CA Root Certificate	512
Certificate Authority Root Certificates	520
Configuring Trustpoint Associated Keys	520
Adding a New Key	521
Transferring Keys	522
Configuring Enhanced Beacons and Probes	523
Configuring the Beacon Table	524
Configuring the Probe Table	526
Reviewing Found Beacons	528
Reviewing Found Probes	529
Chapter 8: Controller Management	531
Displaying the Management Access Interface	531
Configuring Access Control	533
Configuring SNMP Access	535
Configuring SNMP v1/v2 Access	535
Editing an Existing SNMP v1/v2 Community Name	536
Configuring SNMP V3 Access	537
Editing an SNMP v3 Authentication and Privacy Password	539

Accessing SNMP v2/v3 Statistics.....	540
Message Parameters	541
Configuring SNMP Traps.....	542
Enabling Trap Configuration	542
Configuring Email Notifications	545
Configuring Trap Thresholds.....	546
Wireless Trap Threshold Values.....	549
Configuring SNMP Trap Receivers	550
Editing SNMP Trap Receivers.....	552
Adding SNMP Trap Receivers	552
Configuring Management Users.....	553
Configuring Local Users	553
Creating a New Local User	554
Modifying an Existing Local User	557
Creating a Guest Admin and Guest User	558
Configuring Controller Authentication	560
Modifying the Properties of an Existing RADIUS Server.....	561
Adding an External RADIUS Server	563
External RADIUS Server Settings.....	564
Chapter 9: Diagnostics	565
Displaying the Main Diagnostic Interface	565
Controller Environment	566
CPU Performance	567
Controller Memory Allocation	569
Controller Disk Allocation	570
Controller Memory Processes.....	571
Other Controller Resources	572
Configuring System Logging	573
Log Options.....	573
File Management	574
Viewing the Entire Contents of Individual Log Files.....	576
Transferring Log Files	578
Reviewing Core Snapshots	580
Transferring Core Snapshots	581
Reviewing Panic Snapshots.....	582
Viewing Panic Details.....	583
Transferring Panic Files	583
Debugging the Applet.....	585
Configuring a Ping.....	586
Modifying the Configuration of an Existing Ping Test.....	588
Adding a New Ping Test.....	589
Viewing Ping Statistics	590
Appendix A: Customer Support.....	593
Registration	593
Documentation	593
Appendix B: Adaptive AP Overview	595
Adaptive AP Overview.....	595
Where to Go From Here.....	596
Adaptive AP Management	596
Licensing	596
Controller Discovery.....	596
Auto Discovery using DHCP	597
Manual Adoption Configuration.....	598
Securing a Configuration Channel Between Controller and AP	598

Adaptive AP WLAN Topology	598
Configuration Updates	598
Securing Data Tunnels between the Controller and AAP	599
Adaptive AP Controller Failure	599
Remote Site Survivability (RSS).....	599
Adaptive Mesh Support.....	599
AAP RADIUS Proxy Support.....	601
Supported Adaptive AP Topologies	602
Topology Deployment Considerations	602
Extended WLANs Only	603
Independent WLANs Only.....	603
Extended WLANs with Independent WLANs	603
Extended VLAN with Mesh Networking.....	603
How the AP Receives its Adaptive Configuration.....	604
Adaptive AP Prerequisites	604
Configuring the Adaptive AP for Adoption by the Controller	605
Configuring the Controller for Adaptive AP Adoption	605
Establishing Basic Adaptive AP Connectivity.....	605
Adaptive AP Configuration	606
Adopting an Adaptive AP Manually.....	606
Adopting an Adaptive AP Using a Configuration File.....	608
Adopting an Adaptive AP Using DHCP Options	608
Controller Configuration	609
Adaptive AP Deployment Considerations	612
Sample Controller Configuration File for IPsec and Independent WLAN	612
Appendix C: Troubleshooting Information	617
General Troubleshooting.....	617
Wireless Controller Issues.....	617
Controller Does Not Boot Up	618
Controller Does Not Obtain an IP Address through DHCP	618
Unable to Connect to the Controller using Telnet or SSH.....	618
Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond	619
Console Port is Not Responding	619
Access Port/Point Issues	620
Access Ports/Points are Not Adopted.....	620
Access Ports/Points are Not Responding	621
Sensor Port frequently goes up and down.....	621
Mobile Unit Issues.....	621
Access Port/Point Adopted, but MU is Not Being Associated.....	621
MUs Cannot Associate and/or Authenticate with Access Ports/Points.....	622
Poor Voice Quality Issues	622
Miscellaneous Issues	622
Excessive Fragmented Data or Excessive Broadcast	622
Excessive Memory Leak	623
System Logging Mechanism	623
Troubleshooting SNMP Issues.....	623
MIB Browser not able to contact the agent	623
Not able to SNMP WALK for a GET.....	624
MIB not visible in the MIB browser	624
SNMP SETs not working.....	624
Not receiving SNMP traps.....	624
Additional Configuration	624
Security Issues	624
Controller Password Recovery.....	624
RADIUS Troubleshooting.....	625
RADIUS Server does not start upon enable	625
RADIUS Server does not reply to my requests.....	626

RADIUS Server is rejecting the user.....	626
Time of Restriction configured does not work.....	626
Authentication fails at exchange of certificates.....	626
When using another Summit WM3700 (controller 2) as RADIUS server, access is rejected.....	626
Authentication using LDAP fails.....	627
VPN Authentication using onboard RADIUS server fails.....	627
Accounting does not work with external RADIUS Accounting server.....	627
Troubleshooting RADIUS Accounting Issues.....	627
Rogue AP Detection Troubleshooting.....	628
Troubleshooting Firewall Configuration Issues.....	628
Configuration Issue 1.....	628
Configuration Issue 2.....	629
Configuration Issue 3.....	629
Configuration Issue 4.....	629
Appendix D: Open Source Software Information.....	631
Open Source Software Used.....	631
OSS Licenses.....	632
Appendix E: Best Practices.....	633
ACL configuration to reduce the amount of broadcast or multicast traffic in the network.....	633
Settings to reduce DHCP and ARP traffic on air.....	634
Settings to set the rate at which multicast and broadcast packets are sent.....	634
Remove DFS channels from ACS.....	634
Operate a 11bgn radio in the 20MHz band.....	635
Enable Dynamic Chain Selection.....	635
Disable Stateful Firewall Inspection Engine.....	635
Disable Cluster Master Support.....	635
Disable MSTP if not used in the network.....	636

1

CHAPTER

About This Guide

Introduction

This guide provides information about using the following Extreme Networks® wireless LAN controllers:

- Summit® WM3400 wireless LAN controller
- Summit WM3600 wireless LAN controller
- Summit WM3700 wireless LAN controller



NOTE

Screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set



NOTE

Check for the latest versions of documentation on the Extreme Networks documentation website at: <http://www.extremenetworks.com/go/documentation>.

The documentation set for the Extreme Networks wireless LAN controllers is partitioned into the following guides to provide information for specific user needs.

- **Installation Guides**—Each controller has a unique Installation Guide which describes the basic hardware setup and configuration required to transition to more advanced configuration of the controllers.
- **Summit WM3000 Series Controller System Reference Guide**—Describes configuration of the Extreme Networks Summit Wireless LAN Controllers using the Web UI.
- **Summit WM3000 Series Controller CLI Reference Guide**—Describes the *Command Line Interface (CLI)* and *Management Information Base (MIB)* commands used to configure the Extreme Networks Summit Wireless LAN Controllers.

- *Wireless Management Suite* (WMS)—Describes how to use Extreme Networks WMS to set up and monitor your wireless controller in respect to areas of good RF throughput and defined physical barriers.

Document Conventions

The following conventions are used in this document to draw your attention to important information:



NOTE

Indicate tips or special requirements.



CAUTION

Indicates conditions that can cause equipment damage or data loss.



WARNING!

Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following additional notational conventions are used in this document:

- *Italics* are used to highlight the following:
 - Chapters and sections in this and related documents
 - Dialog box, window and screen names
 - Drop-down list and list box names
 - Check box and radio button names
 - Icons on a screen.
- *GUI* text is used to highlight the following:
 - Screen names
 - Menu items
 - Button names on a screen.
- Bullets (●) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

2 Overview

CHAPTER

An Extreme Networks wireless LAN controller is a centralized management solution for wireless networking. It connects to Access Ports through Layer 2 or Layer 3, and Access Points through Layer 3.



NOTE

The discussion of the controller GUI within this guide is presented generically, making it equally relevant to the Summit WM3400, Summit WM3600 and Summit WM3700 controller platforms. However, some subtle differences do exist among these baselines. These differences are noted within the specific GUI elements impacted. When these differences are noted, the options available to each controller baseline are described in detail.

Access Port and Access Point

Access Port, Access Points and Adaptive Access Point (AAP) are frequently used throughout the text of this document. The functional differences between these terminologies are explained below:

Access Port in this guide refers specifically to a special type of 802.11 access point, such as an AP4600 Access Port device, on which only portion of the 802.11 packet processing is conducted and the rest of the 802.11 packet processing, such as the 802.11 encryption/decryption function, is carried out on the controller. The Access Port and the controller are linked by a tunnel called WISPe (Enhanced Wireless Switch Platform). The packet on the tunnel may still be encrypted with WEP, WPA or WPA2 as defined in the 802.11 standards and contains 802.11 information. An Access Port is also commonly named as “thin” Access Point or “Split MAC” Access Point. Access Ports function as controller managed radio antennas for data traffic management and routing. Wireless network configuration and intelligence resides with the controller. A controller uses Access Ports to bridge data to and from connected wireless devices. The controller applies appropriate policies to data packets before forwarding them to their destination. An Access Port's configuration is managed by the controller through a Web UI Graphical User Interface (GUI), SNMP or the controller's Command Line Interface (CLI). An Access Port receives 802.11x data from wireless clients and forwards the data to the controller which applies appropriate policies and routes the packets to their destinations.

On the other hand, the term Access Point used in this guide refers to a more generic 802.11 access point, such as an Altitude™ AP35xx Access Point device, with complete 802.11 PHY and MAC functions, including the 802.11 encryption/decryption function. The 802.11 information is not present on the packets coming in to or going out of the wired Ethernet port of an Access Point. In addition, an Access Point may function as an integrated router, gateway, firewall, DHCP and AAA RADIUS server, as well as a VPN client and hot-spot gateway. An Access Point can be configured to operate independently as a

standalone device without the control by a wireless controller (so called “thick” or “fat” AP mode). It can also be configured to operate with a controller (namely, to get adopted by a controller). An Access Point in this operation mode is called Adaptive Access Point (AAP). An AAP is an Access Point that can adopt like an Access Port. The management of an AAP is conducted by the controller, once the Access Point connects to a controller and receives its AAP configuration. An AAP provides two concurrent network services for the wireless clients: bridge traffic at the AP (Independent WLAN mode) and tunnel client traffic to the controller (Extended WLAN mode). The AAP Independent WLAN mode may offer identical functions as a standalone Access Point except that it is managed by a controller. The AAP Extended WLAN mode is similar to an Access Port in many of its functions. However, the key difference is that the 802.11 encryption/decryption function of an AAP resides on the AP, not on the controller. There is a tunnel, called WISPh (Hybrid Wireless Switch Platform), between the controller and the AAP for control traffic and data traffic (Extended WLAN). WISPh is a CAPWAP-like encapsulation protocol. It enables better wireless network security and faster roaming. AAP provides a flexible network architecture that allows better traffic load balance between the network core and the edge. Once an Access Point receives its AAP configuration, its WLAN and radio configuration is similar to an Access Port. An AAP's radio mesh configuration can also be configured from the controller. However, non-wireless features (DHCP, NAT, Firewall etc.) cannot be configured from the controller and must be defined using the Access Point's resident interfaces before its conversion to an AAP. For more details regarding AAPs, refer to [“Adaptive AP Overview” on page 595](#).

For better security, the controller-Access Port (AP4600) control packets encapsulated with WISPe can be encrypted by enabling the Secured WISPe feature. By default, it is not encrypted. For an AAP (AP35xx), the WISPh tunnel can also be encrypted with IPSec VPN to protect the control traffic and the data traffic. When in cluster mode, Generic Routing Encapsulation (GRE) is used for the controller-controller tunnel. The controller-controller GRE tunnel can be encrypted with IPSec VPN.

In terms of functionality, an AP4600 Series device is an Access Port, and an AP35xx device is an Access Point. Currently, only the AAP mode of the AP35xx Access Point is supported. The standalone mode of AP35xx is not supported.

The acronym “AP” may be short for an Access Port or an Access Point.

Hardware Overview

The Summit WM3400, Summit WM3600 and Summit WM3700 are rack-mountable devices that manage all inbound and outbound traffic on the wireless network. They provide security, network service and system management applications.

Unlike traditional wireless infrastructure devices that reside at the edge of a network, the controller uses centralized, policy-based management to apply sets of rules or actions to all devices on the wireless network. The controller collects management “intelligence” from individual Access Ports/Points and moves the collected information to the centralized controller.

Access Points or Access Ports are 48V Power-over-Ethernet devices. The Altitude 3510 AP, AP4600 APs and Altitude 4700 APs are powered by standard 802.3af POE source. The Altitude 3550 outdoor AP must be powered by a special Extreme Networks POE injector (Power Tap).

Access Ports do not have software or firmware upon initial receipt from the factory. When the Access Port is first powered on and cleared for the network, the controller initializes the Access Port and installs a small firmware file automatically. Therefore, installation and firmware upgrades are automatic and transparent.

Physical Specifications

The physical dimensions and operating parameters of the Summit WM3400 include:

Width	304.8mm (12.0 in)
Height	44.45mm (1.75 in)
Depth	254mm (10.0 in)
Weight	2.15 Kg (4.75 lbs)
Operating Temperature	0°C–40°C (32°F–104°F)
Operating Humidity	5%–85% RH, non-condensing

The physical dimensions and operating parameters of the Summit WM3600 include:

Width	440mm (17.32 in)
Height	44.45mm (1.75 in)
Depth	390.8mm (15.38 in)
Weight	6.35 Kg (14 lbs)
Operating Temperature	0°C–40°C (32°F–104°F)
Operating Humidity	5%–85% RH, non-condensing

The physical dimensions and operating parameters of the Summit WM3700 include:

Width	440mm (17.32 in)
Height	44.45mm (1.75 in)
Depth	390.8mm (15.38 in)
Weight	6.12 Kg (13.5 lbs)
Operating Temperature	0°C–40°C (32°F–104°F)
Operating Humidity	5%–85% RH, non-condensing

A power cord is not supplied with a Summit WM3400, Summit WM3600 or Summit WM3700 model controller. Use only a correctly rated power cord certified for the country of operation.

Power Consumption

The power consumption for the Summit WM3400, Summit WM3600 or Summit WM3700 model controller is shown in the following table:

Summit WM3400	Maximum Power Consumption: 100W
Summit WM3600	Maximum Power Consumption: 300W
Summit WM3700	AC Input Voltage: 100-240 VAC 50/60 Hz Maximum Power Consumption: 120W

Power Protection

To best protect the controller from unexpected power surges or other power-related problems, ensure the controller installation meets the following guidelines:

- *If possible, use a dedicated circuit to protect data processing equipment.* Commercial electrical contractors are familiar with wiring for data processing equipment and can help with the load balancing of dedicated circuits.
- *Install surge protection.* Use a surge protection device between the electricity source and the controller.
- *Install an Uninterruptible Power Supply (UPS).* A UPS provides continuous power during a power outage. Some UPS devices have integral surge protection. UPS equipment requires periodic maintenance to ensure reliability.

Cabling Requirements

A minimum of one category 6 Ethernet cable (not supplied) is required to connect the controller to the LAN and WLAN. The cable(s) are used with the Ethernet ports on the front panel of the controller.



NOTE

On an Summit WM3600 and Summit WM3700, Extreme Networks recommends connecting via the Management Ethernet (ME) interface to better ensure secure and easier management. The ME interface is connected to the management VLAN, and is therefore separate from production VLANs.



NOTE

On the Summit WM3400 and Summit WM3600, the Uplink (UP) port is the preferred method of connecting the controller to the network. The Uplink port has its own dedicated 1Gbps connection which is unaffected by internal traffic across the GE ports.

The console cable included with the controller connects the controller to a computer running a serial terminal emulator program to access the controller's *Command Line Interface (CLI)* for initial configuration. An initial configuration is described within the *Installation Guide* shipped with each controller.

Software Overview

The controller includes a robust set of features. The features are listed and described in the following sections:

- [Infrastructure Features on page 19](#)
- [Wireless Switching on page 22](#)
- [Wired Switching on page 32](#)
- [Management Features on page 33](#)
- [Security Features on page 33](#)
- [Supported Access Ports/Points on page 40](#)



NOTE

The Extreme Networks Wireless Management Suite (WMS) is a recommended utility to plan the deployment of the controller and view its configuration once operational in the field. Extreme Networks WMS can help optimize the positioning and configuration of a controller in respect to a WLAN's Mobile Unit (MU) throughput requirements and can help detect rogue devices. For more information, refer to the Extreme Networks documentation website at: <http://www.extremenetworks.com/go/documentation>.

Infrastructure Features

The controller includes the following Infrastructure features:

- [Installation Feature on page 19](#)
- [Configuration Management on page 19](#)
- [Diagnostics on page 20](#)
- [Serviceability on page 20](#)
- [Tracing / Logging on page 20](#)
- [Process Monitor on page 21](#)
- [Hardware Abstraction Layer and Drivers on page 21](#)
- [Redundancy on page 21](#)
- [Secure Network Time Protocol \(SNTP\) on page 21](#)

Installation Feature

The upgrade/downgrade of the controller can be performed at boot time using one of the following methods:

- Web UI
- DHCP
- CLI
- SNMP
- Patches

The controller has sufficient non-volatile memory to store two firmware images. Having a second firmware image provides a backup in case of failure of the primary image. It also allows for testing of new firmware on a controller with the ability to easily revert to a previous image.

Configuration Management

The controller supports the redundant storage of configuration files to protect against corruption during a write operation and ensure (at any given time) a valid configuration file exists. If writing the configuration file fails, it is rolled back and a pre-write file is used.

Text Based Configuration. The configuration is stored in human readable format (as a set of CLI commands).

Diagnostics

The following diagnostics are available:

- 1 *In-service Diagnostics*—In-service diagnostics provide a range of automatic health monitoring features ensuring both the system hardware and software are in working order. In-service-diagnostics continuously monitor available physical characteristics (as detailed below) and issue log messages when warning or error thresholds are reached. There are three types of in-service diagnostics:
 - *Hardware*—Ethernet ports, chip failures, system temperature via the temperature sensors provided by the hardware, etc.
 - *Software*—CPU load, memory usage, etc.
 - *Environmental*—CPU and air temperature, fans speed, etc.
- 2 *Out-of-service Diagnostics*—Out-of-service diagnostics are a set of intrusive tests run from the user interface. Out-of-service diagnostics cannot be run while the controller is in operation. Intrusive tests include:
 - Ethernet loopback tests
 - RAM tests, Real Time Clock tests, etc.
- 3 *Manufacturing Diagnostics*—Manufacturing diagnostics are a set of diagnostics used by manufacturing to inspect quality of hardware.

Serviceability

A special set of Service CLI commands are available to provide additional troubleshooting capabilities for service personnel (access to Linux services, panic logs, etc.). Only authorized users or service personnel are provided access to the Service CLI.

A built-in Packet Sniffer enables service personnel and users to capture incoming and outgoing packets in a buffer.

The controller also collects statistics for RF activity, Ethernet port activity etc. RF statistics include roaming stats, packet counters, octets tx/rx, signal, noise SNR, retry, and information for each MU.

Tracing / Logging

Log messages are well-defined and documented system messages with various destinations. They are numbered and referenced by ID. Each severity level group, can be configured separately to go to either the serial console, telnet interface, log file or remote syslog server.

Trace messages are more free-form and are used mainly by support personnel for tracking problems. They are enabled or disabled via CLI commands. Trace messages can go to a log file, the serial console, or the current tty.

Log and trace messages are interleaved in the same log file, so chronological order is preserved. Log and trace messages from different processes are similarly interleaved in the same file for the same reason.

Log message format is similar to the format used by syslog messages (RFC 3164). Log messages include message severity, source (facility), the time the message was generated and a textual message describing the situation triggering the event. For more information on using the controller logging functionality, see [“Configuring System Logging” on page 573](#).

Process Monitor

The controller Process Monitor checks to ensure processes under its control are up and running. Each monitored process sends periodic heartbeat messages. A process that is down (due to a software crash or stuck in an endless loop) is detected when its heartbeat is not received. Such a process is terminated (if still running) and restarted (if configured) by the Process Monitor.

Hardware Abstraction Layer and Drivers

The *Hardware Abstraction Layer (HAL)* provides an abstraction library with an interface hiding hardware/platform specific data. Drivers include platform specific components such as Ethernet, Flash Memory storage and thermal sensors.

Redundancy

Using the controller redundancy, up to 12 controllers can be configured in a redundancy group (and provide group monitoring). In the event of a controller failure, an existing cluster member assumes control. Therefore, the controller supported network is always up and running even if a controller fails or is removed for maintenance or a software upgrade.

The following redundancy features are supported:

- Up to 12 controller redundancy members are supported in a single group. Each member is capable of tracking statistics for the entire group in addition to their own.
- 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 are load balanced across members of the group.
- Licenses are aggregated across the group. When a new member joins the group, the new member can leverage the Access Port/Point adoption license(s) of existing members.
- Each member of the redundancy group (including the reporting controller) is capable of displaying cluster performance statistics for all members in addition to their own.
- Centralized redundancy group management using the controller CLI.

For more information on configuring the controller for redundancy support, see [“Configuring Controller Redundancy and Clustering” on page 345](#).

Secure Network Time Protocol (SNTP)

Secure Network Time Protocol (SNTP) manages time and/or network clock synchronization within the controller managed network. SNTP is a client/server implementation. The controller (an SNTP client) periodically synchronizes its clock with a master clock (an NTP server). For example, the controller resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server. Time synchronization is recommended for the controller’s network operations. The following holds true:

- The controller can be configured to provide NTP services to NTP clients.
- The controller can provide NTP support for user authentication.
- *Secure Network Time Protocol (SNTP)* clients can be configured to synchronize controller time with an external NTP server.

For information on configuring the controller to support SNTP, see [“Configuring Secure NTP” on page 333](#).

Wireless Switching

The controller includes the following wireless switching features:

- [Adaptive AP on page 22](#)
- [Physical Layer Features on page 23](#)
- [Rate Limiting on page 24](#)
- [Proxy-ARP on page 25](#)
- [HotSpot / IP Redirect on page 25](#)
- [IDM \(Identity Driven Management\) on page 25](#)
- [Voice Prioritization on page 26](#)
- [Self Healing on page 26](#)
- [Wireless Capacity on page 27](#)
- [AP and MU Load Balancing on page 27](#)
- [Wireless Roaming on page 28](#)
- [Power Save Polling on page 28](#)
- [QoS on page 29](#)
- [Wireless Layer 2 Switching on page 30](#)
- [Automatic Channel Selection on page 30](#)
- [WMM-Unscheduled APSD on page 30](#)
- [Multiple VLANs per WLAN on page 30](#)

Adaptive AP

An adaptive AP (AAP) is an AP3510, AP3550 or AP4700 Series Access Point adopted by a wireless controller. The management of an AAP is conducted by the controller, once the Access Point connects to the controller and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- tunneling of centralized traffic to the wireless controller



NOTE

Smart RF is not supported on adaptive APs (access points adopted by the WM controller and functioning in dependent mode). The connection between the AAP and the controller can be secured using IPsec depending on whether a secure WAN link from a remote site to the central site already exists.

The controller can be discovered using one of the following mechanisms:

- DHCP
- Controller fully qualified domain name (FQDN)
- Static IP addresses

The benefits of an AAP deployment include:

- *Centralized Configuration Management & Compliance*—Wireless configurations across distributed sites can be centrally managed by the wireless controller or cluster.
- *WAN Survivability*—Local WLAN services at remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLANs to stores for corporate visitors*—Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location.
- *Maintain local WLANs for specific applications*—WLANs created and supported locally can be concurrently supported with your existing infrastructure.

For an overview of AAP and how it is configured and deployed using the controller and Access Point, see [“Adaptive AP Overview” on page 595](#).

Physical Layer Features

802.11a.

- *DFS Radar Avoidance*—*Dynamic Frequency Selection* (DFS) is mandatory for WLAN equipment intended to operate in the frequency bands 5150 MHz to 5350 MHz and 5470 MHz to 5725 MHz when in countries of the EU.

The purpose of DFS is:

- Detect interference from other systems and avoid co-channeling with those systems (most notably radar systems).
- Provide uniform spectrum loading across all devices.

This feature is enabled automatically when the country code indicates that DFS is required for at least one of the frequency bands that are allowed in the country.

- *TPC—Transmit Power Control* (TPC) meets the regulatory requirement for maximum power and mitigation for each channel. TPC functionality is enabled automatically for every AP that operates on the channel.

802.11bg.

- *Dual mode b/g protection*—ERP builds on the payload data rates of 1 and 2 Mbit/s that use DSSS modulation and builds on the payload data rates of 1, 2, 5.5, and 11 Mbit/s, that use DSSS, CCK, and optional PBCC modulations. ERP provides additional payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s. The transmission and reception capability for 1, 2, 5.5, 11, 6, 12, and 24 Mbit/s data rates is mandatory.

Two additional optional ERP-PBCC modulation modes with payload data rates of 22 and 33 Mbit/s are defined. An ERP-PBCC station may implement 22 Mbit/s alone or 22 and 33 Mbit/s. An optional modulation mode (known as DSSS-OFDM) is also incorporated with payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s.

- *Short slot protection*—The slot time is 20 μ s, except an optional 9 μ s slot time may be used when the BSS consists of only ERP STAs capable of supporting this option. The optional 9 μ s slot time should not be used if the network has one or more non-ERP STAs associated. For IBSS, the Short Slot Time field is set to 0, corresponding to a 20 μ s slot time.

802.11n.

IEEE 802.11n is an amendment to IEEE 802.11, and builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO) and 40 MHz channels to the PHY (physical layer), and frame aggregation to the MAC layer. Coupling MIMO architecture with wider bandwidth channels offers increased physical transfer rate over 802.11a (5 GHz) and 802.11g (2.4 GHz).

- MIMO is a technology which uses multiple antennas to coherently resolve more information than possible using a single antenna. One way it provides this is through Spatial Division Multiplexing (SDM). SDM spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth. MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires a discrete antenna at both the transmitter and the receiver. In addition, MIMO technology requires a separate radio frequency chain and analog-to-digital converter for each MIMO antenna which translates to higher implementation costs compared to non-MIMO systems.
- 40 MHz channels is another feature incorporated into 802.11n which doubles the channel width from 20 MHz in previous 802.11 PHYs to transmit data. This allows for a doubling of the PHY data rate over a single 20 MHz channel. It can be enabled in the 5 GHz mode, or within the 2.4 GHz if there is knowledge that it will not interfere with any other 802.11 or non-802.11 (such as Bluetooth) system using those same frequencies.
- The 802.11n modulation scheme is OFDM-MIMO with 64QAM at maximum data rate. For higher physical layer data rates, the number of OFDM sub-channels per 20 MHz bandwidth in 802.11n is increased from 48 (legacy) to 52. The maximum FEC coding ratio of 802.11n is also increased from 3/4 (legacy) to 5/6. These two modifications together bring the PHY data rate up from 54 Mbps (legacy) to 65 Mbps for a 20 MHz channel. With two-spatial stream MIMO, the data rate is doubled to 130 Mbps per 20 MHz bandwidth. Using 40 MHz channel bonding further increases the MIMO data rate to 270 Mbps because more OFDM sub-channels are available between the two 20 MHz channels. With short guard interval (SI), the maximum data rate for a two spatial stream MIMO system on a 40 MHz channel reaches 300 Mbps. To improve spatial diversity, the number of MIMO radio chains/antennas can be more than the number of spatial data streams. For example,
2x3 MIMO: two spatial data streams TX/RX, two TX radio chains/antennas, and three RX radio chains/antennas.
3x3 MIMO: two spatial data streams TX/RX, three TX radio chains/antennas, and three RX radio chains/antennas.
- The maximum TX power is typically defined per radio chain. For a 3x3 MIMO, if the maximum power per chain is 20 dBm, the total TX power from three radio chains is about 25 dBm.
- A technique called Maximum-Ratio-Combining (MRC) is used in the MIMO receiver to achieve better receiver sensitivity. MRC optimally combines the received signals from different spatial paths through the multiple receive antennas/chains. 3x receive MRC chains are employed in AP4600 Series Access Ports and such implementation reaches a nearly optimal balance between the MRC performance and the implementation cost.

Rate Limiting

Rate Limiting limits the maximum rate sent to or received from the wireless network per mobile unit. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on the Remote Authentication Dial In User Service (RADIUS) server using Extreme Networks vendor specific attributes. The controller extracts the rate limits from RADIUS server response. When such attributes are not present, the global settings on the controller are then applied.

Proxy-ARP

Proxy ARP is provided for MUs whose IP address is known. The WLAN generates an ARP reply on behalf of an MU (if the MU's IP address is known). The ARP reply contains the MAC address of the MU (not the MAC address of the controller). Thus, the MU does not awaken to send ARP replies (increasing MU battery life and conserving wireless bandwidth).

If an MU goes into PSP without transmitting at least one packet, its Proxy ARP will not work.

HotSpot / IP Redirect

A hotspot is a Web page users are forced to visit before they are granted access to the Internet. With the advent of Wi-Fi enabled client devices (such as laptops and PDAs) commercial hotspots are common and can be found at many airports, hotels and coffee shops. The hotspot re-directs the user's traffic on hotspot enabled WLANs to a web page that requires them to authenticate before granting access to the WLAN. The following is a typical sequence for hotspot access:

- 1 A visitor with a laptop requires hotspot access at a site.
- 2 A user ID/ Password and hotspot Extended Service Set ID (ESSID) is issued by the site receptionist or IT staff.
- 3 The user connects their laptop to this ESSID.
- 4 The laptop receives its IP configuration via DHCP.
- 5 The user opens a Web browser and connects to their home page.
- 6 The controller re-directs them to the hotspot Web page for authentication.
- 7 The user enters their User ID/ Password.
- 8 A RADIUS server authenticates the user.
- 9 Upon successful authentication, the user is directed to a Welcome Page that lists (among other things) an Acceptable Use Policy.
- 10 The user agrees to the usage terms and is granted access to the Internet. (or other network services).

To set up a hotspot, create a WLAN ESSID and select Hotspot authentication from the Authentication menu. This is simply another way to authenticate a WLAN user, as it would be impractical to authenticate visitors using 802.1x. For information on configuring a hotspot, see [“Configuring Hotspots” on page 144](#).

IDM (Identity Driven Management)

RADIUS authentication is performed for all protocols using a RADIUS-based authentication scheme (such as EAP). Identity driven management is provided using a RADIUS client. The following IDMs are supported:

- *User based SSID authentication*—Denies authentication to MUs if associated to a ESSID configured differently by their RADIUS server.
- *User based VLAN assignment*—Allows the controller to extract VLAN information from the RADIUS server.
- *User based QoS*—Enables QoS for the MU based on settings within the RADIUS Server.

Voice Prioritization

The controller has the capability of having its QoS policy configured to prioritize network traffic requirements for associated MUs. Use QoS to enable voice prioritization for devices using voice as its transmission priority.

Voice prioritization allows you to assign priority to voice traffic over data traffic, and (if necessary) assign legacy voice supported devices (non WMM supported voice devices) additional priority.

Currently voice support implies the following:

- *Spectralink voice prioritization*—Spectralink sends packets that allow the controller to identify these MUs as voice MUs. Thereafter, any UDP packet sent by these MUs is prioritized ahead of data.
- *Strict priority*—The prioritization is strict.
- *Multicast prioritization*—Multicast frames that match a configured multicast mask bypass the PSP queue. This feature permits intercom mode operation without delay (even in the presence of PSP MU's).

For more information on configuring voice prioritization for a target WLAN, see [“Configuring WMM” on page 176](#).

Self Healing

Self Healing is the ability to dynamically adjust the RF network by modifying transmit power and/or supported rates upon an AP failure.

In a typical RF network deployment, APs are configured for Transmit Power below their maximum level. This allows the Tx Power to be increased when there is a need to increase coverage when an AP fails.

When an AP fails, the Tx Power/Supported rates of APs neighboring the failed AP are adjusted. The Tx power is increased and/or Supported rates are decreased. When the failed AP becomes operational again, Neighbor AP's Tx Power/Supported rates are brought back to the levels before the self healing operation changed them.

The controller detects an AP failure when:

- AP stops sending heartbeats.
- AP beacons are no longer being sent. This is determined when other detector APs are no longer hearing beacons from a particular AP.

Configure 0 (Zero) or more APs to act as either:

- *Detector APs*—Detector APs scan all channels and send beacons to the controller which uses the information for self-healing.
- *Neighbor APs*—When an AP fails, neighbor APs assist in self healing.
- *Self Healing Actions*—When an AP fails, actions are taken on the neighbor APs to do self-healing.

Detector APs. Configure an AP in either—Data mode (the regular mode) or Detector mode.

In Detector mode, an AP scans all channels at a configurable rate and forwards received beacons to the controller. The controller uses the information to establish a *receive signal strength baseline* over a period of time and initiates self-healing procedures (if necessary).

Neighbor Configuration. Neighbor detect is a mechanism allowing an AP to detect its neighbors as well as their signal strength. This enables you to verify your installation and configure it for self-healing when an AP fails.

Self Healing Actions. If AP1 detects AP2 and AP3 as its neighbors, you can assign failure actions to AP2 and AP3 whenever AP1 fails.

Assign up to four self healing actions:

- 1 No action
- 2 Decrease supported rates
- 3 Increase Tx power
- 4 Both 2 and 3.

You can specify the Detector AP (AP2 or AP3) to stop detecting and adopt the RF settings of the failed AP. For more information on configuring self healing, see [“Configuring Self Healing” on page 366](#).

Wireless Capacity

Wireless capacity specifies the maximum numbers of MUs, Access Ports/Points and wireless networks usable by a controller. Wireless capacity is largely independent of performance. Aggregate controller performance is divided among the controller clients (MUs and Access Ports) to find the performance experienced by a given user. Each controller platform is targeted at specific market segments, so the capacity of each platform is chosen appropriately. Wireless controller capacity is measured by:

- The maximum number of WLANs per controller
- The maximum number of Access Ports/Points adopted per controller
- The maximum number of MUs per controller
- The maximum number of MUs per Access Port/Point.

The actual number of Access Ports/Points adoptable by a controller is defined by the controller licenses or the total licenses in the cluster in which this controller is a member.

AP and MU Load Balancing

Fine tune a network to evenly distribute data and/or processing across available resources. Refer to the following:

- [MU Balancing Across Multiple APs on page 27](#)
- [AP Balancing Across Multiple Controllers on page 28](#)

MU Balancing Across Multiple APs. Per the 802.11 standard, AP and MU association is a process conducted independently of the controller. 802.11 provides message elements used by the MU firmware to influence roaming decisions. The controller implements the following MU load balancing techniques:

- *802.11e admission control*—1 byte: channel utilization % and 1 byte: MU count is sent in QBSS Load Element in beacons to MU.
- *Extreme Networks load balancing element*—2 byte: MU Count are sent in beacon to MU.

For more information on Access Port adoption in a layer 3 environment, see [“Configuring Layer 3 Adoption” on page 256](#).

AP Balancing Across Multiple Controllers. At adoption, the AP solicits and receives multiple adoption responses from the controllers on the network. These adoption responses contain preference and loading information the AP uses to select the optimum controller to be adopted by. Use this mechanism to define which APs are adopted by which controllers. By default, the adoption algorithm generally distributes AP adoption evenly among the controllers available.

**NOTE**

Port adoption per controller is determined by the number of licenses acquired.

For more information on Access Port adoption in a layer 3 environment, see [“Configuring Layer 3 Adoption” on page 256](#).

Wireless Roaming

The following types of wireless roaming are supported by the controller:

- [Inter-controller Layer 2 Roaming on page 28](#)
- [Inter-controller Layer 3 Roaming on page 28](#)
- [Fast Roaming on page 28](#)
- [International Roaming on page 28](#)
- [Power Save Polling on page 28](#)

Inter-controller Layer 2 Roaming. An associated MU (connected to a controller) can roam to another Access Port/Point connected to a different controller. Both controllers must be on the same Layer 2 domain. Authentication information is not shared between the controllers, nor are buffered packets on one controller transferred to the other. Pre-authentication between the controller and MU allows faster roaming.

Inter-controller Layer 3 Roaming. Interswitch Layer 3 roaming allows MUs to roam between controllers which are not on the same LAN or IP subnet without the MUs or the rest of the network noticing. This allows controllers to be placed in different locations on the network without having to extend the MU VLANs to every controller.

Fast Roaming. Using 802.11i can speed up the roaming process from one AP to another. Instead of doing a complete 802.1x authentication each time an MU roams between APs, 802.11i allows an MU to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited APs, Opportunistic Key Caching allows multiple APs to share PMKs among themselves. This allows an MU to roam to an AP it has not previously visited and reuse a PMK from another AP to skip the 802.1x authentication.

International Roaming. The wireless controller supports international roaming per the 802.11d specification.

Power Save Polling. An MU uses *Power Save Polling* (PSP) to reduce power consumption. When an MU is in PSP mode, the controller buffers its packets and delivers them using the DTIM interval. The PSP-Poll packet polls the AP for buffered packets. The PSP null data frame is used by the MU to signal the current PSP state to the AP.

QoS

QoS provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic.

If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when the controller's bandwidth is shared by different users and applications.

QoS helps ensure each WLAN on the controller receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards MUs are classified into categories such as Management, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN.

The controller supports the following QoS mechanisms:

802.11e QoS. 802.11e enables real-time audio and video streams to be assigned a higher priority over data traffic. The controller supports the following 802.11e features:

- Basic WMM
- WMM Linked to 802.1p Priorities
- WMM Linked to DSCP Priorities
- Fully Configurable WMM
- Admission Control
- Unscheduled-APSD
- TSPEC Negotiation
- Block ACKQBSS Beacon Element

802.1p Support. 802.1p is a standard for providing QoS in 802-based networks. 802.1p uses three bits to allow controllers to re-order packets based on priority level.

Voice QoS. When controller resources are shared between a *Voice over IP* (VoIP) conversation and a file transfer, bandwidth is normally exploited by the file transfer, thus reducing the quality of the conversation or even causing it to disconnect. With QoS, a VoIP conversation (a real-time session), receives priority, maintaining a high level of voice quality. Voice QoS ensures:

- Strict Priority
- Spectralink Prioritization
- VOIP Prioritization (IP ToS Field)
- Multicast Prioritization

Data QoS. The controller supports the following data QoS techniques:

- Egress Prioritization by WLAN
- Egress Prioritization by ACL

DCSCP to AC Mapping. The controller provides arbitrary mapping between *Differentiated Services Code Point* (DCSCP) values and WMM Access Categories. This mapping can be set manually.

Wireless Layer 2 Switching. The controller supports the following layer 2 wireless switching techniques:

- WLAN to VLAN
- MU User to VLAN
- WLAN to GRE

Automatic Channel Selection. Automatic channel selection works sequentially as follows:

- 1 When a new AP is adopted, it scans each channel. However, the controller does not forward traffic at this time.
- 2 The controller then selects the least crowded channel based on the noise and traffic detected on each channel.
- 3 The algorithm used is a simplified maximum entropy algorithm for each radio, where the signal strength from adjoining APs/MUs associated to adjoining APs is minimized.
- 4 The algorithm ensures adjoining APs are as far away from each other as possible (in terms of channel assignment).



NOTE

Individual radios can be configured to perform automatic channel selection.

WMM-Unsupported APSD

This feature is also known as WMM Power Save or WMM-UPSD (*Unsupported Power Save Delivery*). WMM-UPSD defines an unsupported 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 UPSD power management, it requests (and the AP delivers) buffered frames associated with that flow during an unsupported service period. The controller initiates an unsupported 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 UPSD enabled. After the AP acknowledges the trigger frame, it transmits the frames in its UPSD power save buffer addressed to the triggering controller.

UPSD is well suited to support bi-directional frame exchanges between a voice STA and its AP.

Multiple VLANs per WLAN

The controller permits the mapping of a WLAN to more than one VLAN. When an MU associates with a WLAN, the MU is assigned a VLAN by means of load balance distribution. The VLAN is picked from a pool assigned to the WLAN. The controller tracks the number of MUs per VLAN, and assigns the least used/loaded VLAN to the MU. This number is tracked on a per-WLAN basis.

A broadcast key, unique to the VLAN, encrypts packets coming from the VLAN. If two or more MUs are on two different VLANs, they both hear the broadcast packet, but only one can decrypt it. The controller provides each MU a unique VLAN broadcast key as part of the WPA2 handshake or group key update message of a WPA handshake.

Limiting Users Per VLAN. Not all VLANs within a single WLAN must have the same DHCP pool size. Assign a user limit to each VLAN to allow the mapping of different pool sizes.

Specify the VLAN user limit. This specifies the maximum number of MUs associated with a VLAN (for a particular WLAN). When the maximum MU limit is reached, no more MUs can be assigned to that VLAN.

Packet Flows. There are four packet flows supported when the controller is configured to operate with multiple VLAN per WLAN:

- *Unicast From Mobile Unit*—Frames are decrypted, converted from 802.11 to 802.3 and switched to the wired side of the VLAN dynamically assigned to the mobile device. If the destination is another mobile device on the wireless side, the frame is encrypted and switched over the air.
- *Unicast To Mobile Unit*—The frame is checked to ensure the VLAN is same as that assigned to the mobile device. It is then converted to an 802.11 frame, encrypted, and sent over the air.
- *Multicast/Broadcast From Mobile Unit*—The frame is treated as a unicast frame from the MU, with the exception that it is encrypted with the per-VLAN broadcast key and then transmitted over the air.
- *Multicast/Broadcast from Wired Side*—If the frame comes from a VLAN mapped to the WLAN, it's encrypted using a per-VLAN broadcast key and transmitted over the air. Only MUs on that VLAN have a broadcast key that can decrypt this frame. Other MUs receive it, but discard it.

In general, when there are multiple VLANs mapped to the same WLAN, the broadcast buffer queue size scales linearly to accommodate a potential increase in the broadcast packet stream.

Roaming within the Controller. When an MU is assigned to a VLAN, the controller registers the VLAN assignment in its credential cache. If the MU roams, it is assigned back to its earlier assigned VLAN. The cache is flushed upon detected MU inactivity or if the MU associates over a different WLAN (on the same controller).

Roaming across a Cluster. MUs roam among controller cluster members. The controller must ensure a VLAN remains unchanged as an MU roams. This is accomplished by passing MU VLAN information across the cluster using the interface used by a hotspot. It automatically passes the username/password across the credential caches of the member controllers. This ensures a VLAN MU association is maintained even while the MU roams among cluster members.

Roaming across a Layer 3 Mobility Domain. When an MU roams among controllers in different Layer 3 mobility domains, Layer 3 ensures traffic is tunneled back to the correct VLAN (on the home controller).

Interaction with RADIUS Assigned VLANs. Multiple VLANs per WLAN can co-exist with VLANs assigned by a RADIUS server. Upon association, an MU is assigned to a VLAN from a pool of available VLANs. When the RADIUS server assigns the user another VLAN, MU traffic is forwarded to that VLAN.

When 802.1x is used, traffic from the MU is dropped until authentication is completed. None of the MU data is switched onto the temporarily VLAN. A RADIUS assigned VLAN overrides the statically assigned VLAN.

If the RADIUS assigned VLAN is among the VLANs assigned to a WLAN, it is available for VLAN assignment in the future. If the RADIUS assigned VLAN is not one of the VLANs assigned to a WLAN, it is not available for future VLAN assignment. To configure Multiple VLANs for a single WLAN, see [“Assigning Multiple VLANs per WLAN” on page 140.](#)

Wired Switching

The controller includes the following wired switching features:

- [DHCP Servers on page 32](#)
- [DHCP User Class Options on page 32](#)
- [DDNS on page 32](#)
- [VLAN Enhancements on page 33](#)
- [Interface Management on page 33](#)

DHCP Servers

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network to which they are attached. Each subnet may be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool.

When a DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. For information on defining the controller DHCP configuration, see ["DHCP Server Settings" on page 311](#).

DHCP User Class Options

A DHCP Server groups clients based on defined user-class option values. Clients with a defined set of user-class values are segregated by class. The DHCP Server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses.

DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined).

Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnet. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned. For more information, see ["Configuring the DHCP User Class" on page 328](#).

DDNS

Dynamic DNS (DDNS) keeps a domain name linked to a changing IP address. Typically, when a user connects to a network, the user's ISP assigns it an unused IP address from a pool of IP addresses. This address is only valid for a short period. Dynamically assigning IP addresses increases the pool of assignable IP addresses. DNS maintains a database to map a given name to an IP address used for communication on the Internet. The dynamic assignment of IP addresses makes it necessary to update the DNS database to reflect the current IP address for a given name. Dynamic DNS updates the DNS database to reflect the correct mapping of a given name to an IP address.

VLAN Enhancements

The controller has incorporated the following VLAN enhancements:

- Network interfaces operate in either trunk or access modes.
- A network interface in access mode can only send and receive untagged packets.
- A trunk port can now receive both tagged and untagged packets. Each Ethernet port is assigned a native VLAN.
- You can now configure a set of allowed VLANs on a trunk port. Packets received on this port that belong to other VLANs are discarded.

Interface Management

The controller's physical interfaces auto-negotiate speed and duplex. The controller also allows:

- Manual bandwidth configuration of a physical interface speed to 10/100/1000 Mbps.
- Manual duplex configuration of a physical interface to Full Duplex or Half Duplex.
- Manual configuration of administrative shutdown of a physical interface.

Management Features

The controller supports the following management features:

- A secure, browser-based management console.
- A *Command Line Interface* (CLI) accessible via the serial port or through Telnet or a *Secure Shell* (SSH) application.
- A CLI Service mode enabling the capture of system status information that can be sent to Extreme Networks personnel for use in problem resolution.
- The support for *Simple Network Management Protocol* (SNMP) version 3 as well as SNMP version 2.
- Upload and download of Access Port firmware and configuration files using TFTP and FTP.
- Transfer of firmware and configuration files using Compact Flash (Summit WM3700 only) or USB (Summit WM3400, Summit WM3600 and Summit WM3700)
- The graphing of wireless statistics.
- A GUI dashboard summary of system status.
- Multi controller management via MSP application.
- Heat map support for RF deployment.
- Secure guest access with specific permission intervals.
- Controller discovery enabling users to discover each Extreme Networks controller on the specified network.

Security Features

Controller security can be classified into wireless security and wired security.

The controller includes the following wireless security features:

- [Encryption and Authentication on page 34](#)
- [MU Authentication on page 35](#)

- [Secure Beacon on page 35](#)
- [MU to MU Disallow on page 35](#)
- [802.1x Authentication on page 36](#)
- [WIPS on page 36](#)
- [Rogue AP Detection on page 37](#)

The controller includes the following wired security features:

- [ACLs on page 38](#)
- [Local RADIUS Server on page 38](#)
- [IPSec VPN on page 38](#)
- [NAT on page 39](#)
- [Certificate Management on page 39](#)

Encryption and Authentication

The controller can implement the following encryption and authentication types:

- [WEP on page 34](#)
- [WPA on page 34](#)
- [WPA2 on page 34](#)
- [Keyguard-WEP on page 34](#)

WEP. *Wired Equivalent Privacy* (WEP) is an encryption scheme used to secure wireless networks. WEP was intended to provide comparable confidentiality to a traditional wired network, hence the name. WEP had many serious weaknesses and hence was superseded by *Wi-Fi Protected Access* (WPA). Regardless, WEP still provides a level of security that can deter casual snooping. For more information on configuring WEP for a target WLAN, see [“Configuring WEP 64” on page 163](#) or [“Configuring WEP 128 / KeyGuard” on page 165](#).

WEP uses passwords entered manually at both ends (Pre Shared Keys). Using the RC4 encryption algorithm, WEP originally specified a 40-bit key, but was later boosted to 104 bits. Combined with a 24-bit initialization vector, WEP is often touted as having a 128-bit key.

WPA. WPA is designed for use with an 802.1X authentication server, which distributes different keys to each user. However, it can also be used in a less secure *pre-shared key* (PSK) mode, where every user is given the same passphrase.

WPA uses *Temporal Key Integrity Protocol* (TKIP), which dynamically changes keys as the system is used. When combined with the much larger Initialization Vector, it defeats well-known key recovery attacks on WEP. For information on configuring WPA for a WLAN, see [“Configuring WPA/WPA2 using TKIP and CCMP” on page 166](#).

WPA2. WPA2 uses a sophisticated key hierarchy that generates new encryption keys each time an MU associates with an Access Point. Protocols including 802.1X, EAP and RADIUS are used for strong authentication. WPA2 also supports the TKIP and AES-CCMP encryption protocols. For information on configuring WPA for a WLAN, see [“Configuring WPA/WPA2 using TKIP and CCMP” on page 166](#).

Keyguard-WEP. KeyGuard is a proprietary dynamic WEP solution. Basically, KeyGuard is TKIP without the message integrity check. For information on configuring KeyGuard for a WLAN, see [“Configuring WEP 128 / KeyGuard” on page 165](#).

MU Authentication

The controller uses the following authentication schemes for MU association:

- [Kerberos on page 35](#)
- [802.1x EAP on page 35](#)
- [MAC ACL on page 35](#)

Refer to [“Editing the WLAN Configuration” on page 134](#) for additional information.

Kerberos. Kerberos allows for mutual authentication and end-to-end encryption. All traffic is encrypted and security keys are generated on a per-client basis. Keys are never shared or reused, and are automatically distributed in a secure manner. For information on configuring Kerberos for a WLAN, see [“Configuring Kerberos” on page 143](#).

802.1x EAP. 802.1x EAP is the most secure authentication mechanism for wireless networks and includes EAP-TLS, EAP-TTLS and PEAP. The controller is a proxy for RADIUS packets. An MU does a full 802.11 authentication and association and begins transferring data frames. The controller realizes the MU needs to authenticate with a RADIUS server and denies any traffic not RADIUS related. Once RADIUS completes its authentication process, the MU is allowed to send other data traffic. You can use either an onboard RADIUS server or internal RADIUS Server for authentication. For information on configuring 802.1x EAP for a WLAN, see [“Configuring 802.1x EAP” on page 142](#).

MAC ACL. The MAC ACL feature is basically a dynamic MAC ACL where MUs are allowed/denied access to the network based on their configuration on the RADIUS server. The controller allows 802.11 authentication and association, then checks with the RADIUS server to see if the MAC address is allowed on the network. The RADIUS packet uses the MAC address of the MU as both the username and password (this configuration is also expected on the RADIUS server). MAC-Auth supports all encryption types, and (in case of 802.11i) the handshake is completed before the RADIUS lookup begins. For information on configuring MAC ACL, see [“Configuring MAC Authentication” on page 154](#).

Secure Beacon

Devices in a wireless network use *Service Set Identifiers* (SSIDs) to communicate. An SSID is a text string up to 32 bytes long. An AP in the network announces its status by using beacons. To avoid others from accessing the network, the most basic security measure adopted is to change the default SSID to one not easily recognizable, and disable the broadcast of the SSID.

The SSID is a code attached to all packets on a wireless network to identify each packet as part of that network. All wireless devices attempting to communicate with each other must share the same SSID. Apart from identifying each packet, the SSID also serves to uniquely identify a group of wireless network devices used in a given service set.

MU to MU Disallow

Use MU to MU Disallow to restrict MU to MU communication within a WLAN. The default is ‘no’, which allows MUs to exchange packets with other MUs. It does not prevent MUs on other WLANs from sending packets to this WLAN. You would have to enable MU to MU Disallow on the other WLAN. To define how MU to MU traffic is permitted for a WLAN, see [“Editing the WLAN Configuration” on page 134](#).

802.1x Authentication

802.1x Authentication cannot be disabled (it is always enabled). A factory delivered out-of-the-box AP4600 series device supports 802.1x authentication using a default username (admin) and password (extreme). EAP-MD5 is used for 802.1x.

When you initially switch packets on an out-of-the-box AP4600 series device, it immediately attempts to authenticate using 802.1x. Since 802.1x supports *supplicant initiated* authentication, the AP4600 series device attempts to initiate the authentication process.

On reset (all resets including power-up), the AP4600 series device sends an EAPOL start message every time it sends a Hello message (periodically every 1 second). The *EAPOL start* is the *supplicant initiated* attempt to become authenticated.

If an appropriate response is received in response to the *EAPOL start* message, the AP4600 series device attempts to proceed with the authentication process to completion. Upon successful authentication, the AP4600 series device transmits the Hello message and the download proceeds the way as it does today.

If no response is received from the *EAPOL start* message, or if the authentication attempt is not successful, the AP4600 series device continues to transmit *Hello* messages followed by *LoadMe* messages. If a parent reply is received in response to the *Hello message*, then downloading continue normally—without authentication. In this case, you need not enable or disable the port authentication.

802.1x authentication is conducted:

- At power up
- On an AP4600 series device operator initiated reset (such as pulling Ethernet cable)
- When the controller administrator initiates a reset of the AP4600 series device.
- When re-authentication is initiated by the Authenticator.

Change Username/Password after AP Adoption. Once the AP4600 series device is adopted using 802.1x authentication (such as default username/password) OR using a non-secure access method (hub or controller without 802.1x enabled), use the CLI/SNMP/UI to reconfigure the username/password combination.

Reset Username/Password to Factory Defaults. To restore the AP4600 series device username/password to factory defaults, adopt the AP4600 series device using a non-secure access method (a hub or controller without 802.1x enabled), then reconfigure the username/password combination.

The Access Port does not make use of any parameters (such as MAC based authentication, VLAN based etc.) configured on a RADIUS Server.

WIPS

Extreme Networks WLAN infrastructure solutions can work with Motorola Wireless Intrusion Protection Software (WIPS) to make the wireless network securer. The WIPS monitors for any presence of unauthorized rogue Access Points. Unauthorized attempts to access the WLAN is generally accompanied by anomalous behavior as intruding MUs try to find network vulnerabilities. Basic forms of this behavior can be monitored and reported without needing a dedicated WIPS. When the parameters exceed a configurable threshold, the controller generates an SNMP trap and reports the result via the management interfaces. Basic WIPS functionality does not require monitoring APs and does not perform off-channel scanning.

**NOTE**

When using an AP35xx or AP4700 Series device for use with WIPS and as a sensor you must first configure the WIPS server IP Addresses before converting the AP35xx or AP4700 to a sensor.

Rogue AP Detection

The controller supports the following techniques for rogue AP detection:

- [RF scan by Access Port on all channels on page 37](#)
- [SNMP Trap on discovery on page 38](#)
- [Authorized AP Lists on page 38](#)
- [Rogue AP Report on page 38](#)
- [Extreme Networks WMS Support on page 38](#)

**NOTE**

The Extreme Networks Wireless Management Suite (WMS) is recommended to plan the deployment of the controller. Extreme Networks WMS can help optimize the positioning and configuration of a controller in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Extreme Networks documentation website at: <http://www.extremenetworks.com/go/documentation>.

RF scan by Access Port on one channel. This process requires an Access Port to assist in Rogue AP detection. It functions as follows:

- The controller sends a new configuration message to the adopted AP informing it to detect Rogue APs.
- The Access Port listens for beacons on its present channel.
- It passes the beacons to the controller as it receives them without any modification.
- The controller processes these beacon messages to generate the list of APs.

This process of detecting a Rogue AP is non-disruptive and none of the MUs are disassociated during this process. The Access Port will only scan on its present channel. An AP4600 series device provides this support.

By choosing this option for detection, all capable Access Ports will be polled for getting the information.

RF scan by Access Port on all channels. The process used to scan for Rogue APs on all available channels functions as follows:

- The controller sends a configuration message (with the ACS bit set and channel dwell time) to the Access Port.
- An Access Port starts scanning each channel and passes the beacons it hears on each channel to the controller.
- An Access Port resets itself after scanning all channels.
- A controller then processes this information.

SNMP Trap on discovery. An SNMP trap is sent for each detected and Rogue AP. Rogue APs are only detected, and notification is provided via a SNMP trap.

**NOTE**

Wired side scanning for Rogue APs using WNMP is not supported. Similarly, RADIUS lookup for approved AP is not provided.

Authorized AP Lists. Configure a list of authorized Access Ports based on their MAC addresses. The controller evaluates the APs against the configured authorized list after obtaining Rogue AP information from one of the 2 mechanisms as mentioned in [“Rogue AP Detection” on page 37](#).

Rogue AP Report. After determining which are authorized APs and which are Rogue, the controller prepares a report.

Extreme Networks WMS Support. The controller can provide rogue device detection data to the Extreme Networks Wireless Management Suite application (or Extreme Networks WMS). Extreme Networks WMS uses this data to refine the position and display the rogue on a site map representative of the physical dimensions of the actual radio coverage area of the controller. This is of great assistance in the quick identification and removal of unauthorized devices.

ACLs

ACLs control access to the network through a set of rules. Each rule specifies an action taken when a packet matches a set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. If the action is to mark, the packet is tagged for priority. The controller supports the following types of ACLs:

- IP Standard ACLs
- IP Extended ACLs
- MAC Extended ACLs
- Wireless LAN ACLs

For information on creating an ACL, see [“Configuring Firewalls and Access Control Lists” on page 403](#).

Local RADIUS Server

RADIUS is a common authentication protocol utilized by the 802.1x wireless security standard. RADIUS improves the WEP encryption key standard, in conjunction with other security methods such as EAP-PEAP. The controller has one onboard RADIUS server. For information on configuring the controller’s resident RADIUS Server, see [“Configuring the RADIUS Server” on page 489](#).

IPSec VPN

IP Sec is a security protocol providing authentication and encryption over the Internet. Unlike SSL (which provides services at layer 4 and secures two applications), IPsec works at Layer 3 and secures the network. Also unlike SSL (which is typically built into the Web browser), IPsec requires a client installation. IPsec can access both Web and non-Web applications, whereas SSL requires workarounds for non-Web access such as file sharing and backup.

A VPN is used to provide secure access between two subnets separated by an unsecured network. There are two types of VPNs:

- *Site-Site VPN*—For example, a company branching office traffic to another branch office traffic with an unsecured link between the two locations.
- *Remote VPN*—Provides remote user ability to access company resources from outside the company premises.

The controller supports:

- IPsec termination for site to site
- IPsec termination for remote access
- IPsec traversal of firewall filtering
- IPsec traversal of NAT
- IPsec/L2TP (client to controller)

NAT

Network Address Translation (NAT) is supported for packets routed by the controller. The following types of NAT are supported:

- *Port NAT*—Port NAT (also known as NAPT) entails multiple local addresses are mapped to single global address and a dynamic port number. The user is not required to configure any NAT IP address. Instead IP address of the public interface of the controller is used to NAT packets going out from private network and vice versa for packets entering private network.
- *Static NAT*—Static NAT is similar to Port NAT with the only difference being that it allows the user to configure a source NAT IP address and/or destination NAT IP address to which all the packets will be NATted to. The source NAT IP address is used when hosts on a private network are trying to access a host on a public network. A destination NAT IP address can be used for public hosts to talk to a host on a private network.

Certificate Management

Certificate Management is used to provide a standardized procedure to:

- Generate a Server certificate request and upload the server certificate signed by certificate authority (CA).
- Uploading of CA's root certificate
- Creating a self-signed certificate

Certificate management will be used by the applications HTTPS, VPN, HOTSPOT and RADIUS. For information on configuring controller certificate management, see [“Creating Server Certificates” on page 509](#).

NAC

Using *Network Access Control* (NAC), the controller hardware and software grants access to specific network resources. NAC performs a user and MU authorization check for resources that do not have a NAC agent. NAC verifies an MU's compliance with the controller's security policy. The controller supports only the EAP/802.1x type of NAC. However, the controller also provides a mean to bypass NAC authentication for MU's that do not have NAC 802.1x support (printers, phones, PDAs etc.). For information on configuring NAC support, see [“Configuring NAC Server Support” on page 160](#).

Supported Access Ports/Points

An Extreme Networks wireless LAN controller supports the adoption of the following Extreme Networks Enterprise Access Ports and Access Points:

- Altitude AP4600 Series Access Port
- Altitude AP3510 Access Point
- Altitude AP3550 Access Point
- Altitude AP4710 Access Point
- Altitude AP4750 Access Point

Access Port and Access Point Features

Features are normally AP dependent. The following table shows the features supported by Altitude AP35x0 and AP4700 Series Access Points and Altitude AP4600 Series Access Ports.

Table 1: Access Port and Access Point Features

Features	AP4600 Series	AP35x0 Access Points
802.11k	Y	N
802.11W	Y	N
ACS	Y	Y
Adaptive .11n	NA	N
Adaptive AP Mesh	NA	Y
Adaptive AP Rogue AP Detection	NA	Y
Adaptive AP WLAN Stats	NA	Y
Adaptive AP (Wireless Parameter Configuration, AP and MU stats)	NA	Y
Aeroscout Support	Y	Y
AP Load - Balancing	Y	Y
Centralized login pages for Hotspot	Y	Y on Extended WLAN
Data QoS	Y	Y
DDNS	Y	Y
DHCP Redundancy with Cluster Operation	Y	Y
DHCP relay	Y	Y
DHCP User Class options	Y	Y
DoS attack Protection Enhancements	Y	Y on Extended WLAN
Dynamic Load Balancing of APs (Auto Revert in a cluster)	Y	Y
Dynamic VLAN Assignment	Y	Y
Ekahau Support	Y	Y
Encryption (Keyguard, Kerberos - external KDC, WPA, WPA2, WEP)	Y	Y
Enhanced Beacon	Y	N
Enhanced Probe	Y	N
Fast Roaming (Key Caching)	Y	Y

Table 1: Access Port and Access Point Features (Continued)

Features	AP4600 Series	AP35x0 Access Points
Firewall	Y - On the controller	Y - Native to the AP for the Independent WLAN, on the controller for the Extended WLAN
Firmware upgrade for Adaptive AP	NA	Y
TCP data path flow across a cluster (based on ACL rules and filters)	Y	Y on Extended WLAN
Geofencing	N	N
Hotspot	Y	Y - Controller hotspot on Extended WLAN, AP hotspot on Independent WLAN
IGMP Snooping	Y	Y on Extended WLAN
Integrated Wireless IDS/IPS	Y	Y on Extended WLAN (see note following this table)
IP Filtering on Adaptive AP (Independent WLAN)	NA	Y
IP Sec VPN	Y - On the controller	Y
IPS Sensor Config	N	Y
IPv6 passthrough	Y	Y
L2 Adoption	Y	N
L3 Adoption	Y	Y
L3 Mobility	Y	Y on Extended WLAN
Location-based hotspot	Y	N
Location LED (Flashing LED)	Y	Y
MAC based MU authentication	Y	N
MU Load balancing across Controller/Cluster	Y	N
Multiple VLANs (in WLAN)	Y	N
Mu-Mu Disallow	Y	Y on Extended WLAN
NAC Support	Y	N
NAT	Y - On the controller	Y
Per AP country code setting	Y	Y
Per MU rate Limiting	Y	Y on Extended WLAN
Qos 802.1p/DCSP mapping	Y	Y
QoS ToS	Y	Y
RADIUS(.1x, MAC authorization, dynamic authorization, client accounting)	Y	Y
Rate Limit per WLAN	Y	Y on Extended WLAN
Summit WM3400 controller support	Y	Y
Rogue AP Containment	Y	N
Rogue AP locationing	Y	Y
Role Based Firewall	Y	Y on Extended WLAN
RSSI based locationing	Y	Y
RTLS	Y	Y
Secure beacon	Y	Y

Table 1: Access Port and Access Point Features (Continued)

Features	AP4600 Series	AP35x0 Access Points
Secure WiSPe	Y	NA
Self healing	Y	N
SIP CAC	Y	N
SMART RF	Y	N
Static IP for APs	Y	Y
TSPEC Admission Control	Y	N
Uni Band 3 Support	N in -US SKUs due to regulatory constraints	N in -US SKUs due to regulatory constraints
VLAN Pooling/Multiple VLANs for WLANs	Y	N
WIPS Enhancements	Y	N
WIPS Sensor	N	Y
Wireless Firewall	Y	Y on Extended WLAN
Wireless Proxy ARP	Y	Y
WLAN Bandwidth Management	Y	Y, excluding the Round Robin Option available native on the AP
WMM U-APSD	Y	Y

**NOTE**

The following integrated wireless IDS/IPS anomalies are supported by Altitude AP35x0 Access Points: Fake-ap-flood, ap-default-configuration, ap-ssid-broadcast-in-beacon, suspicious-ap-high-rssi and unauthorized-ap-using-authorized-ssid.

IEEE Standards Support

Table 2: IEEE Standards Support

IEEE Standard	Supported	Notes
IEEE 802.11a	Yes	<p>The IEEE 802.11a standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> Summit WM3400 Summit WM3600 Summit WM3700 <p>The IEEE 802.11a standard is fully supported on the following AP Platforms:</p> <ul style="list-style-type: none"> Altitude™ 4710 Access Point Altitude 4750 Access Point Altitude 3510 Access Point Altitude 3550 Access Point Altitude 4600 Series Access Ports

Table 2: IEEE Standards Support (Continued)

IEEE Standard	Supported	Notes
IEEE 802.11g	Yes	<p>The IEEE 802.11g standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700 <p>The IEEE 802.11g standard is fully supported on the following AP Platforms:</p> <ul style="list-style-type: none"> • Altitude 4710 Access Point • Altitude 4750 Access Point • Altitude 3510 Access Point • Altitude 3550 Access Point • Altitude 4600 Series Access Ports
IEEE 802.11d	Yes	<p>The IEEE 802.11d standard is implemented as part of the IEEE 802.11s standard on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700 <p>The IEEE 802.11d standard is implemented for Mesh networking on the following AP Platforms:</p> <ul style="list-style-type: none"> • Altitude 4710 Access Point • Altitude 4750 Access Point • Altitude 3510 Access Point • Altitude 3550 Access Point • Altitude 4600 Series Access Ports
IEEE 802.11i	Yes	<p>We fully support the 802.11i standard for encryption and authentication. Additionally we also implement 802.11i PMK Caching, Opportunistic PMK Caching and Pre-Authentication.</p> <p>The IEEE 802.11i standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700 <p>The IEEE 802.11i standard is fully supported on the following AP Platforms:</p> <ul style="list-style-type: none"> • Altitude 4710 Access Point • Altitude 4750 Access Point • Altitude 3510 Access Point • Altitude 3550 Access Point • Altitude 4600 Series Access Ports
IEEE 802.11n	Yes	<p>The IEEE 802.11n standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700

Table 2: IEEE Standards Support (Continued)

IEEE Standard	Supported	Notes
IEEE 802.1x	Yes	<p>Full support IEEE 802.1x authentication ether with a fully functional integrated RADIUS server built into our WM Controllers and Access Points or an external RADIUS server such as Microsoft IAS, Microsoft NPS, Cisco Secure ACS, Free RADIUS and Juniper Steel Belted RADIUS (to name a few).</p> <p>When using the integrated RADIUS server we support the following EAP methods:</p> <ul style="list-style-type: none"> • EAP-TLS • EAP-GTC (PEAPv1) • EAP-MSCHAPv2 (PEAPv0) • EAP-TTLS (MD5, PAP, MSCHAPv2) <p>When using an external RADIUS server the EAP type is transparent to the WLAN infrastructure allowing any standard EAP method to be supported.</p> <p>The IEEE 802.1x standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700 <p>The IEEE 802.1x standard is fully supported on the following AP Platforms:</p> <ul style="list-style-type: none"> • Altitude 4710 Access Point • Altitude 4750 Access Point • Altitude 3510 Access Point • Altitude 3550 Access Point • Altitude 4600 Series Access Ports
IEEE 802.3u	Yes	<p>The IEEE 802.3u (100BASE-T) standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700 <p>The IEEE 802.3u (100BASE-T) standard is fully supported on the following AP Platforms:</p> <ul style="list-style-type: none"> • Altitude 4710 Access Point • Altitude 4750 Access Point • Altitude 3510 Access Point • Altitude 3550 Access Point • Altitude 4600 Series Access Ports
IEEE 802.3ab	Yes	<p>The IEEE 802.3ab (1000BASE-T) standard is fully supported on the following Controller Platforms:</p> <ul style="list-style-type: none"> • Summit WM3400 • Summit WM3600 • Summit WM3700

Table 2: IEEE Standards Support (Continued)

IEEE Standard	Supported	Notes
IEEE 802.3z	Yes	The IEEE 802.3z (1000BASE-X) standard is fully supported on the following Controller Platforms: <ul style="list-style-type: none">• Summit WM3600 (SFP Pluggable Optics)• Summit WM3700 (SFP Pluggable Optics)
IEEE 802.1P	Yes	The IEEE 802.1P (QoS) standard is fully supported on the following Controller Platforms: <ul style="list-style-type: none">• Summit WM3400• Summit WM3600• Summit WM3700 The IEEE 802.1P (QoS) standard is fully supported on the following AP Platforms: <ul style="list-style-type: none">• Altitude 4710 Access Point• Altitude 4750 Access Point• Altitude 3510 Access Point• Altitude 3550 Access Point• Altitude 4600 Series Access Ports
IEEE 802.1Q	Yes	The IEEE 802.1Q (VLAN Tagging) standard is fully supported on the following Controller Platforms: <ul style="list-style-type: none">• Summit WM3400• Summit WM3600• Summit WM3700 The IEEE 802.1Q (VLAN Tagging) standard is fully supported on the following AP Platforms: <ul style="list-style-type: none">• Altitude 4710 Access Point• Altitude 4750 Access Point• Altitude 3510 Access Point• Altitude 3550 Access Point

Standards Support

Table 3: Standards Support

Standard	Supported	Notes
RFC 768 UDP	Yes	The controller supports IP, UDP, TCP for various management and control functions and Controller -> AP communications.
RFC 791 IP	Yes	In addition, full IP4 routing support on the controller as well as support IPv4 on wired / wireless stateful inspection firewall is provided.
RFC 792 ICMP	Yes	
RFC 793 TCP	Yes	
RFC 826 ARP	Yes	
RFC 1122 Requirements for Internet Hosts	Yes	
RFC 1519 CIDR	Yes	
RFC 1542 BOOTP	Yes	BOOTP is implemented as part of the Integrated DHCP server. BOOTP clients are implemented on the Altitude 3510 and Altitude 3550.
RFC 2131 DHCP	Yes	DHCP client and server.
RFC 1321 MD5 Message-Digest Algorithm	Yes	Implemented for IPsec VPN, SNMPv3 and EAP-TTLS.
RFC 1851 The ESP Triple DES Transform	Yes	
RFC 2104 HMAC: Keyed Hashing for Message Authentication	Yes	
RFC 2246 TLS Protocol Version 1.0	Yes	
RFC 2401 Security Architecture for the Internet Protocol	Yes	
RFC 2403 HMAC-MD5-96 within ESP and AH	Yes	
RFC 2404 HMAC-SHA-1-96 within ESP and AH	Yes	
RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV	Yes	
RFC 2406 IPsec	Yes	
RFC 2407 Interpretation for ISAKMP	Yes	
RFC 2408 ISAKMP	Yes	
RFC 2409 IKE	Yes	
RFC 2451 ESP CBC-Mode Cipher Algorithms	Yes	
RFC 2459 Internet X.509 PKI Certificate and CRL Profile	Yes	
RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec	Yes	
SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit	Yes	
IPsec: DES-CBC, 3DES, AES-CBC	Yes	

Table 3: Standards Support (Continued)

Standard	Supported	Notes
RFC 2548 Microsoft Vendor-Specific RADIUS Attributes	Yes	
RFC 2716 PPP EAP-TLS	Yes	
RFC 2865 RADIUS Authentication	Yes	Integrated and Pass-through
RFC 2866 RADIUS Accounting	Yes	Integrated and Pass-through
RFC 2867 RADIUS Tunnel Accounting	Yes	
RFC 2869 RADIUS Extensions	Yes	
RFC 3576 Dynamic Authorization Extensions to RADIUS	Yes	
RFC 3579 RADIUS Support for EAP	Yes	
RFC 3580 IEEE 802.1X RADIUS Guidelines	Yes	
RFC 3748 Extensible Authentication Protocol	Yes	
Web-based authentication	Yes	Using internal and external hosting.
SNMP v1, v2c, v3	Yes	
RFC 854 Telnet	Yes	Client and Server.
RFC 1155 Management Information for TCP/IP-Based Internets	Yes	
RFC 1156 MIB	Yes	
RFC 1157 SNMP	Yes	
RFC 1213 SNMP MIB II	Yes	
RFC 1350 TFTP	Yes	Client only.
RFC 1643 Ethernet MIB	Yes	This RFC is obsolete http://tools.ietf.org/html/rfc3638 .
RFC 2030 SNMP	Yes	Client and Server.
RFC 2616 HTTP	Yes	
RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions	Yes	We support everything except the pBridge MIB.
RFC 2819 RMON MIB	Yes	
RFC 2863 Interfaces Group MIB	Yes	ifTable is supported, but ifMIB (mib-2 dot 31) which are later extensions of ifTable (mib-2 dot 2 dot 2) are not supported.
RFC 3164 Syslog	Yes	
RFC 3414 User-Based Security Model (USM) for SNMPv3	Yes	
RFC 3418 MIB for SNMP	Yes	
Web-based: HTTP/HTTPS	Yes	
Command-line interface: Telnet, SSH, serial port	Yes	

3

CHAPTER

Controller Web UI Access and Image Upgrades

The content of this chapter is segregated among the following:

- [Accessing the Controller Web UI on page 49](#)
- [Upgrading the Controller Image on page 51](#)
- [Auto Installation on page 51](#)

Accessing the Controller Web UI

Web UI Requirements

The controller Web UI is accessed using Internet Explorer version 5.5 (or later) and SUN JRE (Java Runtime Environment) 1.5 (or later). Refer to the Sun Microsystems website for information on downloading JRE.



NOTE

To successfully access the controller Web UI through a firewall, UDP port 161 must be open in order for the controller's SNMP backend to function.

To prepare Internet Explorer to run the Web UI:

- 1 Open IE's *Tools* > *Internet Options* panel and select the *Advanced* tab.
- 2 Uncheck the following checkboxes:
 - Use HTTP 1.1
 - Java console enabled (requires restart)
 - Java logging enabled
 - JIT compiler for virtual enabled (requires restart).

Connecting to the Controller Web UI

To display the Web UI, launch a Web browser on a computer with the capability of accessing the controller.



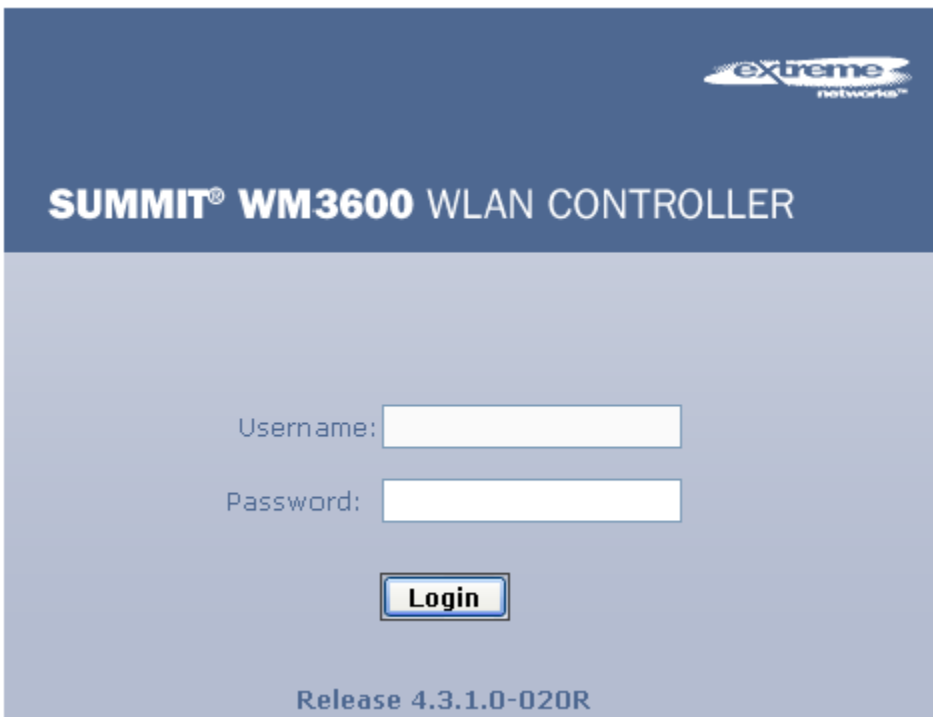
NOTE

Ensure you have HTTP connectivity to the controller, as HTTP is a required to launch the controller Web UI from a browser.

To display the controller Web UI:

- 1 Point the browser to the IP address assigned to the wired Ethernet port (port 2). Specify a secure connection using the `https://` protocol.

The controller login screen displays:



- 2 Enter the Username *admin*, and Password *admin123*. Both are case-sensitive. Click the *Login* button.



NOTE

If using HTTP to log in into the controller, you may encounter a Warning screen if a self-signed certificate has not been created and implemented for the controller. This warning screen will continue to display on future login attempts until a self-signed certificate is implemented. Extreme Networks recommends only using the default certificate for the first few login attempts until a self-signed certificate can be generated.



NOTE

If your password is lost, there is a means to access the controller, but you are forced to revert the controller back to its factory default settings and lose your existing configuration (unless saved to a secure location). Consequently, Extreme Networks recommends keeping the password in a secure location.

Once the Web UI is accessed, the Controller main menu item displays a configuration tab with high-level controller information. Click the *Show Dashboard* button to display an overall indicator of

controller health. Once the controller is fully configured, the dashboard is the central display for the user to view the version of firmware running on the controller, quickly assess the last 5 alarms generated by the controller, view the status of the controller's Ethernet connections and view controller CPU and memory utilization statistics.



NOTE

The chapters within this System Reference Guide are arranged to be complementary with the main menu items in the menu tree of the controller Web UI. Refer to this content to configure controller network addressing, security and diagnostics as required.

Upgrading the Controller Image

The controller ships with a factory installed firmware image with the full feature functionality described in this *System Reference Guide*. However, Extreme Networks periodically releases controller firmware that includes enhancements or resolutions to known issues. Verify your current controller firmware version with the latest version available from the Extreme Networks website before determining if your system requires an upgrade.

Auto Installation

The controller auto install function can be configured manually or using a DHCP server. When configuring auto installation using DHCP, the server requires the definition of a vendor class and four sub-options under option 43 namely:

- Option 186—defines the tftp/ftp server and ftp username, password information
- Option 187—defines the firmware path and file name
- Option 188—defines the config path and file name
- Option 190—defines the cluster config path and file name.

The individual features (config, cluster-config and image) can be enabled separately using the CLI, SNMP or Web UI. If a feature is disabled, it is skipped when auto install is triggered.

For manual configuration (where the URLs for the configuration and image files are not supplied by DHCP), the URLs can be specified using the CLI, SNMP or Applet. Use the CLI to define the expected firmware image version. If the image version is not specified, the controller will derive it from the header of the firmware image file.

Configuration files are tracked by their MD5 checksum and contents. If a file is renamed its contents remain the same and the file will not be reloaded.

The requested image file version (if any) is checked against the current version before any attempt is made to load it. If the requested version is the same as the running version, no action is taken. If the image file version (embedded in the file header) does not match the expected version, no further action is taken. If the version has not been specified, the image file header is compared to the local version. If they are the same, no action is taken.

**NOTE**

Once the system has been operating for ten minutes, Auto Install is disabled, though it may still be reconfigured. This is to prevent the system from attempting to re-install each time a DHCP lease is renewed.

Configuring Auto Install via the CLI. There are three compulsory and four optional configuration parameters.

The compulsory parameters are:

- configuration upgrade enable
- cluster configuration upgrade enable
- image upgrade enable

Optional (only for the static case):

- configuration file URL
- cluster configuration file URL
- image file URL
- expected image version

To set default to no, and the URLs and the version default to "" (blank):

```
WMController(config)#show autoinstall
feature      enabled      URL
config      no           --not-set--
cluster cfg  no           --not-set--
image       no           --not-set--
expected image version  --not-set--
```

Enables are set using the *autoinstall <feature>* command:

```
WMController>en
WMController#conf t
WMController(config)#autoinstall image
WMController(config)#autoinstall config
WMController(config)#autoinstall cluster-config
```

After this configuration update, any controller reboot with DHCP enabled on the RON port will trigger an auto install, provided the DHCP Server is configured with appropriate options.

The “enables” are cleared using the *no autoinstall <feature>*

URLs and the version string are stored in the configuration file as text and can be cleared using an empty pair of double quotes to denote the blank string. In the following example, define the three URLs and the expected version of the image file, then enable all three features for the auto install.

```
WMController(config)#autoinstall config url ftp://ftp:ftp@192.9.200.1/WMController/
config
WMController(config)#autoinstall cluster-config url ftp://ftp:ftp@192.9.200.1/
WMController/cluster-config
WMController(config)#autoinstall image url ftp://ftp:ftp@147.11.1.11/WMController/
images/WM3600.img
WMController(config)#autoinstall image version 3.1.0.0-XXXXX
WMController(config)#autoinstall config
```

```
WMController(config)#autoinstall cluster-config
WMController(config)#autoinstall image
WMController(config)#show autoinstall
feature      enabled      URL
config       yes          ftp://ftp:ftp@192.9.200.1/WMController/config
cluster cfg  yes          ftp://ftp:ftp@192.9.200.1/WMController/cluster-config
image        yes          ftp://ftp:ftp@147.11.1.11/WMController/images/WM3600.img
expected image version 4.3.1.0-XXXXX
```

Once again, for DHCP option based auto install the URLs is ignored and those passed by DHCP are not stored.

Whenever a string is blank it is shown as *--not-set--*.

4

CHAPTER

Controller Information

This chapter describes the controller main menu information used to configure the controller. This chapter consists of the following sections:

- [Viewing the Controller Interface on page 55](#)
- [Viewing Controller Port Information on page 68](#)
- [Viewing Controller Configurations on page 81](#)
- [Viewing Controller Firmware Information on page 86](#)
- [Controller File Management on page 91](#)
- [Configuring Automatic Updates on page 98](#)
- [Viewing the Controller Alarm Log on page 100](#)
- [Viewing Controller Licenses on page 102](#)
- [How to use the Filter Option on page 104](#)

Viewing the Controller Interface

The controller *Configuration* tab provides high-level system, controller name and address information accessible from one location. Use this information to assess whether the current firmware version is the most recent and if the number of licenses available is correct to support the number of radio devices deployed. The values displayed within the screen can be defined in numerous additional locations throughout the controller applet.



NOTE

The Extreme Networks Wireless Management Suite (WMS) is a recommended utility to plan the deployment of the controller and view its interface statistics once operational in the field. Extreme Networks WMS can help optimize the positioning and configuration of a controller (and its associated radios) in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Extreme Networks website.

The controller screen displays two tabs supporting the following configuration activities:

- [Setting the Controller Country Code on page 56](#)
- [Viewing Controller Statistics on page 66](#)



NOTE

When the controller's configuration is successfully updated (using the Web UI), the affected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the affected screen's Status field and the screen remains displayed. With file transfer operations, the transfer screen remains open during the transfer and remains open upon completion (with status displayed within the Status field).

Setting the Controller Country Code

When initially logging into the system, the controller requests that you enter the correct country code for your region. If a country code is not configured, a warning message will display stating that an incorrect country setting will lead to the illegal use of the controller. Consequently, selecting the correct country is extremely important. Each country has its own regulatory restrictions concerning electromagnetic emissions (channel range) and the maximum RF signal strength transmitted. To ensure compliance with national and local laws, be sure to set the *Country* value correctly.



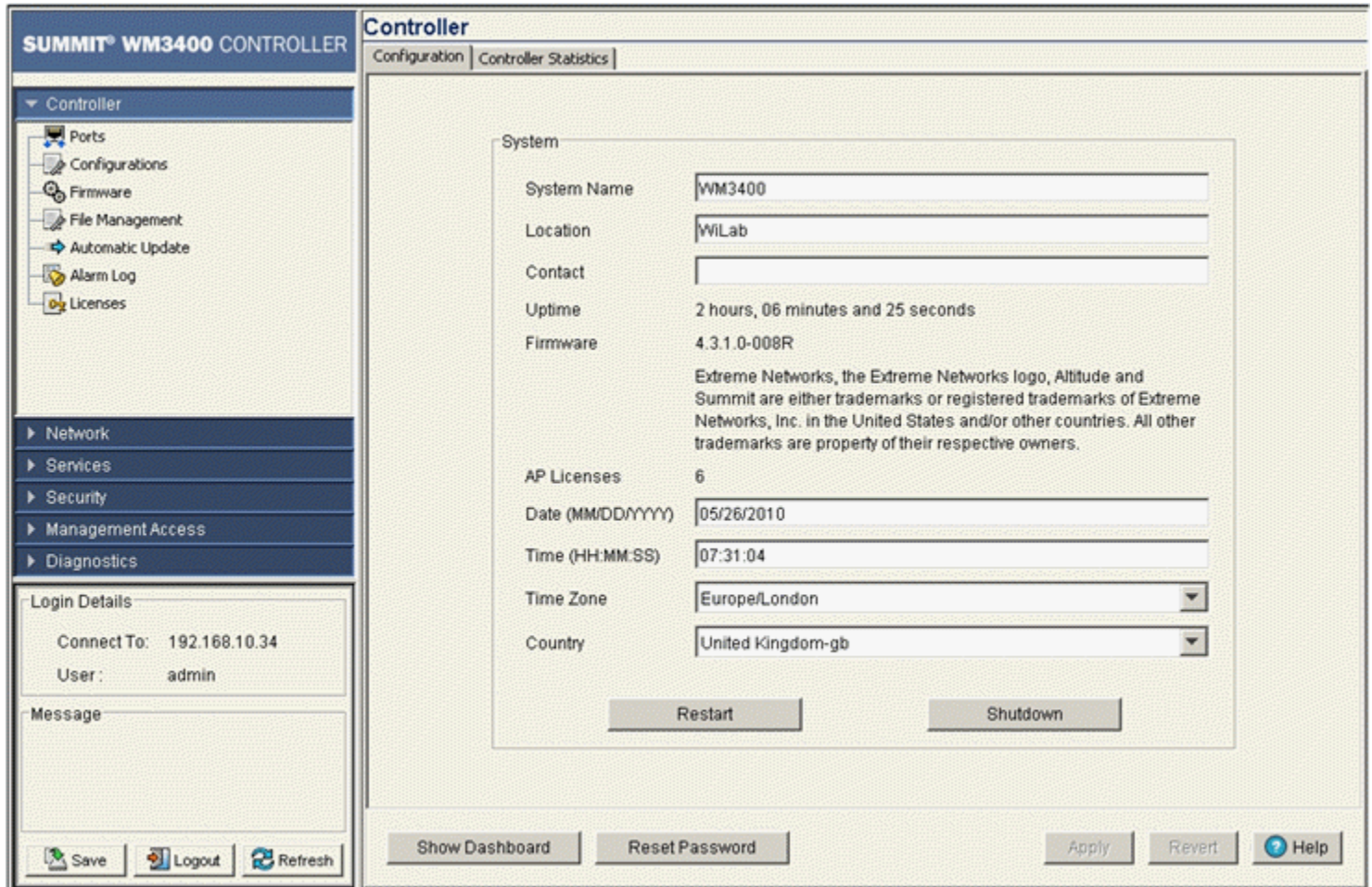
NOTE

To ensure proper operation of the wireless controller and Access Ports, make sure the country code set on the wireless controller matches the country code set on the Access Ports or Adaptive APs.

Viewing the Controller Configuration

To view a high-level display of the controller configuration:

- 1 Select *Controller* from the main menu tree.
- 2 Click the *Configuration* tab.



3 Refer the *System* field to view or define the following information:

System Name	Displays the designated system name. Provide a system name serving as a reminder of the user base the controller supports (engineering, retail, etc.).
Location	The Location parameter serves as a reminder of where the controller can be found. Define the System Name as a specific identifier of the controller's location. Use the System Name and Location parameters together to optionally define the controller name by the radio coverage type it supports and physical location. For example, "second floor engineering."
Contact	Displays a <i>Contact</i> value for system administration and troubleshooting. This name should be the network administrator responsible for controller operations.
Uptime	Displays the current operational time for the device name defined within the System Name field. Uptime is the cumulative time since the controller was last rebooted or lost power.
Firmware	Displays the current firmware version running on the controller. This version should be periodically compared to the most recent version available on the Extreme Networks website, as versions with increased functionality are periodically released.

AP Licenses	Displays the number of Access Port/AAP licenses currently available for the controller. This value represents the maximum number of Access Ports the controller is licensed to adopt.
Date (MM/DD/YYYY)	Displays the day, month and year currently used with the controller.
Time	Displays the time of day used by the controller.
Time Zone	Use the drop-down menu to specify the time zone used with the controller. Adjusting the time zone will in turn, cause an adjustment to the time displayed.
Country	Use the drop-down menu to specify the correct country of operation. Selecting the country incorrectly could render your controller as operating illegally.

- Click the *Restart* button to reboot the controller. The controller itself does not include a hardware reset feature.



CAUTION

When rebooting the controller, the RADIUS Server will also be restarted regardless of its state before the reboot.

- Click the *Shutdown* button to shutdown and power off the controller.



NOTE

The shutdown command will shutdown the controller, but the fans will remain on.

- Click the *Show Dashboard* button to display a screen with important indicators of controller health and status. For more information, see [“Controller Dashboard Details” on page 59](#). Referencing the *Details* screen is recommended before new configurations are employed that utilize increased controller bandwidth.
- Click the *Reset Password* button to display a screen to reset the password.

Enter the new password within the *Password* and *Confirm Password* fields and click *OK*.

**NOTE**

When entering a new password for the controller, please note that the password must be a minimum of 8 characters long.

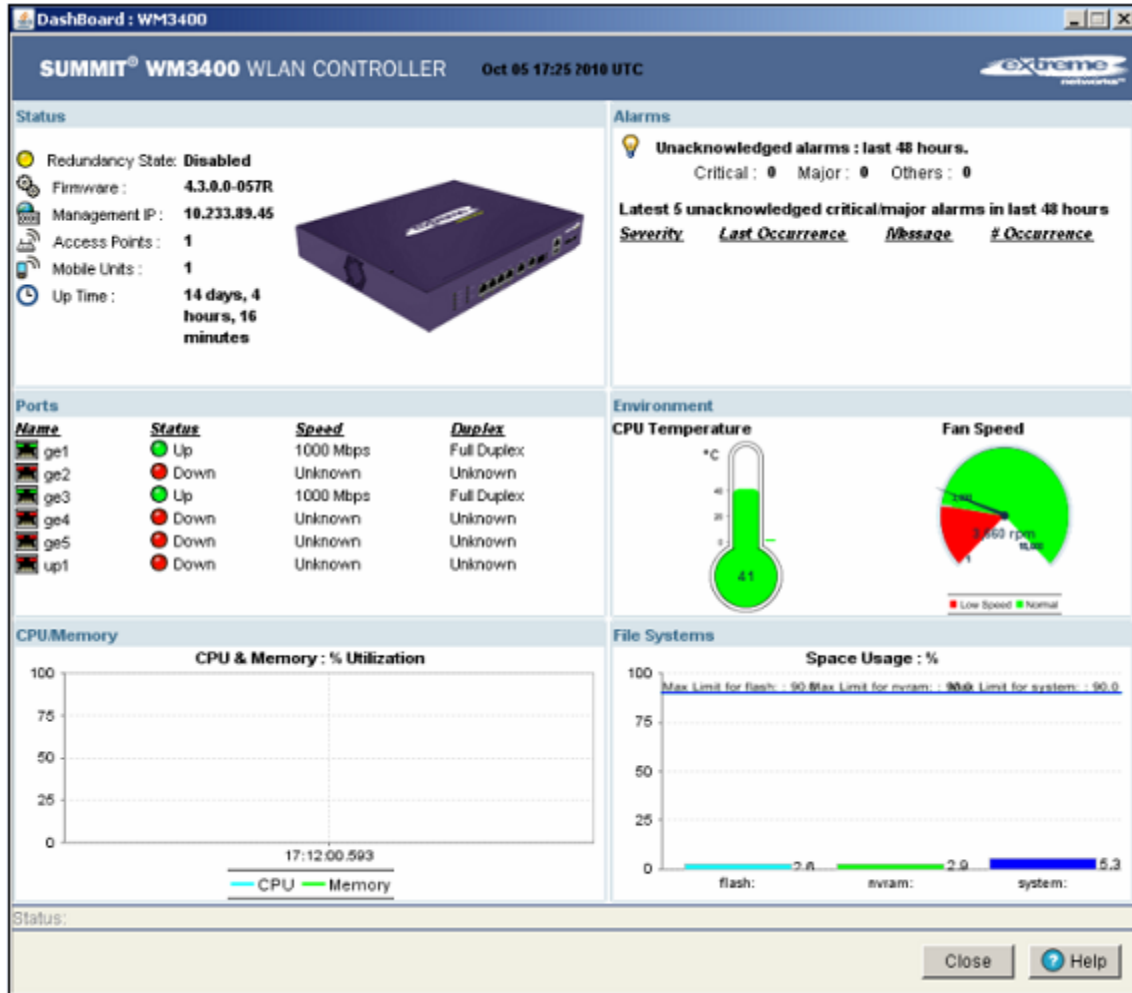
- 8 Click the *Revert* button to undo any changes. The *Revert* button must be clicked before hitting the *Apply* button for any changes to be reverted.
- 9 Click the *Apply* button to save the updates (to the Time Zone or Country parameters specifically).

Controller Dashboard Details

Each Extreme Networks wireless LAN controller platform contains a dashboard which represents a high-level graphical overview of central controller processes and hardware. When logging into the controller, the dashboard should be the first place you go to assess overall controller performance and any potential performance issues.

Click the *Show Dashboard* button (within the Controller screen's Configuration tab) to display the current health of the controller:

Summit WM3400 Controller Dashboard








The *Dashboard* screen displays the current health of the controller and is divided into fields representing the following important diagnostics:

- Alarms
- Ports
- Environment
- CPU/Memory
- File Systems

Apart from the sections mentioned above, it also displays the following status:

Redundancy State Displays the Redundancy State of the controller. The status can be either Enabled or Disabled.

- *Enabled*—Defined a green state.
- *Disabled*—Defined by a yellow state.

	Firmware	Displays the Firmware version of the current software running on the wireless controller.
	Management IP	Displays the Management IP address of the controller.
	Access Ports	Displays the total number of Access Ports adopted by the controller.
	Mobile Units	Displays the total number of MUs associated with the controller.
	Up Time	Displays the actual controller uptime. The <i>Uptime</i> is the current operational time of the device defined within the System Name field. Uptime is the cumulative time since the controller was last rebooted or lost power.

1 Refer to the *Alarms* field for details of all the unacknowledged alarms generated during the past 48 hours. The alarms are classified as:

- *Critical*—Denoted by a red indicator. These alarms warrant immediate attention.
- *Major*—Denoted by a yellow indicator. These alarms warrant attention.
- *Others*—Denoted by a blue indicator.

The alarms field also displays details (in a tabular format) of the 5 most recent unacknowledged critical/major alarms raised during the past 48 hours. The table displays the following details:

Severity	Displays the severity of the alarm. It can be either Critical or Major.
Last Occurrence	Displays the time when the alarm was reported.
Message	Displays the message associated with the alarm.
# Occurrence	Displays the number of times during the past 48 hours such an alarm was generated.

2 Refer to the *Ports* field for link, speed and duplex status of each physical port on the controller's front panel. It displays the following details in a tabular format:

Name	Displays the name of the port (ge1-5 or up1)
Status	Displays the status of the port, either—Up or Down
Speed	Displays the speed at which the port transmits or receives data.
Duplex	Displays the status of the port, either—Full Duplex or Unknown.

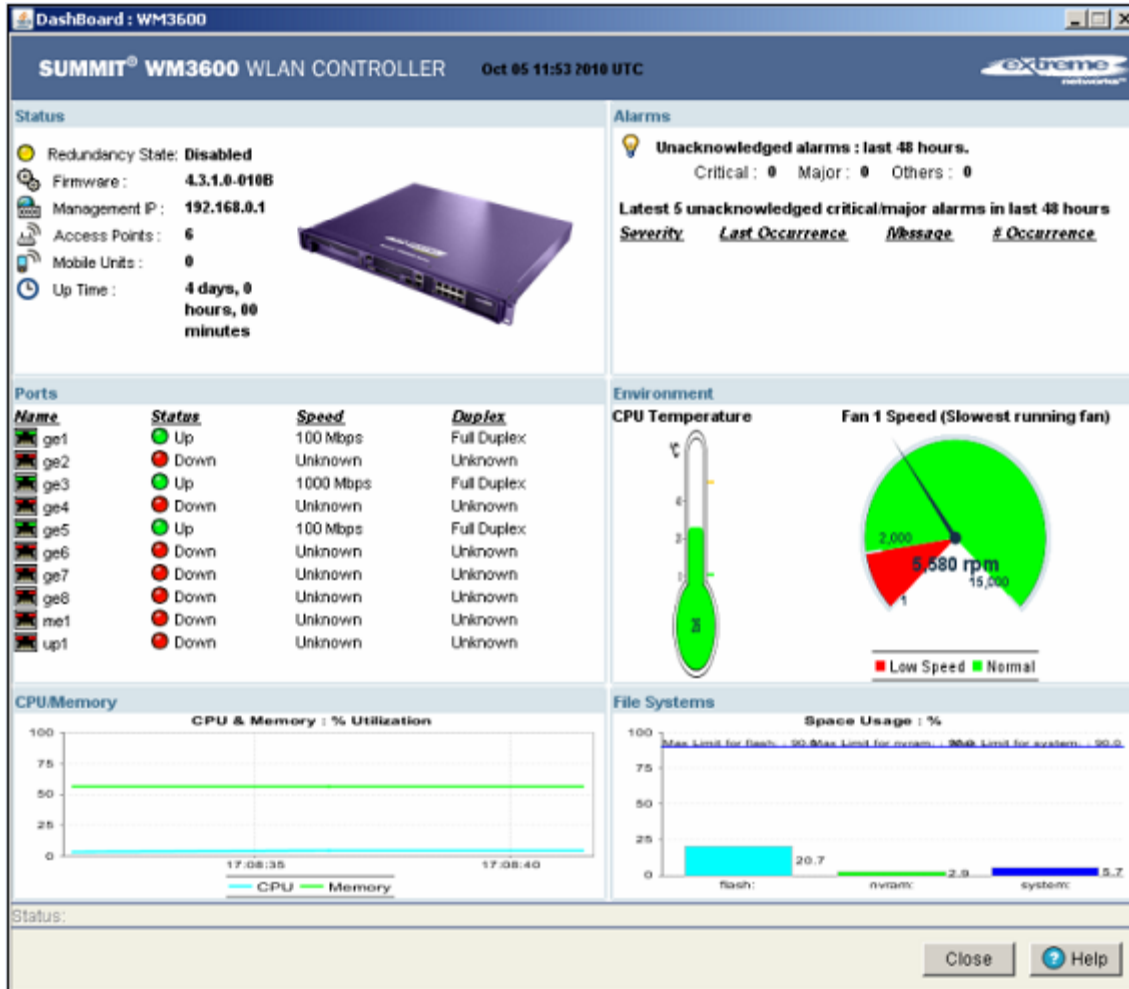
3 The *Environment* section displays the CPU temperature. On the WM3400, WM3600 and WM3700 platforms, it displays the fan speed of the slowest running fan in the system. It also displays the valid threshold range set by the user.

4 The *CPU/Memory* section displays the free memory available with the RAM.

5 The *File Systems* section displays the free file system available for:

- flash
- nvram
- system







Summit WM3600 Controller Dashboard



The *Dashboard* screen displays the current health of the controller and is divided into fields representing the following important diagnostics:

- Alarms
- Ports
- Environment
- CPU/Memory
- File Systems

Apart from the sections mentioned above, it also displays the following status:

Redundancy State	Displays the Redundancy State of the controller. The status can be either Enabled or Disabled.
	<ul style="list-style-type: none">• <i>Enabled</i>—Defined a green state.• <i>Disabled</i>—Defined by a yellow state.
Firmware	Displays the Firmware version of the current software running on the wireless controller.
	
Management IP	Displays the Management IP address of the controller.
	
Access Ports	Displays the total number of Access Ports adopted by the controller.
	
Mobile Units	Displays the total number of MUs associated with the controller.
	
Up Time	Displays the actual controller uptime. The <i>Uptime</i> is the current operational time of the device defined within the System Name field. Uptime is the cumulative time since the controller was last rebooted or lost power.
	

1 Refer to the *Alarms* field for details of all the unacknowledged alarms generated during the past 48 hours. The alarms are classified as:

- *Critical*—Denoted by a red indicator. These alarms warrant immediate attention.
- *Major*—Denoted by a yellow indicator. These alarms warrant attention.
- *Others*—Denoted by a blue indicator.

The alarms field also displays details (in a tabular format) of the 5 most recent unacknowledged critical/major alarms raised during the past 48 hours. The table displays the following details:

Severity	Displays the severity of the alarm. It can be either Critical or Major.
Last Occurrence	Displays the time when the alarm was reported.
Message	Displays the message associated with the alarm.
# Occurrence	Displays the number of times during the past 48 hours such an alarm was generated.

2 Refer to the *Ports* field for link, speed and duplex status of each physical port on the controller's front panel. It displays the following details in a tabular format:

Name	Displays the name of the port (ge1-8, me1 or up1)
Status	Displays the status of the port, either— Up or Down
Speed	Displays the speed at which the port transmits or receives data.
Duplex	Displays the status of the port, either— Full Duplex or Unknown.

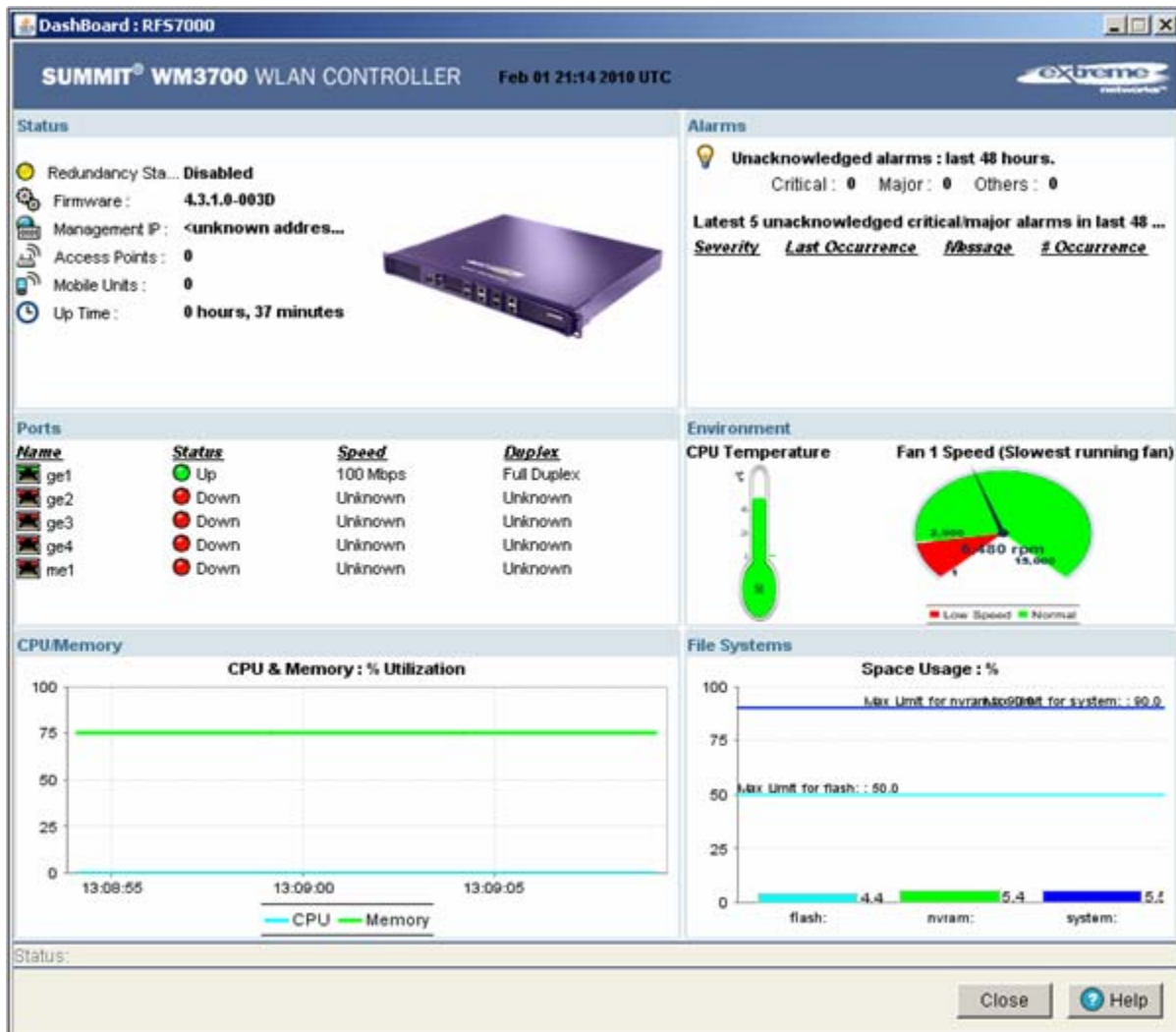
3 The *Environment* section displays the CPU temperature. It displays the valid threshold range set by the user.

4 The *CPU/Memory* section displays the free memory available with the RAM.

5 The *File Systems* section displays the free file system available for:

- flash
- nvram
- system







Summit WM3700 Controller Dashboard



The *Dashboard* screen displays the current health of the controller and is divided into fields representing the following important diagnostics:

- Alarms
- Ports
- Environment
- CPU/Memory
- File Systems

Apart from the sections mentioned above, it also displays the following status:

Redundancy State	Displays the Redundancy State of the controller. The status can be either Enabled or Disabled.
	<ul style="list-style-type: none">• <i>Enabled</i>—Defined by a green state.• <i>Disabled</i>—Defined by a yellow state.
Firmware	Displays the Firmware version of the current software running on the wireless controller.
	
Management IP	Displays the Management IP address of the controller.
	
Access Ports	Displays the total number of Access Ports adopted by the controller.
	
Mobile Units	Displays the total number of MUs associated with the controller.
	
Up Time	Displays the actual controller uptime. The <i>Uptime</i> is the current operational time of the device defined within the System Name field. Uptime is the cumulative time since the controller was last rebooted or lost power.
	

1 Refer to the *Alarms* field for details of all the unacknowledged alarms generated during the past 48 hours. The alarms are classified as:

- *Critical*—Denoted by a red indicator. These alarms warrant immediate attention.
- *Major*—Denoted by a yellow indicator. These alarms warrant attention.
- *Others*—Denoted by a blue indicator.

The alarms field also displays details (in a tabular format) of the 5 most recent unacknowledged critical/major alarms raised during the past 48 hours. The table displays the following details:

Severity	Displays the severity of the alarm. It can be either Critical or Major.
Last Occurrence	Displays the time when the alarm was reported.
Message	Displays the message associated with the alarm.
# Occurrence	Displays the number of times during the past 48 hours such an alarm was generated.

2 Refer to the *Ports* field for link, speed and duplex status of each physical port on the controller's front panel. It displays the following details in a tabular format:

Name	Displays the name of the port (ge1, ge2, ge3, ge4 and me1).
Status	Displays the status of the port, either—Up or Down
Speed	Displays the speed at which the port transmits or receives data.
Duplex	Displays the status of the port, either—Full Duplex or Unknown.

3 The *Environment* section displays the CPU temperature. It displays the valid threshold range set by the user.

4 The *CPU/Memory* section displays the free memory available with the RAM.

5 The *File Systems* section displays the free file system available for:

- flash
- nvram
- system

Viewing Controller Statistics

The *Controller Statistics* tab displays an overview of the recent network traffic and RF status for the controller.

To display the Controller Statistics tab:

- 1 Select *Controller* from the main menu tree.
- 2 Click the *Controller Statistics* tab at the top of the Controller screen.

SUMMIT® WM3400 CONTROLLER

Controller

Configuration | **Controller Statistics**

Number of MUs Associated 1 Number of APs Adopted 1
 Number of Radios Adopted 2

Traffic (does not include retry overhead)

	Total	Received	Transmitted
Pkts per second	0.00 0.00 pps	0.00 0.00 pps	0.00 0.00 pps
Throughput	0.00 0.00 Mbps	0.00 0.00 Mbps	0.00 0.00 Mbps
Avg. Bit Speed	0.00 0.00 Mbps		
% Non-unicast pkts	0.00 0.00		

RF Status

Average Signal	0.00 0.00 dBm
Average Noise	0.00 0.00 dBm
Average SNR (dB)	0.00 0.00

Errors

Average Number of Retries	0.00 0.00
% Gave Up Pkts	0.00 0.00
% Non-decryptable Pkts	0.00 0.00

■ last 30 seconds ■ last hour

Save Logout Refresh ? Help

3 Refer to the *Controller Statistics* field for the following read-only information about associated MUs:

- | | |
|--------------------------|---|
| Number of MUs Associated | Displays the total number of MUs currently associated to the controller. |
| Number of APs Adopted | Displays the total number of Access Ports/Points currently adopted by the controller. |

Number of Radios Adopted Displays the total number of radios currently adopted by the controller.

4 Refer to the *Traffic* field to assess network traffic for associated APs and radios:

Pkts per second Displays the packet transmission rate for received and transmitted packets over last 30 seconds and 1 hour.

Throughput Displays the traffic throughput for packets received, packets transmitted, and total packets over last 30 seconds and 1 hour.

Avg. Bit Speed Displays the average bit speed for the controller over last 30 seconds and 1 hour. Use the average bit speed value to help determine overall network speeds and troubleshoot network congestion.

% Non-unicast pkts Displays the percentage of non-unicast packets seen (received & transmitted) by the controller over last 30 seconds and 1 hour. Non-unicast traffic includes both multicast and broadcast traffic.

Broadcast multicast, and flooded packets are sent over the air at the slowest rate on every radio in the WLAN and therefore have a much larger airtime utilization than unicast packets and a greater chance of causing collisions.

5 The *RF Status* section displays the following read-only RF radio signal information for associated APs and radios:

Avg. Signal Displays the average signal strength for MUs associated with the controller over the last 30 seconds and 1 hour. Typically, the higher the signal, the closer the MU.

Avg. Noise Displays the average RF noise for all MUs associated with the selected WLAN. MU noise for the last 30 seconds is displayed in black and the number in blue represents MU noise for the last hour. If MU noise is excessive, consider moving the MU closer to the Access Point, or in area with less conflicting network traffic. Excessive noise may also be an indication of network interference.

Avg. SNR Displays the average *Signal to Noise Ratio* (SNR) for all MUs associated with the controller. The Signal to Noise Ratio is an indication of overall RF performance on the wireless network.

6 Refer to the *Errors* field for read-only packet error and loss information for associated Access Points/Points and radios:

Average Number of Retries Displays the average number of retries for all MUs associated with the controller. The number in black represents average retries for the last 30 seconds and the number in blue represents average retries for the last hour.

If the Average Number of Retries starts increasing, this indicates that MUs are not getting a good link back to the AP.

% Gave Up Pkts Displays the percentage of packets which the controller gave up on for all MUs associated with the controller. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

If this field displays a non-zero number it indicates bad links causing packets to the MUs.

% Non-decryptable Pkts	<p>Displays the percentage of undecryptable packets for all MUs associated with the controller. The number in black represents undecryptable pkts for the last 30 seconds and the number in blue represents undecryptable pkts for the last hour.</p> <p>If this field displays a non-zero number it can indicate outside intrusion into the network or an MU using incorrect cryptography such as a a misconfigured static key.</p>
------------------------	--

Viewing Controller Port Information

The *Port* screen displays configuration, runtime status, and statistics of the ports on the controller.



NOTE

The ports available vary by controller platform.

Summit WM3600: ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1

Summit WM3700: ge1, ge2, ge3, ge4, me1

Summit WM3400: ge1, ge2, ge3, ge4, ge5, up1

The port types are defined as follows:

GE#	GE ports are available on the Summit WM3400, Summit WM3600 and Summit WM3700 platforms. GE ports on the Summit WM3400 and Summit WM3600 are RJ-45 which support 10/100/1000Mbps. GE ports on the Summit WM3700 can be RJ-45 or fiber ports which support 10/100/1000Mbps.
ME#	ME ports are available on the Summit WM3600 and Summit WM3700 platforms. ME ports are out-of-band management ports which can be used to manage the controller via CLI or Web UI even when the other ports on the controller are unreachable.
UP#	An UP port is available on the Summit WM3400 and Summit WM3600 platform only. This port is used to connect the controller to the backbone network. The UP port on the controller supports either RJ-45 or fiber. The UP port is the preferred way to connect to the backbone as it has a non-blocking 1gbps connection unlike the ge ports.

The *Port* screen contains three tabs supporting the following port assessment activities:

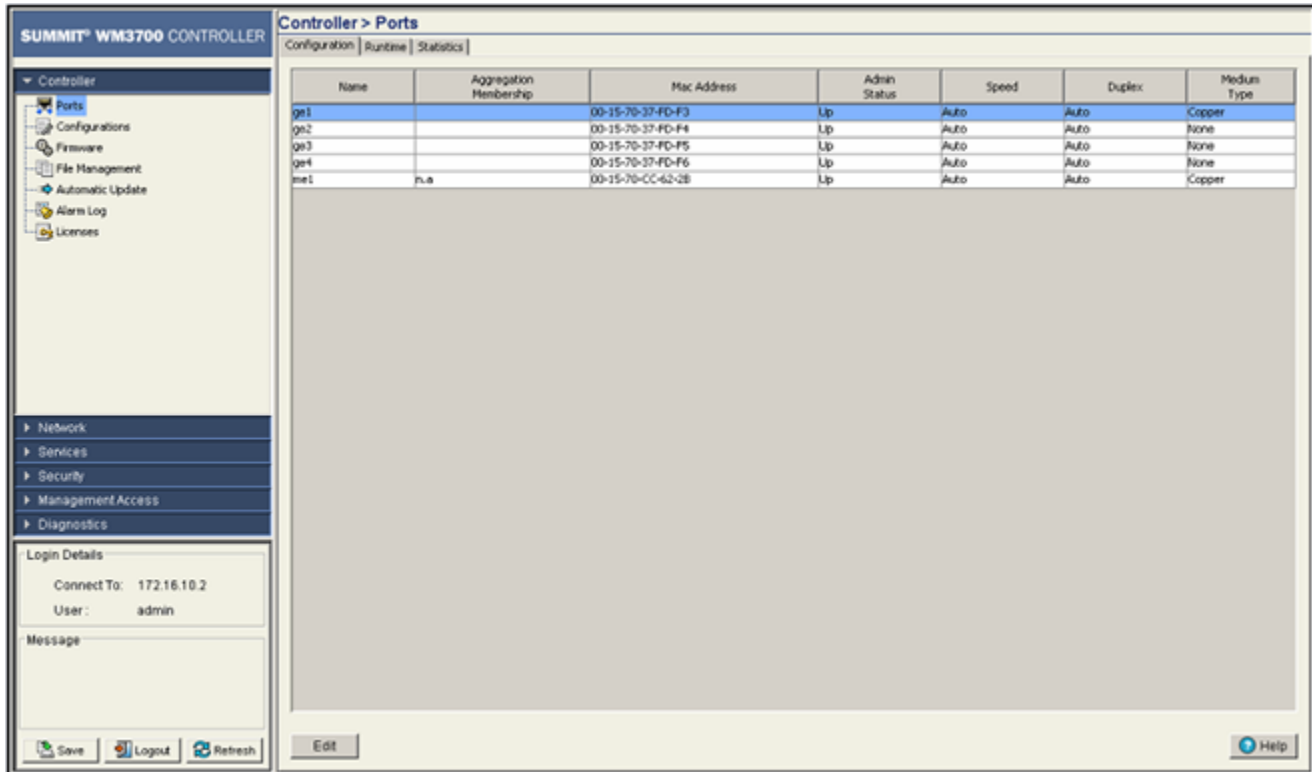
- “Viewing the Port Configuration”
- “Viewing the Ports Runtime Status”
- “Reviewing Port Statistics”

Viewing the Port Configuration

The *Configuration* tab displays the current configuration for the controller ports. Use the port configuration information to determine whether an existing port configuration can be used as is or requires modification for use within the controller managed network.

To view configuration details for the uplink and downlink ports:

- 1 Select *Controller > Ports* from the main menu tree.
- 2 Select the *Configuration* tab to display the following read-only information:



Name	Displays the current port name. The port names available vary by controller. Summit WM3600: ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1, wan Summit WM3700: ge1, ge2, ge3, ge4, me1 Summit WM3400: ge1, ge2, ge3, ge4, ge5. up1
Aggregation Membership	The Aggregation Membership value displays the channel group the port is a member of. (Available on WM3400, WM3600 and WM3700.)
MAC Address	Displays the port's MAC Address. This value is read-only, set at the factory and cannot be modified.
Admin Status	Displays whether the port is currently Up or Down.
Speed	Displays the current speed of the data transmitted and received over the port.
Duplex	Displays the port as either half or full duplex.
Medium Type	(Available on WM3400, WM3600 and WM3700.) The Medium Type value displays the physical connection type of the port. Medium types are: Copper: Used on RJ-45 Ethernet Ports Optical: Used on Fiber Optic Gigabit Ethernet Ports

- 3 Select a port and click the *Edit* button to modify the port configuration. For additional information, see [“Editing the Port Configuration” on page 70.](#)

Editing the Port Configuration

To modify the port configuration:

- 1 Select a port from the table displayed within the Configuration screen.
- 2 Click the *Edit* button.

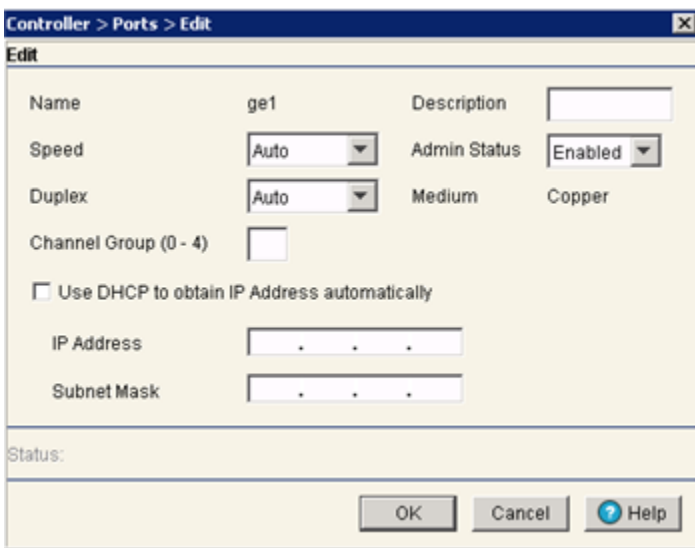
A *Port Change Warning* screen displays, stating any change to the port setting could disrupt access to the controller. Communication errors may occur even if modifications made are successful.



- 3 Click the *OK* button to continue.

Optionally, select the *Don't show this message again for the rest of the session* checkbox to disable the pop-up.

- 4 Use the *Edit* screen to modify the following port configurations for the selected port.



Name Displays the read-only name assigned to the port.

Speed	Select the speed at which the port can receive and transmit the data. Select from the following range: <ul style="list-style-type: none"> • 10 Mbps • 100 Mbps • 1000 Mbps • Auto
Duplex	Modify the duplex status by selecting one of the following options: <ul style="list-style-type: none"> • Half • Full • Auto
Channel Group	(Available on WM3400, WM3600 and WM3700.) Optionally set the Channel Group number 0 through 4 on the WM3400, WM3600 or WM3700 to associate the port with one of the channel aggregation groups. The controller bundles individual Ethernet links (over the selected channel) into a single logical link that provides bandwidth between the controller and another controller or host. The port speed used is dependant on the Duplex value selected (full, half, or auto). If a segment within a channel fails, traffic previously carried over the failed link is routed to the remaining segments within the channel. A trap is sent upon a failure identifying the controller, channel, and failed link.
Description	Enter a brief description for the port. The description should reflect the port's intended function to differentiate it from others with similar configurations.
Admin Status	Either Enable (activate) or Disable (shutdown) the admin status of the port.
Medium	Displays the current (read-only) connection medium used by this port.

Read-only details about the port's cabling connection also display within the *Edit* screen. This information should be used to determine the configuration defined for this port.

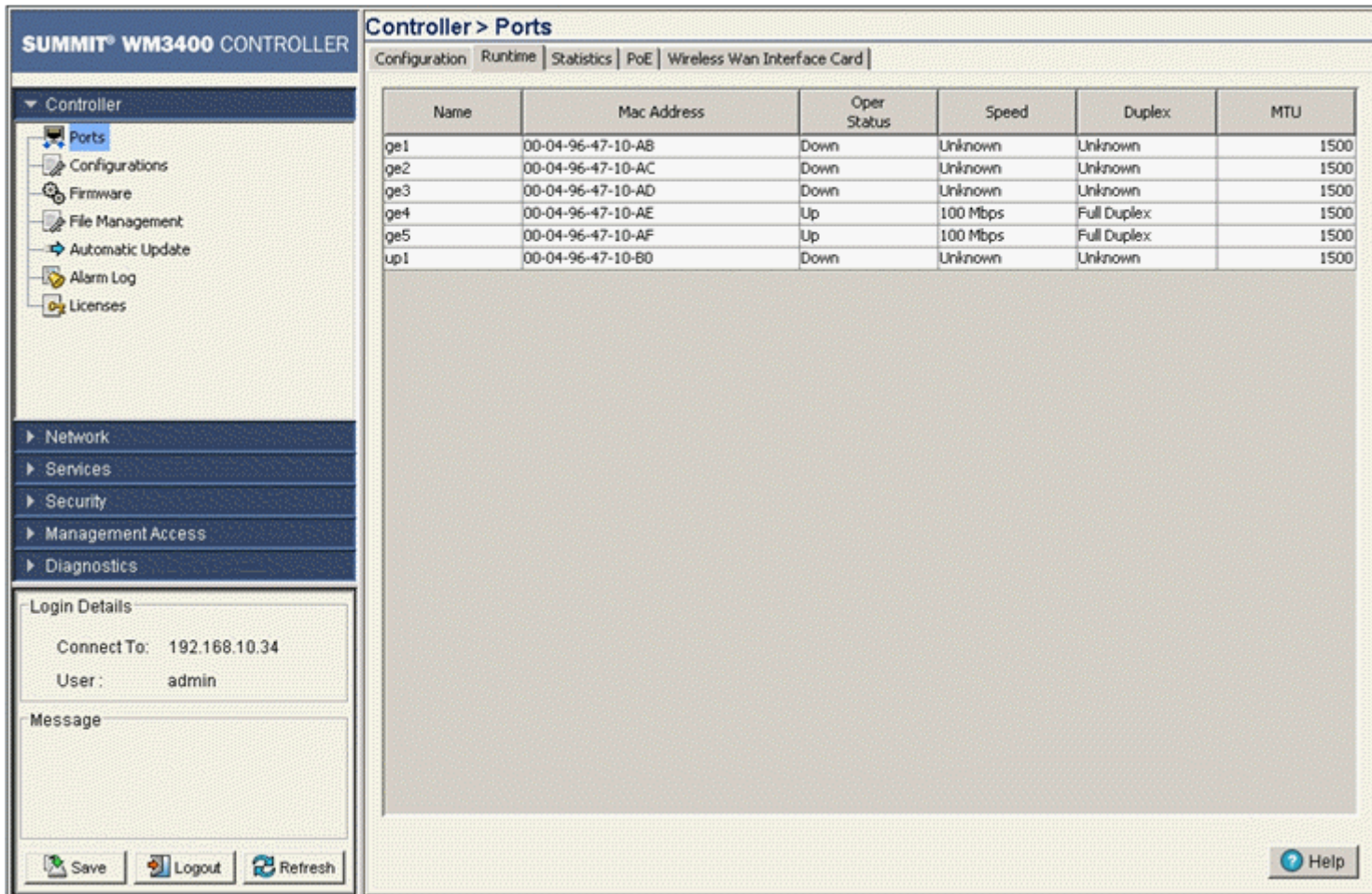
- 5 Click the *OK* button to commit the changes made to the port configurations.
- 6 Click *Cancel* to disregard any changes and revert back to the last saved configuration.

Viewing the Ports Runtime Status

The *Runtime* tab displays read-only runtime configuration for uplink and downlink ports.

To view the runtime configuration details of the uplink and downlink ports:

- 1 Select *Controller* > *Ports* from the main menu tree.



- 2 Select the *Runtime* tab to display the following read-only information:

Name	Displays the port's current name.
MAC Address	Displays the port's MAC Address. This value is read-only, set at the factory and cannot be modified.
Oper Status	Displays the link status of the port. The port status can be either Up or Down.
Speed	Displays the current speed of the data transmitted and received over the port.
Duplex	Displays the port as either <i>half duplex</i> , <i>full duplex</i> , or <i>Unknown</i> .
MTU	Displays the <i>maximum transmission unit</i> (MTU) setting configured on the port. The MTU value represents the largest packet size that can be sent over a link. 10/100 Ethernet ports have a maximum MTU setting of 1500.

Reviewing Port Statistics

The *Statistics* tab displays read-only statistics for Ethernet ports. Use this information to assess if configuration changes are required to improve network performance.

To view the runtime configuration details of the controller ports:

- 1 Select *Controller > Ports* from the main menu tree.
- 2 Select the *Statistics* tab.

The screenshot shows the Summit WM3400 Controller web interface. The main menu on the left includes 'Controller', 'Network', 'Services', 'Security', 'Management Access', and 'Diagnostics'. Under 'Controller', there are sub-menus for 'Ports', 'Configurations', 'Firmware', 'File Management', 'Automatic Update', 'Alarm Log', and 'Licenses'. The 'Ports' sub-menu is selected, and the 'Statistics' tab is active. The table below shows the following data:

Name	Bytes In	Packets In	Packets In Dropped	Packets In Error	Bytes Out	Packets Out	Packets Out Dropped	Packets Out Error
ge1	0	0	0	0	0	0	0	0
ge2	0	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0	0
ge4	687764	4630	0	0	2211856	10094	0	0
ge5	1836945	5962	0	0	252416	1010	0	0
up1	0	0	0	0	0	0	0	0

3 Refer to the *Statistics* tab to display the following read-only information:

- Name** Defines the port name. The port names available vary by controller.
Summit WM3600: ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1, wan
Summit WM3700: ge1, ge2, ge3, ge4, me1
Summit WM3400: ge1, ge2, ge3, ge4, ge5, up1
- Bytes In** Displays the total number of bytes received by the port.
- Packets In** Displays the total number of packets received by the port.
- Packets In Dropped** Displays the number of packets dropped by the port. If the number appears excessive, a different port could be required.
- Packets In Error** Displays the number of erroneous packets received by the port. If the number appears excessive, try using a different port and see if the problem persists.
- Bytes Out** Displays the total number of bytes transmitted by the port.
- Packets Out** Displays the total number of packets transmitted by the port. A low value could be an indication of a network problem.

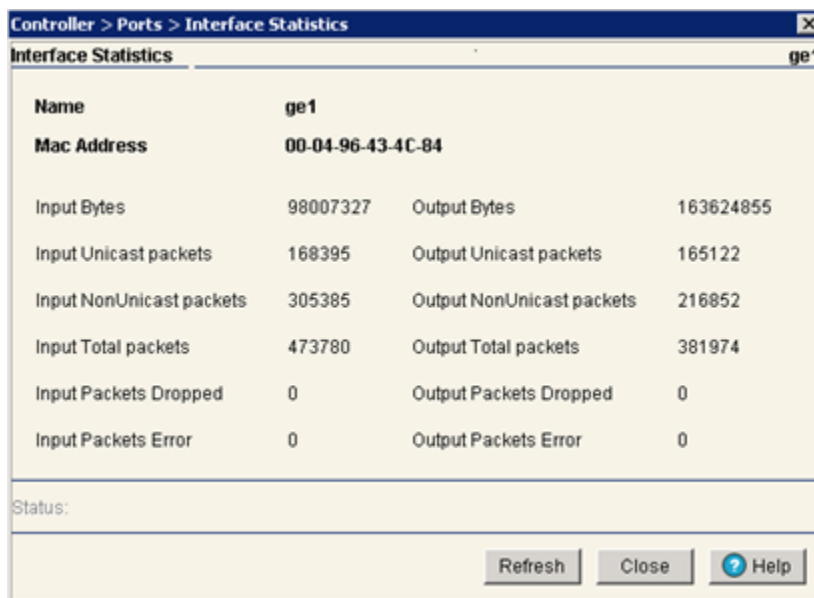
Packets Out Dropped	Displays the total number of packets dropped during transmission. A high value may be an indication of network throughput issues.
Packets Out Error	Displays the total number of erroneous transmitted packets.

- 4 Select a port and click the *Details* button to see the detailed port statistics. For more information, refer to [“Detailed Port Statistics” on page 74](#).
- 5 Select a port and click the *Graph* button to view the port statistics in a graphical format. For more information, refer to [“Viewing the Port Statistics Graph” on page 75](#).

Detailed Port Statistics

To view detailed statistics for a port:

- 1 Select a port from the table displayed within the *Statistics* screen.
- 2 Click the *Details* button.



- 3 The *Interface Statistics* screen displays. This screen displays the following statistics for the selected port:

Name	Displays the port name.
MAC Address	Displays physical address information associated with the interface. This address is read-only (hard-coded at the factory) and cannot be modified.
Input Bytes	Displays the number of bytes received on the interface.
Input Unicast Packets	Displays the number of unicast packets (packets directed towards the interface) received on the interface.
Input NonUnicast Packets	Displays the number of NonUnicast Packets (Multicast and Broadcast Packets) received on the interface.
Input Total Packets	Displays the total number of packets received on the interface.
Input Packets Dropped	Displays the number of received packets dropped by the interface by the input Queue of the hardware unit /software module associated with the VLAN. Packets are dropped when the input Queue is full or unable to process incoming traffic.

Input Packets Error	Displays the number of packets with errors received on the interface. Input Packet Errors are input errors due to: no buffer space/ignored packets due to broadcast storms, packets larger than maximum packet size, framing errors, input rate exceeding the receiver's data handling rate, or cyclic redundancy check errors. In all of these cases, an error is reported and logged.
Output Bytes	Displays the number of bytes transmitted from the interface.
Output Unicast Packets	Displays the number of unicast packets (packets directed towards a single destination address) transmitted from the interface.
Output NonUnicast Packets	Displays the number of unicast packets transmitted from the interface.
Output Total Packets	Displays the total number of packets transmitted from the interface.
Output Packets Dropped	Displays the number of transmitted packets dropped from the interface. Output Packets Dropped are packets dropped when the output queue of the device associated with the interface is saturated.
Output Packets Error	Displays the number of transmitted packets with errors. Output Packet Errors are the sum of all the output packet errors, malformed packets, and misaligned packets received.

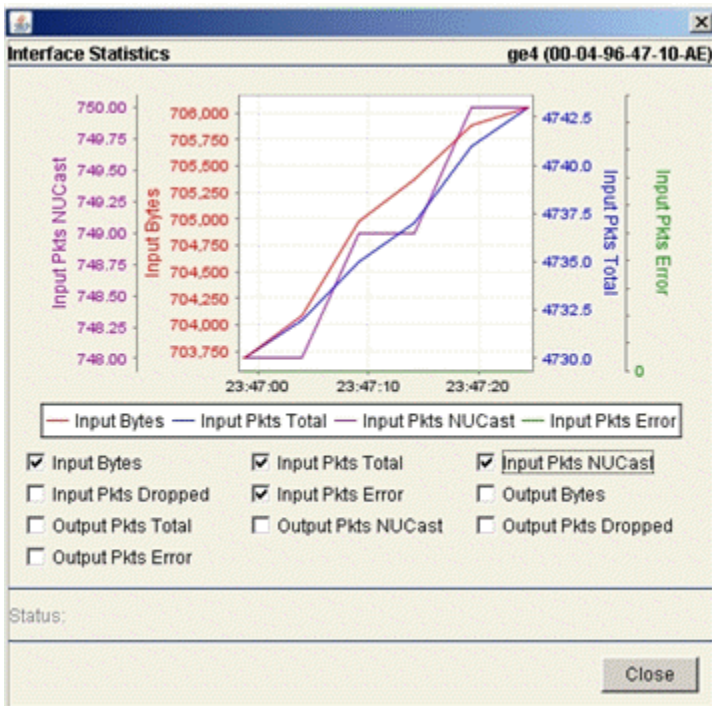
- 4 The *Status* is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 5 Click the *Refresh* button to refresh the port statistics.
- 6 Click the *Close* button to exit out of the screen.

Viewing the Port Statistics Graph

The controller continuously collects data for port statistics. Even when the port statistics graph is closed, data is still tallied. Periodically display the port statistics graph for assessing the latest information.

To view a detailed graph for a port:

- 1 Select a port from the table displayed in the *Statistics* screen.
- 2 Click the *Graph* button.



The *Interface Statistics* screen displays for the selected port. The screen provides the option to view the following:

- Input Bytes
- Input Pkts Dropped
- Output Pkts Total
- Output Pkts Error
- Input Pkts Total
- Input Pkts Error
- Output Pkts NUCast
- Input Pkts NUCast
- Output Bytes
- Output Pkts Dropped

3 Display any of the above by selecting the checkbox associated with it.



NOTE

You are not allowed to select (display) more than four parameters at any given time.

4 Click the *Close* button to exit out of the screen.

Power over Ethernet (PoE)



NOTE

Power over Ethernet is supported on Summit WM3600 and Summit WM3400 controllers.

The Summit WM3600 and Summit WM3400 controllers support 802.3af 802.3af Power over Ethernet (PoE) on each of its eight *ge* ports. The PoE screen allows users to monitor the power consumption of the ports and configure power usage limits and priorities for each of the *ge* ports.

To view the PoE configuration:

- 1 Select *Controller* > *Ports* from the main menu tree.
- 2 Select the *PoE* tab:

SUMMIT® WM3400 CONTROLLER

Controller > Ports

Configuration | Runtime | Statistics | **PoE** | Wireless Wan Interface Card

PoE Global Configuration

PoE Firmware Version: 211 build 1

Power Budget: 90.0 watts

Power Consumption: 5.0 watts

Power Usage Threshold for Sending Trap: %

Port	PoE	Class	Priority	Limit (watts)	Power (watts)	Voltage (volts)	Current (mA)	Status
ge1	Up	0	High	36.0	0.0	0.0	0	Off
ge2	Up	0	High	36.0	0.0	0.0	0	Off
ge3	Up	0	High	36.0	0.0	0.0	0	Off
ge4	Up	0	High	36.0	5.7	48.1	119	On
ge5	Up	0	High	36.0	0.0	0.0	0	Off

Buttons: Save, Logout, Refresh, Edit, Help



NOTE

The PoE screen is available on the Summit WM3600 and Summit WM3400 controllers. The Summit WM3700 controller does not have Power over Ethernet on any ports and will not display the PoE tab.

The *PoE Global Configuration* section displays the following power information.

PoE Firmware Version	Displays build number.
Power Budget	Displays the total watts available for Power over Ethernet on the controller.
Power Consumption	Displays the total watts in use by Power over Ethernet on the controller.
Power Usage Threshold for Sending Trap	Specify a percentage of power usage as the threshold before the controller sends an SNMP trap. The percentage is a percentage of the total power budget of the controller.

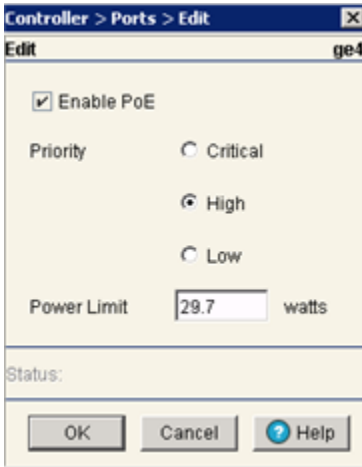
If you have modified the *Power Usage Threshold for Sending Trap* value, click the *Apply* button to save the changes.

Port	Displays the port name for each of the PoE capable ports.
PoE	Displays the PoE status of each PoE capable port. Status will display Up when PoE is available on the port and Down when PoE is unavailable on the port.
Class	Displays the IEEE Power Classification for each port: Class Number—Maximum Power Required from Controller <ul style="list-style-type: none"> • 0 (unknown)—15.4 Watts • 1—4 Watts • 2—7 Watts • 3—15.4 Watts
Priority	Displays the priority mode for each of the PoE ports. The priority options are: <ul style="list-style-type: none"> • Critical • High • Low
Limit (watts)	Displays the power limit in watts for each of the PoE ports. The maximum power limit per port is 36 watts.
Power (watts)	Displays each PoE ports power usage in watts.
Voltage (volts)	Displays each PoE ports voltage usage in volts.
Current (mA)	Displays each PoE ports current usage in milliAmps.
Status	Displays the operational status for each PoE port. Ports can be either <i>On</i> or <i>Off</i> .

Editing Port PoE Settings

To modify the PoE settings for a port:

- 1 Select a port to edit from the table.
- 2 Click the *Edit* button. The *PoE Edit* screen shows the port PoE status, Priority, and Power Limit.



- 3 Check the *Enable PoE* checkbox to configure the selected port to use Power over Ethernet. To disable PoE on a port, uncheck this box.
- 4 Select the *Priority* level for PoE on this port. The *Priority* level is used in cases where the controller's PoE power consumption exceeds the available power. When this happens, ports with higher *Priority* levels will be given precedence over those with a lower *Priority* level.
- 5 Set the *Power Limit* (in watts) for this port's PoE usage. Setting the *Power Limit* places a cap on the maximum amount of power which can be drawn from the selected port.



NOTE

Power limits and power budgets are based on worst case operating conditions to deliver power at the level requested. The worst case operating conditions assume the controller is operating at its maximum operating temperature and at a maximum cable length. As a result power levels may be between 5% and 10.5% over requested level.

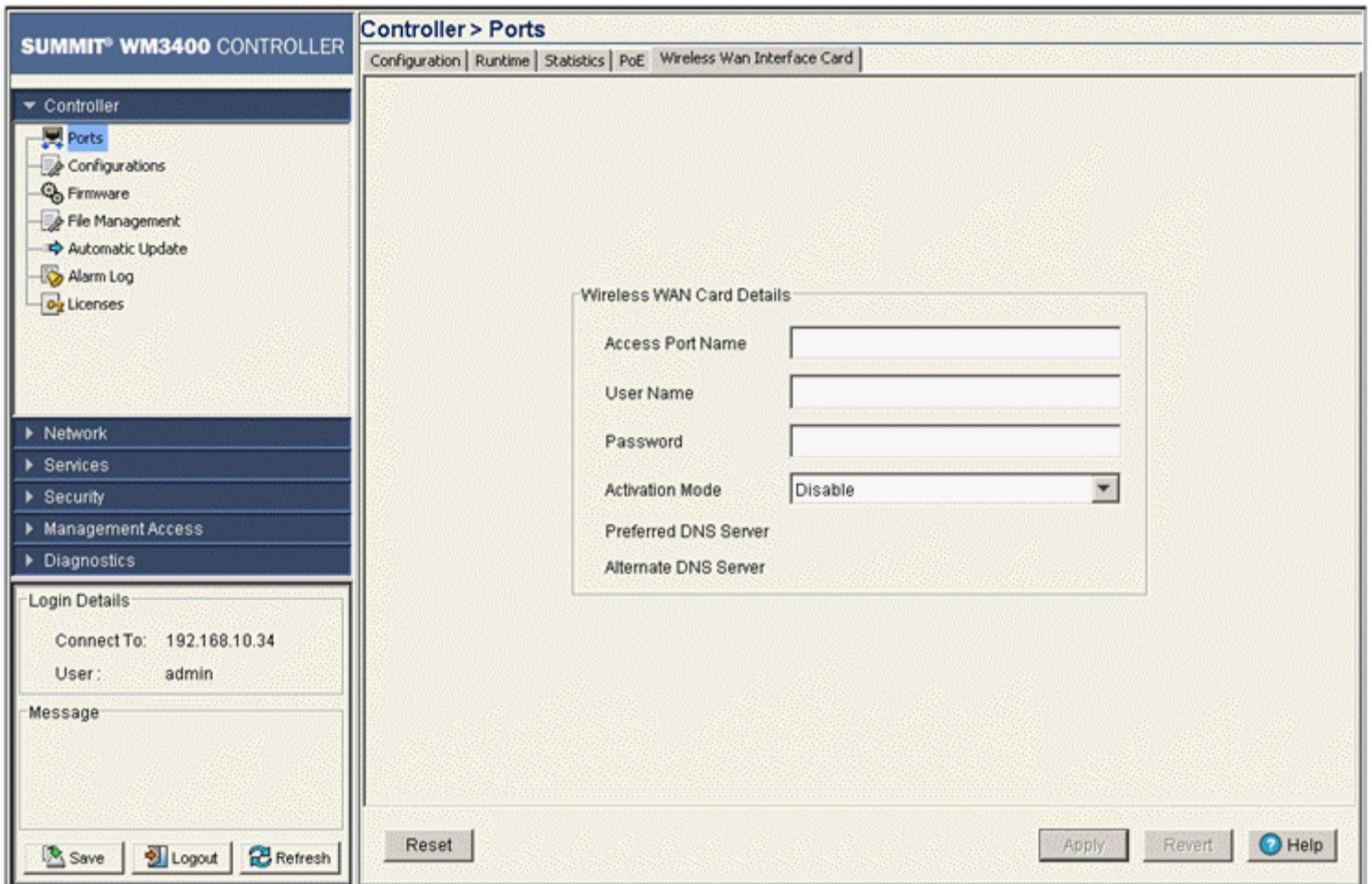
- 6 Click *OK* to save and add the changes to the running configuration and close the dialog.

Configuring WAN Interface Cards

The Summit WM3400 and Summit WM3600 controllers support 3G Wireless WAN cards using the ExpressCard slot. In order to use a 3G Wireless WAN card with the controller, it must first be initialized on a laptop. For activation and initialization information, refer to the instructions included with the card. If your Wireless WAN Interface card service provider makes use of a PIN number for access to the network, disable the PIN number before using the card with the controller.

To configure a Wireless WAN Interface card:

- 1 Select *Controller > Ports* from the main menu tree.
- 2 Select the *Wireless WAN Interface Card* tab.



3 Enter the following parameters to configure a WAN Interface Card:

- | | |
|----------------------|--|
| Access Port Name | If your Wireless WAN service provider requires you to specify an Access Port Name, enter that value here. The range is <0-25> and default value is 0. |
| User Name | Enter the <i>User Name</i> configured for use with the Wireless WAN Interface Card. The string range is <0-32> and default value is 0. |
| Password | Enter the <i>Password</i> associated with the above User Name for the Wireless WAN Interface Card. The string range is <0-30> and default value is 0. |
| Activation Mode | Select <i>Enable</i> from the pull-down menu to enable the Wireless WAN Interface Card. Select <i>Disable</i> from the pull-down menu to turn off the Wireless WAN Interface Card. |
| Preferred DNS Server | Displays the primary/preferred DNS Server provided by the Wireless WAN service provider. |
| Alternate DNS Server | Displays the secondary/alternate DNS Server provided by the Wireless WAN service provider. |

**NOTE**

To use a 3G Wireless WAN card with the controller, it must first be initialized on a laptop. For activation and initialization information, refer to the instructions included with the WAN card. If your Wireless WAN Interface card service provider makes use of a PIN number for access to the network, disable the PIN number before using the card with the controller.

- 4 To reset the WAN Interface card configuration, click the *Reset* button and the configuration fields will be cleared.

Viewing Controller Configurations

Use the *Configurations* screen to review the configuration files available to the controller. The details of each configuration can be viewed individually. Optionally, edit the file to modify its name or use the file as the controller startup configuration. A file can be deleted from the list of available configurations or transferred to a user specified location.

**NOTE**

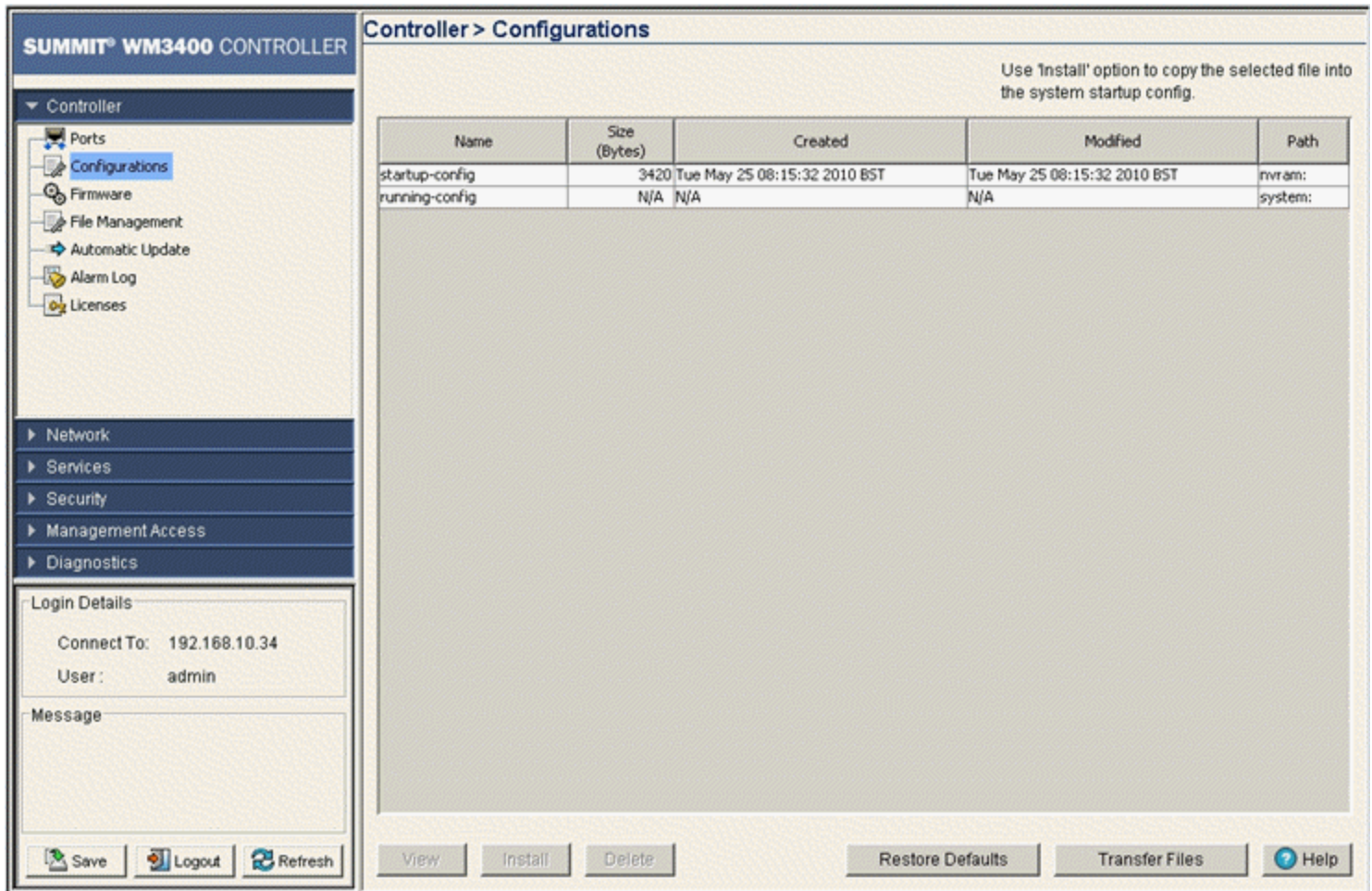
To view the entire controller configuration using SNMP, the controller CLI provides a better medium to review the entire controller configuration.

**NOTE**

The Extreme Networks Wireless Management Suite (WMS) is a recommended utility to plan the deployment of the controller and view its configuration once operational in the field. Extreme Networks WMS can help optimize the positioning and configuration of a controller (and its associated radios) in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Extreme Networks website.

To view the Configuration files available to the controller:

- 1 Select *Controller > Configurations* from the main menu tree.



The following information is displayed in tabular format. Configuration files (with the exception of startup-config and running-config) can be edited, viewed in detail, or deleted.

Name	Displays the name of each existing configuration file.
Size (Bytes)	Displays the size (in bytes) of each available configuration file.
Created	Displays the date and time each configuration file was created. Use this information as a baseline for troubleshooting problems by comparing event log data with configuration file creation data.
Modified	Displays the date and time each configuration file was last modified. Compare this column against the Created column to discern which files were modified and make informed decisions whether existing files should be further modified or deleted.
Path	Displays the path (location) to the configuration file.

- 2 To view the contents of a config file in detail, select a config file by selecting a row from the table and click the *View* button. For more information, see [“Viewing the Detailed Contents of a Config File”](#) on page 83.
- 3 Select a configuration (other than the start-up-config or running config) and click the *Install* button to install the file on the controller and replace the existing startup-config file.

If a file (for example, *sample-config*) is selected, a message displays stating, “When *sample-config* is installed, it will replace start-up config. Are you sure you want to install *sample-config*.” Click *Yes* to continue.



NOTE

Selecting either the startup-config or running-config does not enable the Edit button. A different configuration must be available to enable the Edit function for the purposes of replacing the existing startup-config.

- 4 To permanently remove a file from the list of configurations available to the controller, select a configuration file from the table and click the *Delete* button.

If startup-config is deleted, a prompt displays stating the default controller startup-config will automatically take its place. The controller running-config cannot be deleted.

- 5 To restore the system’s default configuration and revert back to factory default, click the *Restore Defaults* button.



NOTE

After setting the controller to revert to factory default settings, the system must be rebooted before the default settings take effect. When this occurs, the controller IP address may change.

- 6 Click the *Transfer Files* button to move a target configuration file to a secure location for later use. For more information, see “[Transferring a Config File](#)” on page 85.

Viewing the Detailed Contents of a Config File

The View screen displays the entire contents of a configuration file. Extreme Networks recommends a file be reviewed carefully before it is selected from the Config Files screen for edit or designation as the controller startup configuration.

- 1 Select a configuration file from the Configuration screen by highlighting the file.
- 2 Click the *View* button to see the contents of the selected configuration file.

```

!
! configuration of WM3600 Summit-WM3600 version 4.3.1.0-003D
!
!
version 1.5
!
!
aaa authentication login default local none
service prompt crash-info
!
hostname Summit-WM3600
!
network-element-id Summit-WM3600
!
username "admin" password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username "admin" privilege superuser
username "operator" password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
  name My Name
!
country-code in
redundancy interface-ip 172.16.10.2
redundancy member-ip 172.16.10.5
redundancy member-ip 172.16.10.8
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b456747c2a982
snmp-server susername Summit-WM3600

```

Page 1 of 4 Go

Status: Lines 1 to 31 of 115

Refresh Close Help

Use the up and down navigation facilities on the right-hand side of the screen to view the entire page.

- 3 The *Page* parameter displays the portion of the configuration file in the main viewing area. The total number of pages in the file are displayed to the right of the current page. The total number of lines in the file display in the *Status* field at the bottom of the screen. Scroll to corresponding pages as required to view the entire contents of the file. To navigate to a specific page, enter the page number in the text area (next to *Page* item) and click the *Go* button. The source parameter differs depending on the source selected.
- 4 Refer to the *Status* field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 5 Click *Refresh* to get the most recent updated version of the configuration file.
- 6 Click *Close* to close the dialog without committing updates to the running configuration.

Transferring a Config File

Transfer a configuration file to and from the controller using the *Transfer* screen. Transferring the controller configuration is recommended to keep viable configurations available in a secure location. The following file transfer configurations are possible:

- controller to controller, server, or local disk
- server to controller
- local disk to controller

To transfer the contents of a configuration file:

- 1 Click the *Transfer Files* button on the bottom of the Configuration screen.

The screenshot shows a window titled "Controller > Configurations > Transfer". The window is divided into two main sections: "Source" and "Target".

Source Section:

- From:** A dropdown menu with "Server" selected.
- File:** A text input field.
- Using:** A dropdown menu with "FTP" selected.
- Port:** A text input field with "21" entered.
- IP Address:** A text input field with three dots.
- User ID:** A text input field.
- Password:** A text input field.
- Path:** A text input field.

Target Section:

- To:** A dropdown menu with "Controller" selected.
- File:** A text input field.

At the bottom of the window, there is a "Status:" label and a row of buttons: "Transfer", "Abort", "Close", and "Help".

- 2 Refer to the *Source* field to define the location and address information for the source config file.

From	Select the location representing the source file's current location using the <i>From</i> drop-down menu. Options include <i>Server</i> , <i>Local Disk</i> , and <i>Controller</i> .
File	Specify a source file for the file transfer. If the controller is selected, the file used at startup automatically displays within the File parameter.
Using	Refer to the <i>Using</i> drop down-menu to configure whether the log file transfer is conducted using FTP or TFTP. FTP transfers require a valid user ID and password.
IP Address	Enter the <i>IP Address</i> of the server or system receiving the source configuration. Ensure the IP address is valid or risk jeopardizing the success of the file transfer.
User ID	Enter the <i>User ID</i> credentials required to transfer the configuration file from a FTP server.
Password	Enter the <i>Password</i> required to send the configuration file from an FTP server.
Path	Specify an appropriate <i>Path</i> name to the target directory on the local system disk or server. The Target options are different depending on the target selected.

3 Refer to the *Target* field to specify the details of the target file.

To	Use the <i>To</i> drop-down menu to define the location of the configuration file. Options include the controller (default location), external server, or local disk.
File	Use the <i>File</i> field to specify a target file for the file transfer. Use the File Browser icon to search attached files systems for target file location.

4 Refer to the *Status* field for the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.

5 Click the *Transfer* button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired configuration file to the specified location.

6 Click the *Abort* button to cancel the file transfer process before it is complete.

7 Click the *Close* button to exit the Transfer screen and return to the Config Files screen. Once a file is transferred, there is nothing else to be saved within the Transfer screen.

Viewing Controller Firmware Information

The controller can store (retain) two software versions (primary and secondary). Information supporting the two versions displays within the *Firmware* screen. The *Version* column displays the version string. The *Build Time* is the date and time each version was generated. *Install* represents the date and time the upgrade was performed. *Next Boot* indicates which version should be used on the next reboot. The Next Boot version should match the *Running Version*, unless the system has failed over to another version.

SUMMIT® WM3400 CONTROLLER Controller > Firmware

Image Failover is **enabled**.
Use 'Global Settings' to disable it.

[Show Filtering Options](#)

Image	Version	Current Boot	Next Boot	Built Time	Install Time
Primary	4.2.1.0-006B	✘	✘	Wed Feb 03 22:06:24 2010 ...	Fri Feb 05 01:13:09 2010 GMT
Secondary	4.2.1.0-006R	✔	✔	Tue Feb 16 20:35:20 2010 ...	Tue May 04 06:53:34 2010 ...

Filtering is disabled

Patch

Patch Name	Version

To view the firmware files available to the controller:

- 1 Select *Controller > Firmware* from the main menu tree.
- 2 Refer to the following information displayed within the Firmware screen:

Image	Displays whether a firmware image is the primary image or a secondary image. The primary image is typically the image loaded when the controller boots.
Version	Displays a unique alphanumeric version for each firmware file listed.
Current Boot	A check mark within this column designates this version as the version used by the controller the last time it was booted. An "X" in this column means this version was not used the last time the controller was booted.
Next Boot	A check mark within this column designates this version as the version to be used the next time the controller is booted. An "X" in this column means this version will not be used the next time the controller is booted. To change the boot designation, highlight an image and click the <i>Edit</i> button.
Built Time	Displays the time the version was created (built). Do not confuse the Built Time with the time the firmware was last loaded on the controller.
Install Time	The Install Time is the time this version was loaded with on the controller. Periodically review this information to assess the relevance of older files.

- 3 Refer to the *Patch* field for a listing of the patches available to the controller. The name and version of each patch file is displayed. Each patch file has an associated .txt file designation. The text file describes nuances associated with the file that may make it optimal for use with the controller.
- 4 Select an existing firmware version and click the *Edit* button to change the firmware version used when the controller is booted next. For more information, see [“Editing the Controller Firmware” on page 88](#).
- 5 Click the *Global Settings* button to specify a firmware version for use with the failover image. For more information, see [“Enabling Global Settings for the Image Failover” on page 89](#).
- 6 Click the *Update Firmware* button to update the firmware file loaded onto the controller. For more information, see [“Updating the Controller Firmware” on page 89](#).

**NOTE**

To apply a patch to the controller, follow the same instructions for updating the controller’s firmware.

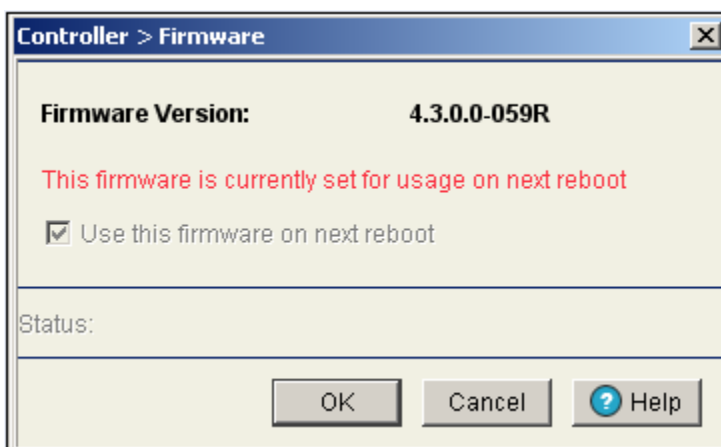
- 7 To remove a patch, select it from among those displayed within the Patch field and click the *Remove Patch* button.

Editing the Controller Firmware

The Edit screen enables the user to select a firmware file and designate it as the version used the next time the controller is booted.

- 1 Select the primary firmware image from the Firmware screen.
- 2 Click the *Edit* button.

The *Firmware* screen displays the current firmware version and whether this version is used for the next reboot.



- 3 Select the checkbox to use this version on the next boot of the controller.
- 4 To edit the secondary image, select the secondary image, click the *Edit* button, and select the *Use this firmware on next reboot* checkbox.

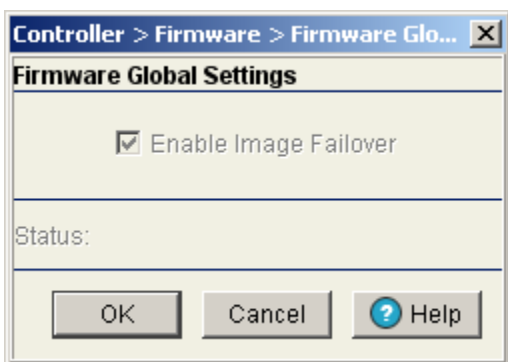
This firmware version will now be invoked after the next reboot of the controller.

- 5 Refer to the *Status* field for the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click the OK button to commit the changes made and exit the screen.

Enabling Global Settings for the Image Failover

Use the *Global Settings* screen to specify a firmware version for use with the failover image.

- 1 Select an image from the table in the Firmware screen.
- 2 Click the *Global Settings* button.



- 3 Select the *Enable Image Failover* checkbox to load an alternative firmware version if the WLAN module fails to load the selected version successfully after 2 reboot attempts.
- 4 Refer to the *Status* field for the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 5 Click OK to save and add the changes to the running configuration and close the dialog.

Updating the Controller Firmware

Use the *Update* screen to update the firmware version currently used by the controller.



NOTE

When performing a firmware update using the controller CLI, use the following syntax (specific to FTP) <ftp://username:password@ipaddress:port/path/filename>. If using TFTP, use <tftp://ipaddress/path/filename>.



NOTE

When performing a firmware update using FTP, be sure that TCP port 21 is open between the controller and the FTP server where the firmware file is located.

- 1 Select an image from the table in the Firmware screen.
- 2 Click the *Update Firmware* button.

- 3 Use the *From* drop-down menu to specify the location from which the file is sent.
- 4 Enter the name of the file containing the firmware update in the *File* text field.
This is the file that will append the file currently in use.
- 5 From the *Using* drop down menu, select either FTP or TFTP as a medium to update the firmware.
 - a Use *FTP* to get the firmware update from a *File Transfer Protocol* (FTP) server. A user account must be established on the FTP server specified for the firmware update.
 - b Use *TFTP* to get the firmware update from a *Trivial File Transfer Protocol* (TFTP) server. When using CF, USB1 or USB2 as the transfer method, this field will not be available.
 - c Use *HTTP* to get the firmware update from a *Hyper Text Transfer Protocol* (HTTP) server.
 - d Use *SFTP* to get the firmware update from a *Secure File Transfer Protocol* (SFTP) server. A user account must be established on the SFTP server specified for the firmware update.

**NOTE**

On the Summit WM3700, users can also transfer firmware files using USB or Compact Flash. On the Summit WM3600, users can also transfer firmware files using USB. On the Summit WM3400, users can also transfer firmware files using USB or PCI Express card.

- 6 Enter the IP address for the FTP or TFTP server in the *IP address* field.
- 7 Enter the username for FTP server login in the *User ID* field.
- 8 Enter the password for FTP server login in the *Password* field.
- 9 Enter the complete file path for the file that contains the firmware update in the *Path* field.
- 10 Click the *Do Update* button to initiate the update.
A warning prompt displays. Upon confirming the firmware update, the controller reboots and completes the firmware update.

**CAUTION**

When restarting or rebooting the controller, the RADIUS server is restarted regardless of its state before the reboot.

-
- 11 Click *OK* to add the changes to the running configuration and close the dialog.
 - 12 Refer to the *Status* field for the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
 - 13 Click *Cancel* to close the dialog without committing updates to the running configuration.

Controller File Management

Use the *File Management* screen to transfer configuration file to and from the controller and review the files available.

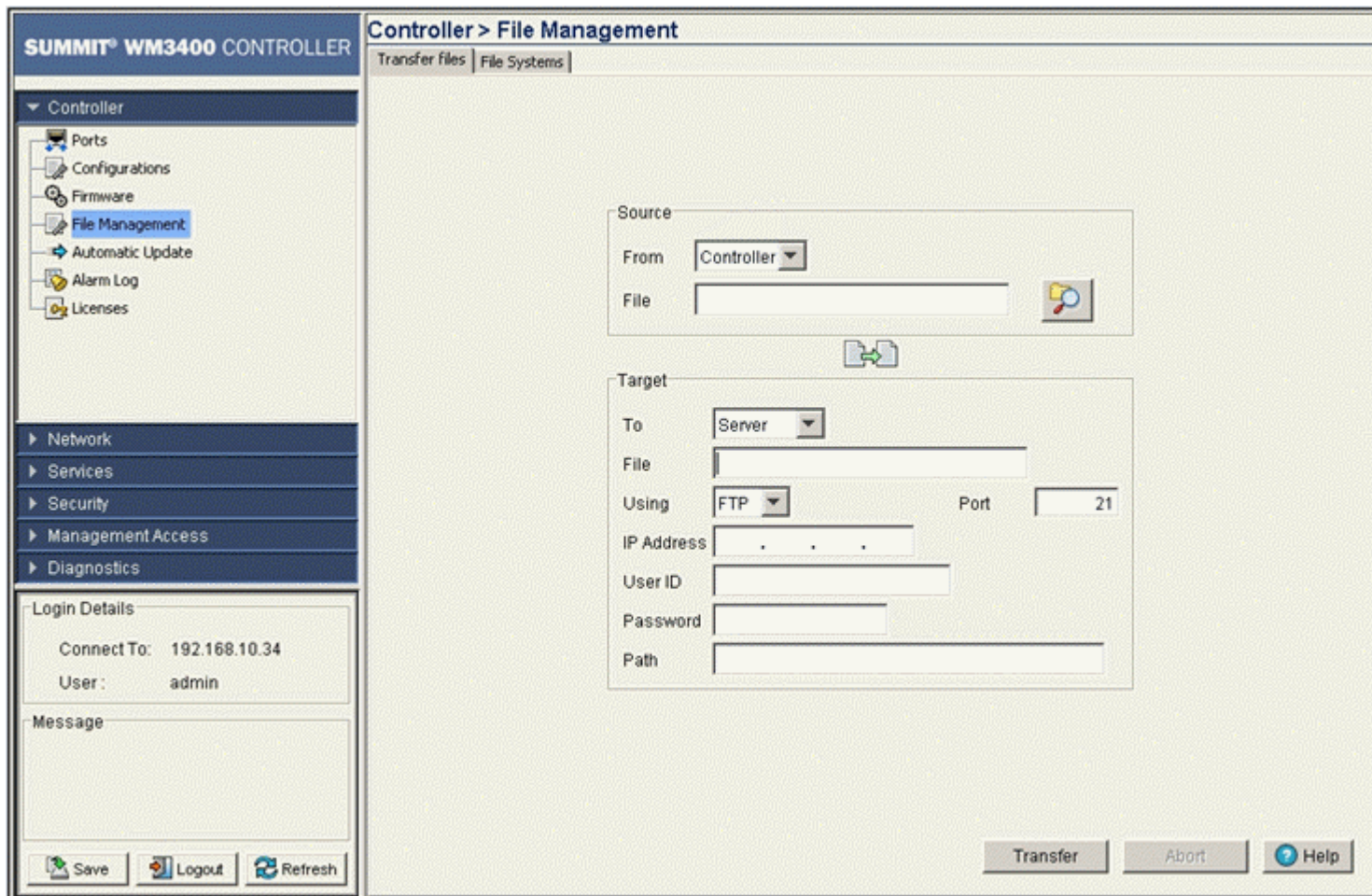
Transferring Files

Use the *Transfer Files* screen to transfer files to and from the controller. Transferring files is recommended to keep files in a secure location. The following file transfer options are available:

- Wireless Controller to Wireless Controller
- Wireless Controller to Server
- Server to Wireless Controller

To define the properties of the file transfer configuration:

- 1 Select *Controller > File Management* from the main menu tree.



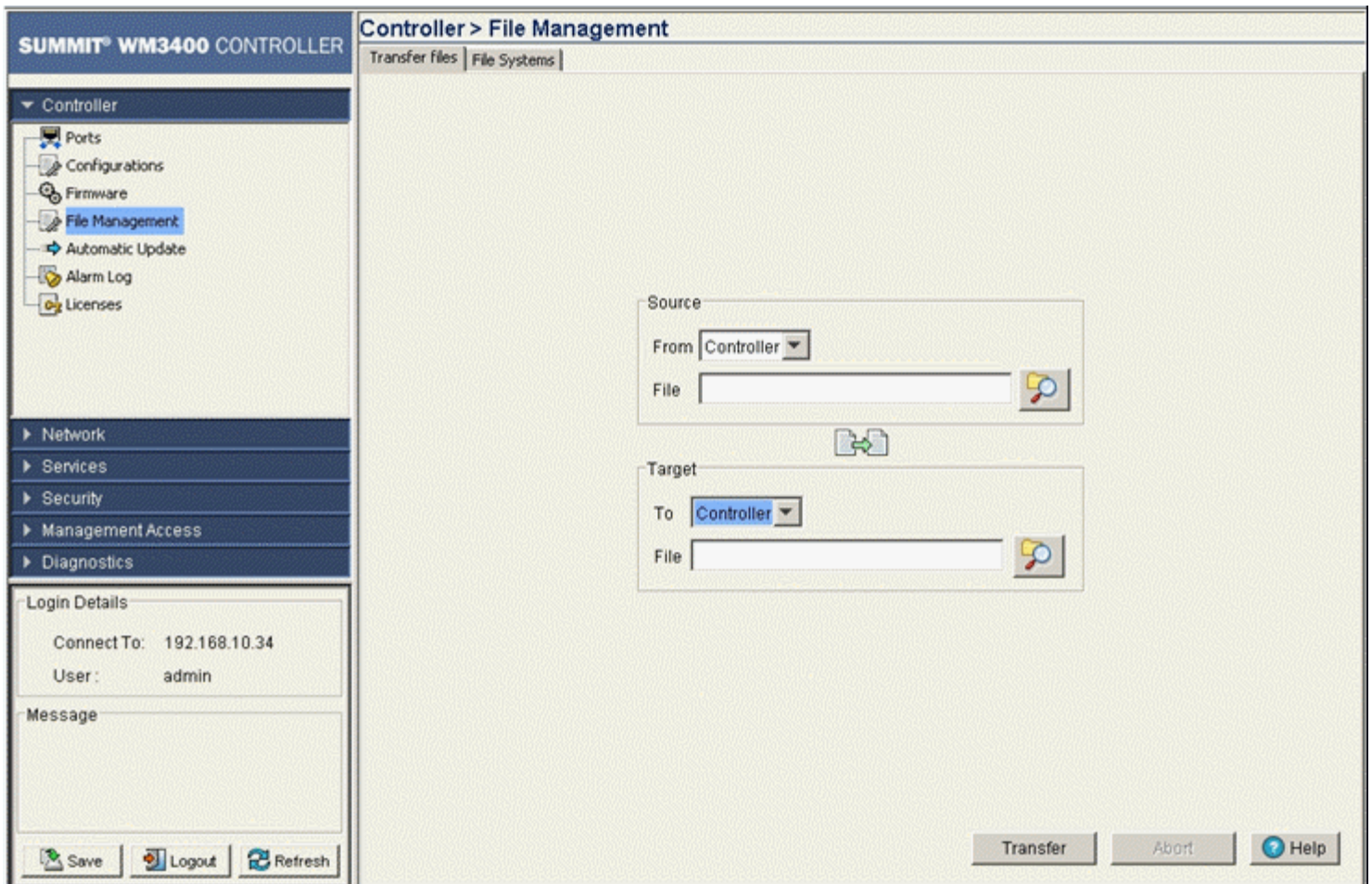
- 2 Refer to the *Source* field to specify the details of the source file.

From	Use the <i>From</i> drop-down menu to select the source file's current location. The options include Wireless Controller and Server. The following transfer options are possible: <ul style="list-style-type: none"> • Wireless Controller to Wireless Controller • Wireless Controller to Server • Server to Wireless Controller. <p>The parameters displayed in the <i>Source</i> and <i>Target</i> fields differ based on the above selection. These different kinds of file transfer techniques are described in the sections that follow.</p>
File	Use the <i>Browse</i> button to navigate to a target file for transfer. If the controller is selected from the From drop-down menu (within the <i>Source</i> field), the file used at startup automatically displays.

Transferring a file from Wireless Controller to Wireless Controller

To transfer a file from one controller to another:

- 1 Select *Controller* from the *From* drop-down menu



- 2 Use the *Browse* button to locate a target file for the file transfer.
- 3 Use the *To* drop-down menu (within the *Target* field) and select *Controller*. This defines the location of the file.
- 4 Use the *Browse* button to define a location for the transferred file.
- 5 Click the *Transfer* button to complete the file transfer.
- 6 The *Message* section in the main menu area displays the file transfer message.
- 7 Click *Abort* at any time during the transfer process to abort the file transfer.

Transferring a File from a Wireless Controller to a Server

To transfer a file from the Controller to a Server:

- 1 Refer to the *Source* field to specify the source file. Use the *From* drop-down menu and select *Controller*.

- 2 Use the *Browse* button and select a file for transfer.
- 3 Use the *To* drop-down menu (within the Target field) and select *Server*. This defines the transfer location of the configuration file. Enter the file location marked to store the transferred file.
- 4 Use the *Using* drop down-menu to configure whether the log file transfer is conducted using FTP, TFTP, HTTP, or SFTP. This field displays the default port for FTP, TFTP, HTTP, or SFTP. The value in this field can be configured as required. Enter the IP Address of the server receiving the source configuration. Ensure the IP address is valid or risk jeopardizing the success of the file transfer. Enter the User ID credentials required to transfer the configuration file from an FTP server.



NOTE

On the Summit WM3700, users can also transfer files using USB or Compact Flash. On the Summit WM3600, users can also transfer files using USB. On the Summit WM3400, users can also transfer the files using USB, or PCI Express.

- 5 Enter the *Password* required to send the configuration file from an FTP server.

- 6 Specify the appropriate *Path* name to the target directory on the server. The target options are different depending on the target selected.
- 7 Click the *Transfer* button to complete the file transfer. The *Message* section in the main menu area displays the file transfer message.
- 8 Click *Abort* at any time during the transfer process to abort the file transfer.

Transferring a File from a Server to a Wireless Controller

To transfer a file from a Server to the controller:

- 1 Refer to the *Source* field to specify the details of the source file. Use the *From* drop-down menu and select *Server*.

The screenshot shows the Summit WM3400 Controller's File Management interface. The main window is titled "Controller > File Management" and has two tabs: "Transfer files" (selected) and "File Systems". On the left, a navigation tree shows "Controller" expanded with sub-items: Ports, Configurations, Firmware, File Management (highlighted), Automatic Update, Alarm Log, and Licenses. Below this are sections for Network, Services, Security, Management Access, and Diagnostics. A "Login Details" section shows "Connect To: 192.168.10.34" and "User: admin". A "Message" section is empty. At the bottom left are "Save", "Logout", and "Refresh" buttons. The main content area contains a "Source" section with a "From" dropdown set to "Server", a "File" text box, a "Using" dropdown set to "FTP", a "Port" text box with "21", an "IP Address" text box with three dots, "User ID" and "Password" text boxes, and a "Path" text box. A double-headed arrow icon is below the Source section. The "Target" section has a "To" dropdown set to "Controller" and a "File" text box with a magnifying glass icon. At the bottom right are "Transfer", "Abort", and "Help" buttons.

- 2 Provide the name of the *File*.
- 3 Use the *Using* drop-down menu to configure whether the file transfer is conducted using FTP, TFTP, HTTP, or SFTP.
FTP transfers require a valid user ID and password.
- 4 Enter an *IP Address* of the server receiving the configuration file. Ensure that the IP address is valid or risk jeopardizing the success of the file transfer.
- 5 Enter the *User ID* credentials required to transfer the configuration file from an FTP server.
- 6 Enter the *Password* required to send the configuration file from an FTP server.

- 7 Specify the appropriate *Path* name to the target directory on the server. The *Target* options are different depending on the target selected.
- 8 Use the *To* drop-down menu (within the Target field) and select *Controller*.
- 9 Use the *Browse* button to browse and select the location to store the file marked for transfer.
- 10 Click the *Transfer* button to complete the file transfer. The *Message* section displays the status of the file transfer message.
- 11 Click the *Abort* button any time during the transfer process to abort the file transfer.

Viewing Files

Use the *File System* tab to review the files available to the controller. The controller maintains the following file types:

- flash
- nvram
- system
- Compact Flash
- USB 1
- USB 2



NOTE

USB 1 is available on the Summit WM3400, Summit WM3600 and Summit WM3700 controllers. USB2 and Compact Flash are only available on the Summit WM3700 controller.

Transfer files between the controller and the server from any one of the above mentioned locations. Since compact flash (CF) and USB are external memory locations, the File System window displays the status of these devices. Transfer files to compact flash and USB only if they are connected and available.

To view the file systems currently available to the controller:

- 1 Select *Controller > File Management* from the main menu tree.
- 2 Select the *File System* tab.

The screenshot shows the 'Controller > File Management' interface. On the left is a navigation tree with 'File Management' selected. Below it are sections for 'Login Details' (Connect To: 192.168.10.34, User: admin) and a 'Message' field. At the bottom are 'Save', 'Logout', and 'Refresh' buttons. The main area displays a table with two tabs: 'Transfer files' and 'File Systems'. The 'File Systems' tab is active, showing a table with columns 'Name', 'Available', and 'Formatted'.

Name	Available	Formatted
flash	✓	✗
nvrnm	✓	✗
system	✓	✗
usb1	✗	✗
usb2	✗	✗

3 Refer to the following *File Systems* information.

Name	Displays the memory locations available to the controller.
Available	<p>Displays the current status of the memory resource. By default, nvrnm and system are always available.</p> <p>A green check indicates the device is currently connected to the controller and is available.</p> <p>A red X indicates the device is currently not available.</p>
Formatted	<p>Displays the format status of the memory devices. This ensures that the external and internal memory devices store the files securely. A formatted memory device is less prone to crash and loss of data.</p> <p>A green check mark indicates that the device is currently connected to the controller and is available.</p> <p>A red X indicates that the device is currently not available.</p>

Configuring Automatic Updates

Use the *Automatic Updates* screen to enable a facility that will poll a server address (you designate) when the controller is booted. If updates are found since the last time the controller was booted, the updated version is uploaded to the controller the next time the controller is booted. Enable this option for either the firmware, configuration file, or cluster configuration file. Extreme Networks recommends leaving this setting disabled if a review of a new file is required before it is automatically uploaded by the controller.

To enable and configure the automatic update feature for controller firmware, configuration files, and cluster configurations:

- 1 Select *Controller > Automatic Updates* from the main menu tree.

The screenshot displays the 'Controller > Automatic Update' configuration page on the Summit WM3400 Controller. The interface is organized into three main configuration sections, each with an 'Enable' checkbox and associated fields:

- Controller Configuration:** Includes an 'Enable' checkbox, an IP Address field (0.0.0.0), a Protocol dropdown menu (FLASH), User ID, Password, and File Name (With Path) fields.
- Redundancy Configuration:** Includes an 'Enable' checkbox, an IP Address field (0.0.0.0), a Protocol dropdown menu (FLASH), User ID, Password, and File Name (With Path) fields.
- Firmware:** Includes an 'Enable' checkbox, an IP Address field (0.0.0.0), a Protocol dropdown menu (Unset), User ID, Password, File Name (With Path), and Version fields.

At the bottom right of the page, there are four buttons: 'Start Update', 'Apply', 'Revert', and 'Help'. The left sidebar shows the navigation menu with 'Automatic Update' selected under the 'Controller' section.

- 2 Refer to the *Controller Configuration* field to enable and define the configuration for automatic configuration file updates. If enabled, the located (updated) configuration file will be used with the controller the next time the controller boots.

Enable

Select the *Enable* checkbox to allow an automatic configuration file update when a newer (updated) file is detected (upon the boot of the controller) at the specified IP address.

IP Address	Define the <i>IP address</i> of the server where the configuration files reside. If a new version is detected when the controller is booted, it is uploaded to the controller and used upon the next boot of the controller.
User ID	Enter the <i>User ID</i> required to access the FTP or TFTP server.
File Name (With Path)	Provide the complete and accurate path to the location of the configuration files on the server. This path must be accurate to ensure that the most recent file is retrieved.
Protocol	Use the <i>Protocol</i> drop-down menu to specify the <i>FTP</i> , <i>TFTP</i> , <i>HTTP</i> , <i>SFTP</i> , or resident controller <i>FLASH</i> medium used for the file update from the server. FLASH is the default setting.
Password	Enter the password required to access the server.



NOTE

In addition to the Protocols listed on the Summit WM3700, users can also auto-update using USB or Compact Flash. On the Summit WM3400 and Summit WM3600, users can also auto-update using USB.

3 Refer to the *Redundancy Configuration* field to enable and define the configuration for automatic cluster file updates.

Enable	Select the <i>Enable</i> checkbox to allow an automatic cluster file update when a new (updated) file is detected (upon the boot of the controller) at the specified IP address.
IP Address	Define the <i>IP address</i> of the server where the cluster files reside. If a new version is detected when the controller is booted, it will be uploaded to the controller and used upon the next boot of the controller.
User ID	Enter the <i>User ID</i> required to access the FTP or TFTP server.
File Name (With Path)	Provide the complete and accurate path to the location of the cluster files on the server. This path must be accurate to ensure that the most recent file is retrieved.
Protocol	Use the <i>Protocol</i> drop-down menu to specify the <i>FTP</i> , <i>TFTP</i> , <i>HTTP</i> , <i>SFTP</i> , or resident controller <i>FLASH</i> medium used for the file update from the server. FLASH is the default setting.
Password	Enter the password required to access the server.

4 Refer to the *Firmware* field to enable and define the configuration for automatic firmware updates. If enabled, the located (updated) controller firmware is used with the controller the next time the controller boots.

Enable	Select the <i>Enable</i> checkbox to allow an automatic firmware update when a new (updated) version is detected (upon the boot of the controller) at the specified IP address.
IP Address	Define the <i>IP address</i> of the server where the firmware files reside. If a new version is detected when the controller is booted, it will be uploaded to the controller and used upon the next boot of the controller.
User ID	Enter the <i>User ID</i> required to access the FTP or TFTP server.
File Name (With Path)	Provide the complete and accurate path to the location of the firmware files on the server. This path must be accurate to ensure that the file is retrieved.
Protocol	Use the <i>Protocol</i> drop-down menu to specify the <i>FTP</i> , <i>TFTP</i> , <i>HTTP</i> , <i>SFTP</i> , or resident controller <i>FLASH</i> medium used for the file update from the server. FLASH is the default setting.
Password	Enter the password required to access the server.

Version Provide the target firmware version to ensure that the controller is upgrading to the intended baseline.

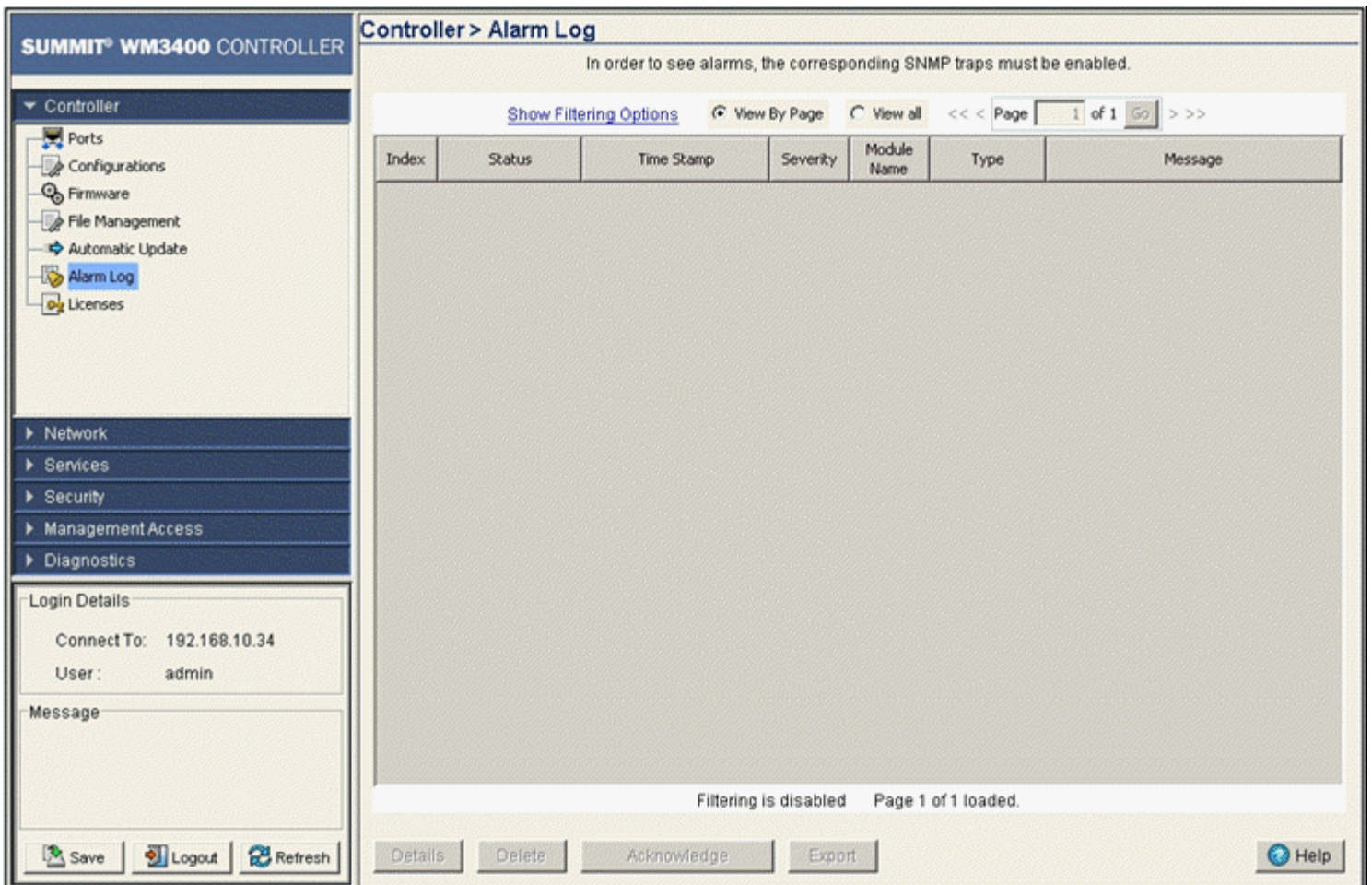
- 5 Select the *Start Update* button to begin the file updates for the enabled controller configuration, cluster configuration, or firmware facilities.
- 6 Click the *Apply* button to save the changes to the configuration.
- 7 Click the *Revert* button to revert back to the last saved configuration.

Viewing the Controller Alarm Log

Use the *Alarm Log* screen as an initial snapshot for alarm log information. Expand alarms (as needed) for greater detail, delete alarms, acknowledge alarms, or export alarm data to a user-specified location for archive and network performance analysis.

To view controller alarm log information:

- 1 Select *Controller > Alarm Log* from the main menu tree.



- 2 Use the Alarm Log screen's filtering options to view alarm log data by page or by its entire content.

3 Select either of the two available options to view alarm log information:

View By Page	Select the <i>View By Page</i> radio button to view alarm log information on a per page basis. Use the <i>View By Page</i> option to page through alarm logs. If there are a large number of alarms, the user can navigate to the page that has been completely loaded. All operations can be performed on the currently loaded data. Enter a page number next to "Page" and click the <i>Go</i> button to move to the specific page.
View All	Select the <i>View All</i> radio button to display the complete alarm log within the table. If there are a large number of alarms, the <i>View All</i> option will take several minutes to load.

4 Refer to the table within the *Alarm Log* screen for the following information:

Index	Displays the unique numerical identifier for trap events (alarms) generated in the system. Use the index to help differentiate an alarm from others with similar attributes.
Status	Displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The <i>Status</i> displays error messages if something goes wrong in the transaction between the applet and the controller.
Time Stamp	Displays the date, year, and time the alarm was raised (as well as the time zone of the system). The time stamp only states the time the alarm was generated, not the time it was acknowledged.
Severity	Displays the severity level of the event. Use this (non numerical and verbal) description to assess the criticality of the alarms. Severity levels include: <ul style="list-style-type: none">• Critical• Major• Warning• Informational Normal
Module Name	Displays the module name that triggered this alarm. Use this information to assess if this alarm is a recurring problem or if it is an isolated incident.
Type	Displays the alarm type.
Message	Displays a detailed event message corresponding to the alarm event. It contains an event-specific message for information about the alarm. Use this value along with the <i>Details</i> description for optimal problem event identification.

5 Select an alarm and click the *Details* button to display an alarm description along with a system proposed solution and possible causes. For more information, see ["Viewing Alarm Log Details" on page 102](#).

6 Select the alarm(s) from those listed and click the *Delete* button to remove them from the list of alarms.

This is not recommended in instances where the problem is unacknowledged and the criticality has not yet been assessed.

7 Select the unacknowledged alarm(s) from those listed and click the *Acknowledge* button to acknowledge them.

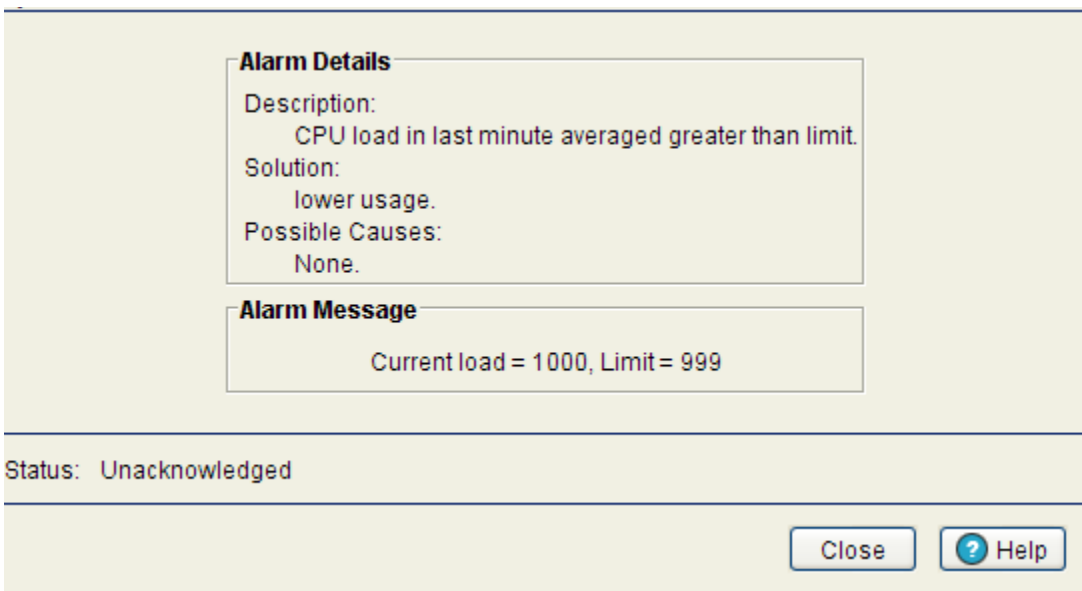
8 Click the *Export* button to export the content of the table to a *Comma Separated Values* file (CSV).

Viewing Alarm Log Details

Use the *Details* option when additional information is required for a specific alarm to make an informed decision on whether to delete, acknowledge, or export the alarm.

To review controller alarm details:

- 1 Select *Controller > Alarm Log* from the main menu tree.
- 2 Select an alarm and click the *Details* button



- 3 Refer to the *Alarm Details* and *Alarm Message* for the following information:

Description	Displays the details of the alarm log event. This information can be used in conjunction with the <i>Solution</i> and <i>Possible Causes</i> items to troubleshoot the event and determine how the event can be avoided in future.
Solution	Displays a possible solution to the alarm event. The solution should be attempted first to rectify the described problem.
Possible Causes	Describes the probable causes that could have raised this specific alarm. Determine whether the causes listed can be remedied to avoid this alarm from being raised in future.
Alarm Message	Displays the radio (and MAC address if relevant) reporting the alarm detail information.

- 4 Click *Close* to exit the dialog.

Viewing Controller Licenses

Use the *Licenses* screen to install and add a new controller license.



NOTE

- By default the following licenses are automatically activated on Summit WM3400 controllers:
- 6 AP licenses, which will work for Access Ports or Adaptive APs
 - Advanced Security License
 - Locating Application License
 - WAN Backhaul License

To install a new license:

- 1 Select *Controller > Licenses* from the main menu tree.

Controller > Licenses

Install License

License Key

Serial Number 1007C-40002

Feature Licenses

Feature Name	License Count	License Usage	License Key
ADSEC	activated	activated	84f41716 74c6c66e 596c2988 1054a4ee bb76f...
AP	6	1	c750cf96 26e065a0 1f49f1ec 9b51fb99 8a1ae2...
LOCATION	activated	activated	8247c31a ad86d238 459faafc 1be76393 ceac5...
WIRELESS_WAN	activated	activated	384688d6 42a6932c 1329c8bc 518f5dde 6e0f0...

Save Logout Refresh Help

- 2 Refer to the *Install License* field for the following information:

- License Key Enter the license key required to install a particular feature. The license key is returned when you supply the controller serial number to Extreme Networks support.
- Serial Number Displays the serial number of the controller used for generating the license key.

- 3 Click the *Install* button to install the selected license.

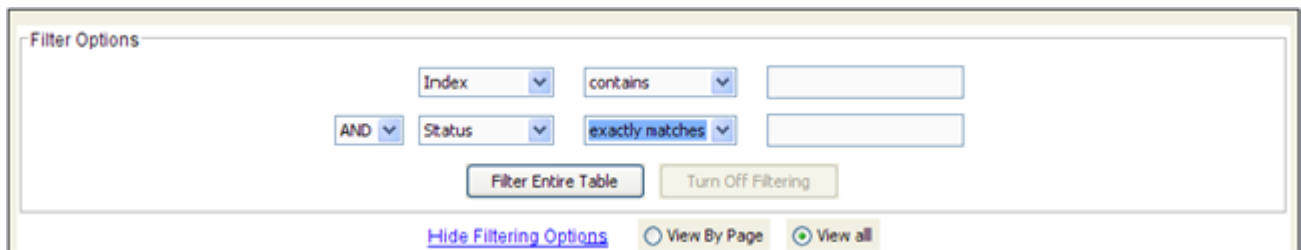
4 Refer to the *Feature Licenses* table for the following license specific information:

Feature Name	<p>Displays the name of the feature either installed or upgraded on the controller.</p> <p>Available feature licenses on the controller are:</p> <ul style="list-style-type: none"> • Access Point Licenses—AP: This enables you to adopt a specified number of Access Ports/Points to the controller. The available number of Access Point licences varies by controller platform. • Advanced Security License—ADSEC: This enables the Role Based Firewall feature and increases the number of IPSec VPN tunnels. The number of IPSec tunnels varies by controller platform. • Location Application License—LOC-APP: This enables the controller's integrated RTLS engine which allows for locationing of wireless clients and Wi-Fi tags. It also enables RFID support, and reader management and Gen2 tag support. In addition this, license enables Application Level Event support for sending location updates to 3rd-party applications. • 3G License: This enables the use of the controller's 3G support in addition to the controller's WAN. 3G license support is either enabled or disabled.
License Count	Displays the number of licenses applied while entering the license key.
License Usage	Lists the number of license in use. Determine whether this number adequately represents the number of controllers needed to deploy.
License Key	The license key for the feature installed/upgraded.

How to use the Filter Option

Use the Filter Option to sort the display details of screen that employ the filtering option as a means of sorting how data is displayed within the screen.

- 1 Click the *Show Filtering Option* to expand the Filter Option zone, whenever it appears in any screen.



- 2 Enter the filter criteria as per the options provided in the Filter Option zone.
The parameters in the Filter Option field are populated with the parameters of the screen in which it appears. Not all controller Web UIs contain the filtering option.
- 3 Click the *Filter Entire Table* button to filter the entire table in which the filter zone appears.
The result of the filtering operation displays at the bottom of the table.
- 4 Click the *Turn Off Filtering* button to disable the filtering option for the screen where it appears.
Filtering status (when filtering is turned off) displays at the bottom of the table.
- 5 Click the *Hide Filtering Option* button to hide the Filter Option zone.

5

CHAPTER

Network Setup

This chapter describes the Network Setup menu information used to configure the controller. This chapter consists of the following controller network configuration activities:

- [Displaying the Network Interface on page 105](#)
- [Viewing Network IP Information on page 107](#)
- [Viewing and Configuring Layer 2 Virtual LANs on page 114](#)
- [Configuring Controller Virtual Interfaces on page 120](#)
- [Viewing and Configuring Controller WLANs on page 129](#)
- [Viewing Associated MU Details on page 190](#)
- [Viewing Access Port/Point Information on page 203](#)
- [Viewing Access Point Adoption Defaults on page 249](#)
- [Viewing Adopted Access Ports/Points on page 262](#)
- [Configuring Access Ports/Points on page 262](#)
- [Multiple Spanning Tree on page 280](#)
- [IGMP Snooping on page 293](#)
- [Wired Hotspot on page 297](#)



NOTE

HTTPS must be enabled to access the controller applet. Ensure HTTPS access has been enabled before using the login screen to access the controller applet.

Displaying the Network Interface

The main *Network* interface displays a high-level overview of the configuration (default or otherwise) as defined within the Network main menu. Use the information to determine if items require additional configuration using the sub-menu items under the main Network menu item.



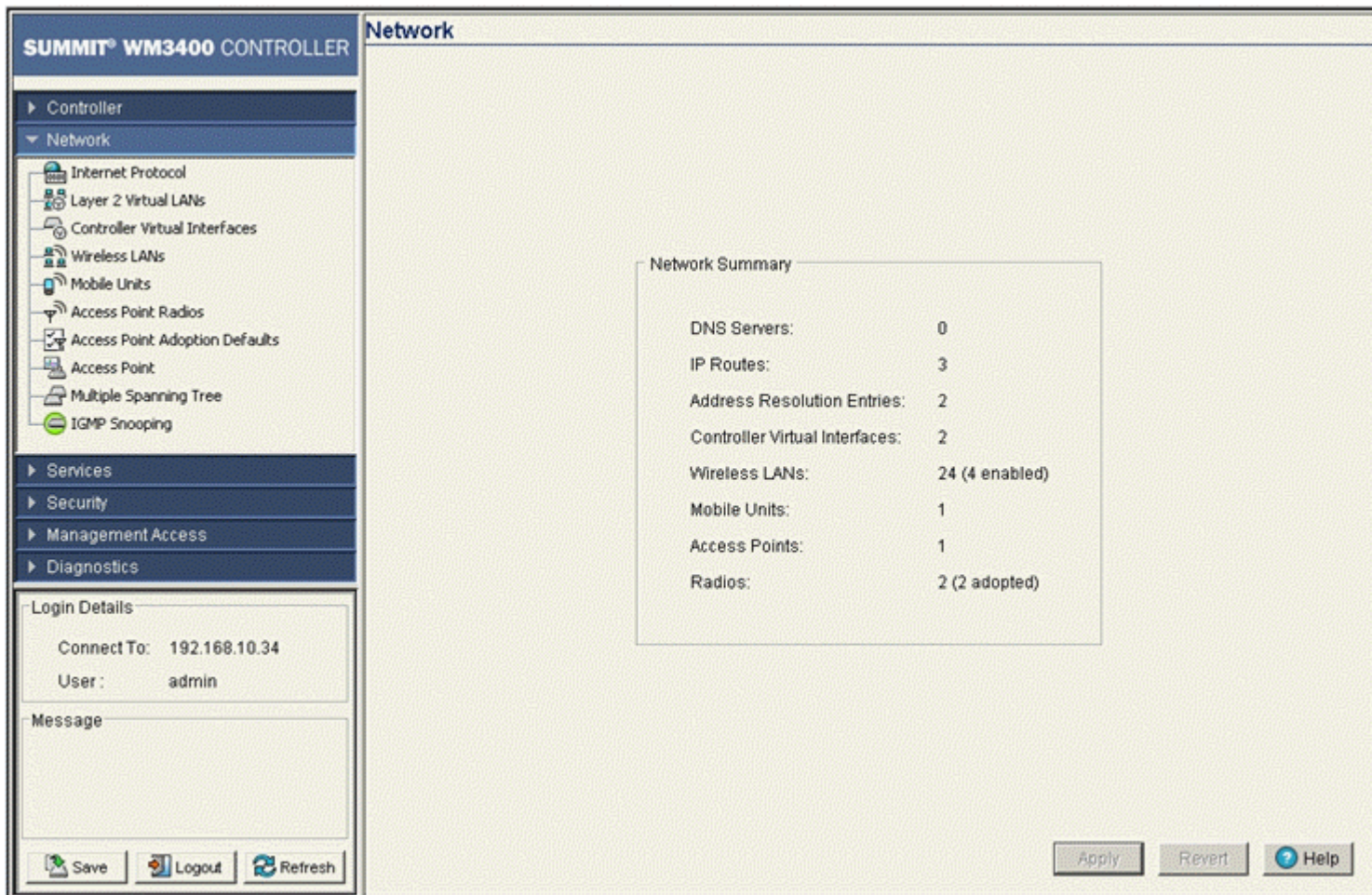
NOTE

When the controller's configuration is successfully updated (using the Web UI), the affected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the affected screen's Status field and the screen remains displayed. In the case of file transfer operations, the

transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To view the controller’s Network configuration:

- 1 Select *Network* from the main menu tree.



- 2 Refer to the following information to discern if configuration changes are warranted:

DNS Servers	Displays the number of DNS Servers configured thus far for use with the controller. For more information, see “Viewing Network IP Information” on page 107.
IP Routes	Displays the number of IP routes for routing packets to a defined destination. For information on defining IP Routes, see “Configuring IP Forwarding” on page 110.
Additional Resolution Entries	Displays the number of layer three (IP) address to layer two (MAC) address mappings. For more information, see “Viewing Address Resolution” on page 113.
Controller Virtual Interfaces	Displays the number of virtual interfaces (VLANs) defined thus far for the controller. New VLANs can be defined or existing VLANs can be modified as needed. For more information, see “Configuring Controller Virtual Interfaces” on page 120.

Wireless LANs	Displays the number of WLANs currently defined on the controller. The controller has 32 default WLANs. New WLANs can be added as needed, and their descriptions, VLAN assignments, and security schemes modified. For more information, see “Viewing and Configuring Controller WLANs” on page 129 .
Mobile Units	Displays the number of MUs currently associated to (and interacting with) the controller. The details of individual MUs can be displayed as needed. For more information, see “Viewing Associated MU Details” on page 190 .
Access Ports	Displays the number of <i>Access Ports/Points</i> (APs) active on the controller. Access Ports/Points can be added or existing APs can have their VLAN assignments changed, their descriptions modified, and their current authentication and encryption schemes modified. For more information, see “Viewing Access Port/Point Information” on page 203 .
Radios	Displays the number of AP radios detected over the controller managed network. Displayed with this information is the number of radios detected that have been adopted by the controller. For more information, see “Configuring Access Port/Point Radios” on page 204 .

The *Apply* and *Cancel* buttons are grayed out within this screen, as there is no data to be configured or saved.

Viewing Network IP Information

Use the *Internet Protocol* screen to view and configure network-associated IP details. The *Internet Protocol* screen contains tabs supporting the following configuration activities:

- [Configuring DNS on page 107](#)
- [Configuring IP Forwarding on page 110](#)
- [Viewing Address Resolution on page 113](#)

Configuring DNS

Use the *Domain Name System* tab to view Server address information and delete or add servers to the list of servers available. To configure DNS:

- 1 Select *Network > Internet Protocol* from the main tree menu.
- 2 Select the *Domain Network System* tab (displayed by default).

Use the *Show Filtering Options* link to view the details displayed in the table.

The screenshot displays the configuration page for the Domain Name System on a Summit WM3600 Controller. The interface includes a navigation menu on the left with categories like Controller, Network, Services, Security, Management Access, and Diagnostics. The main content area shows the 'Domain Name System' configuration, which is currently disabled. A table lists the configured DNS servers:

Server IP Address	Server Type
10.255.181.87	Static
10.0.4.72	Static

Below the table, it indicates 'Filtering is disabled'. At the bottom of the configuration area, there are buttons for 'Delete', 'Add', 'Global Settings', and 'Help'. The left sidebar also shows 'Login Details' with 'Connect To: 10.255.108.36' and 'User: admin', and a 'Message' field.

3 The *Domain Name System* tab displays DNS details in a tabular format.

Server IP Address Displays the IP address of the domain name server(s) the system can use for resolving domain names to IP addresses. Domain look up order is determined by the order of the servers listed. The first server queried is the first server displayed. Therefore, ensure obsolete addresses are periodically removed.

Server Type Displays whether the DNS IP address entry has been created statically (manually) or dynamically. The DHCP server provides the dynamic DNS IP address entry displayed. A static DNS IP address can be created by clicking the *Add* button.

4 Select an IP address from the table and click the *Delete* button to remove the selected entry from the list.

5 Click the *Add* button to display a screen used to add another domain name server. For more information, see [“Adding an IP Address for a DNS Server” on page 109](#).

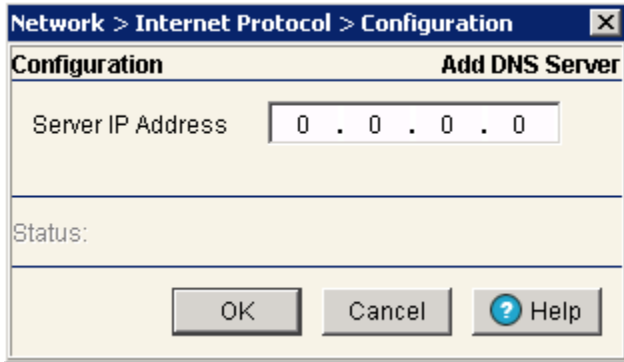
6 Click the *Global Settings* button to open a screen that allows the domain lookup to be enabled/disabled and the domain name to be specified. For more information, see [“Configuring Global Settings” on page 109](#).

Adding an IP Address for a DNS Server

Add an IP address for a new domain server using the *Add* screen.

- 1 Click the *Add* button within the *Domain Network System* screen.

The new *Configuration* screen displays enabling you to add IP address for the DNS Server.



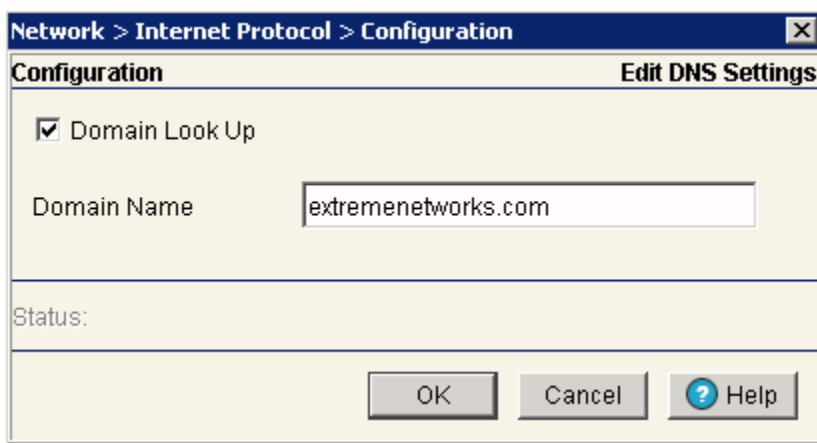
The screenshot shows a dialog box titled "Network > Internet Protocol > Configuration" with a close button (X) in the top right corner. The dialog has two tabs: "Configuration" (selected) and "Add DNS Server". Under the "Configuration" tab, there is a text field labeled "Server IP Address" containing the value "0 . 0 . 0 . 0". Below this field is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

- 2 Enter the *Server IP Address* to define the IP address of the new static domain name server.
- 3 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 4 Click *OK* to use the changes to the running configuration and close the dialog.
- 5 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Global Settings

Use the *Global Settings* screen to query domain name servers to resolve domain names to IP addresses. Use this screen to enable/disable the *Domain look up*, which allows you to use commands like ping, traceroute, etc. using hostnames rather than IP addresses.

- 1 Click the *Global Settings* button in the main *Domain Network System* screen.



The screenshot shows a dialog box titled "Network > Internet Protocol > Configuration" with a close button (X) in the top right corner. The dialog has two tabs: "Configuration" (selected) and "Edit DNS Settings". Under the "Configuration" tab, there is a checked checkbox labeled "Domain Look Up". Below this checkbox is a text field labeled "Domain Name" containing the value "extremenetworks.com". Below this field is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

A *Configuration* screen displays for editing the DNS settings of the server.

- 2 Select the *Domain Look Up* checkbox to enable the controller to query domain name servers to resolve domain names to IP addresses.



NOTE

The order of look up is determined by the order of the servers within the Domain Name System tab. The first server queried is the first server displayed.

- 3 Enter a *Domain Name* in the text field. This is the domain of the controller.
- 4 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 5 Click *OK* to use the changes to the running configuration and close the dialog.
- 6 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring IP Forwarding

The IP Forwarding table lists all the routing entries to route the packets to a specific destination. To view the IP forwarding configuration:

- 1 Select *Network > Internet Protocol* from the main tree menu.
- 2 Select the *IP Forwarding* tab.
Use the Filtering Option to view the details displayed in the table.

SUMMIT® WM3600 CONTROLLER

Network > Internet Protocol

Domain Name System | IP Forwarding | Address Resolution

Routing between VLANs **enabled**, use "Disable" to change this option.

Show Filtering Options

Destination Subnet	Subnet Mask	Gateway Address	Interface	Protocol	Active
0.0.0.0	0.0.0.0	10.255.108.1	vlan1	Static	✓
10.1.1.0	255.255.255.0	0.0.0.0	me1	Connected	✓
10.255.108.0	255.255.255.0	0.0.0.0	vlan1	Connected	✓
192.168.70.0	255.255.255.0	0.0.0.0	vlan70	Connected	✓

Filtering is disabled

Save Logout Refresh Delete Add Disable Help

- 3 The read-only *IP Forwarding* tab displays the current status between VLANs. To toggle the status of routing between VLANs, use the *Enable/Disable* options located at the bottom of the screen.

The following details are displayed in the table:

Destination Subnet	Displays the mask used for destination subnet entries. The Subnet Mask is the IP mask used to divide internet addresses into blocks (known as subnets). A value of 255.255.255.0 will support 256 IP addresses.
Subnet Mask	Displays the mask used for destination subnet entries. The Subnet Mask is the IP mask used to divide internet addresses into blocks (known as subnets). A value of 255.255.255.0 will support 256 IP addresses.
Gateway Address	Displays the IP address of the Gateway used to route the packets to the specified destination subnet. Do not set the gateway address to any VLAN interface used by the controller.
Interface	Displays the interface name with which the destination subnet entries are attached.

Protocol	Displays the name of the routing protocol with which this route was obtained. Possible values are: <ul style="list-style-type: none"> • <i>Static</i>—Routes are statically added by the operator. • <i>DHCP</i>—Routes obtained from the DHCP server. • <i>Connected</i>—Routes automatically installed by the controller for directly connected networks based on interface IP addresses. • <i>Kernel/ ICMP</i>—Routes added as a result of receiving an ICMP redirect from an intermediate router.
Active	When IP Forwarding is enabled for the selected subnet, a green check displays in the <i>Active</i> column. A red X defines the subnet as disabled.

- 4 Select an entry and click the *Delete* button to remove the selected entry from the IP forwarding table.
- 5 Click the *Add* button to create a new static route. For more information, see [“Adding a New Static Route” on page 112](#).
- 6 Click *Enable* (to allow) or *Disable* (to deny) routing between VLANs.

Adding a New Static Route

Use the *Add* screen to add a new destination subnet, subnet mask, and gateway for routing packets to a defined destination. Use the screen when an existing destination subnet does not meet the needs of the network.

To add a new static route:

- 1 Click the *Add* button.

A new *Configuration* screen displays enabling you to add a new destination subnet, subnet mask, and gateway for routing packets to a defined destination.

- 2 In the *Destination Subnet* field, enter an IP address to route packets to a specific destination address.
- 3 Enter a subnet mask for the destination subnet in the *Subnet Mask* field.

The Subnet Mask is the IP mask used to divide internet addresses into blocks known as subnets. A value of 255.255.255.0 supports 256 IP addresses.

- 4 In the *Gateway Address* field, enter the IP address of the gateway used to route the packets to the specified destination subnet. Do not set the gateway address to any VLAN interface used by the controller.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing Address Resolution

The *Address Resolution* table displays the mapping of layer three (IP) addresses to layer two (MAC) addresses. To view address resolution details:

- 1 Select *Network > Internet Protocol* from the main tree menu.
- 2 Select the *Address Resolution* tab.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation tree with 'Internet Protocol' selected. The main content area displays the 'Address Resolution' tab, which contains a table with the following data:

Interface	IP Address	MAC Address	Type
vlan1	10 . 255 . 108 . 1	00-04-96-35-FD-98	Dynamic
vlan1	10 . 255 . 108 . 183	00-15-70-E9-CE-73	Dynamic
vlan1	10 . 255 . 108 . 199	00-04-96-43-50-71	Dynamic

At the bottom of the interface, there are buttons for 'Save', 'Logout', 'Refresh', 'Clear', and 'Help'.

- 3 Refer to the *Address Resolution* table for the following information:

Interface	Displays the name of the actual interface where the IP address was found (typically a VLAN).
-----------	--

IP Address	Displays the IP address being resolved.
MAC Address	Displays the MAC address corresponding to the IP address being resolved.
Type	Defines whether the entry was added statically or created dynamically in respect to network traffic. Entries are typically static.

- 4 Click the *Clear* button to remove the selected AP entry if no longer usable.

Viewing and Configuring Layer 2 Virtual LANs

A virtual LAN (VLAN) is similar to a Local Area Network (LAN), however devices do not need to be connected to the same segment physically. Devices operate as if connected to the same LAN, but could be connected at different physical connections across the LAN segment. The VLAN can be connected at various physical points but react as if it were connected directly. One of the biggest advantages of a VLAN is, when a computer is physically moved to another location, it can stay on the same VLAN without reconfiguration. The controller can support multiple VLANs. Use the *Layer 2 Virtual LANs*

screen to view and configure *VLANs by Port* and *Ports by VLAN* information. Refer to the following VLAN configuration activities:

- [Viewing and Configuring VLANs by Port on page 115](#)
- [Viewing and Configuring Ports by VLAN on page 117](#)

Viewing and Configuring VLANs by Port

- 1 Select *Network > Layer 2 Virtual LANs* from the main menu tree. *VLAN by Port* details display within the Virtual LANs screen.

SUMMIT® WM3600 CONTROLLER

Network > Layer 2 Virtual LANs

VLANs by Port | Ports by VLAN

Name	Mode	Native VLAN	Allowed VLANs	Tagged Native VLAN
ge1	Access	1	1	✗
ge2	Access	1	1	✗
ge3	Access	1	1	✗
ge4	Access	1	1	✗
ge5	Access	1	1	✗
ge6	Access	1	1	✗
ge7	Access	70	70	✗
ge8	Access	70	70	✗
up1	Access	1	1	✗

Buttons: Save, Logout, Refresh, Edit, Help

- 2 Refer to the following details within the table:

Name	Displays the name of the VLAN to which the controller is currently connected.
Mode	It can be either Access or Trunk. <ul style="list-style-type: none"> ● <i>Access</i>—This Ethernet interface accepts packets only from the native VLANs. ● <i>Trunk</i>—The Ethernet interface allows packets from the given list of VLANs you add to the trunk.

Native VLAN	Displays the tag assigned to the native VLAN.
Allowed VLANs	Displays VLAN tags allowed on this interface
Tagged Native VLAN	Displays if the Native VLAN for each port is tagged or not. The column displays a green check mark if the Native VLAN is tagged. If the Native VLAN is not tagged, the column will display a red "x".

A Native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode.

- 3 Select a record from the table and click the *Edit* button to modify the record. For more information, see [“Editing the Details of an Existing VLAN by Port” on page 116.](#)



NOTE

For Adaptive AP to work properly with Summit WM3700, you need to have independent and extended VLANs mapped to a different VLAN than the ge port.



NOTE

The IP address on vlan1 is set to “192.168.0.1/24” by default and the on-board DHCP server will serve IPs from this IP subnet in the range 192.168.1.150-192.168.1.170. If the DSL or Cable modem that is connected to the Summit WM3400 via UP1 (vlan2100) is configured to be in the subnet, then the Summit WM3400 will not install the IP address given out by the DSL/Cable modem on vlan2100. The IP subnet on either the Summit WM3400 or the DSL/Cable modem needs to be changed to resolve the conflict.

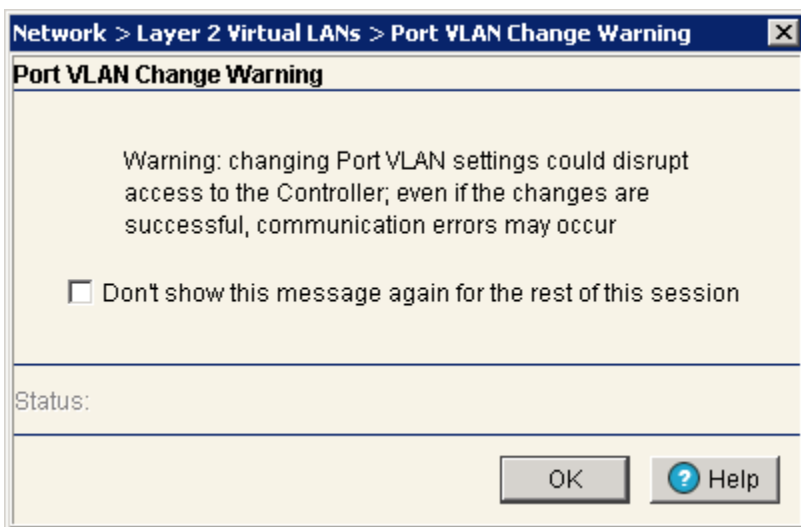
Editing the Details of an Existing VLAN by Port

To revise the configuration of an existing VLAN:

- 1 Select *Network > Layer 2 Virtual LANs* from the main menu tree.
- 2 Select an Ethernet for which you want to configure the VLAN and click the *Edit* button.

The system prompts you with a *Port VLAN Change Warning* message stating that communication disruptions could occur with the controller.

- 3 Click *OK* to continue.



- 4 Use the *Edit* screen to modify the VLAN's mode, access VLAN, and allowed VLAN designation.

The screenshot shows a dialog box titled "Network > Layer 2 Virtual LANs > Edit". The dialog has a title bar with a close button. The main area is labeled "Edit" and contains the following fields:

- Name: ge1
- Mode: Access (dropdown menu)
- Access VLAN: 10
- Allowed VLANs: A section with two radio buttons: "No VLANs" (unselected) and "Selected VLANs" (selected). Below the radio buttons is a text box containing "10".
- Status: (empty field)

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- 5 Use the *Edit* screen to modify the following:

Name	Displays a read-only field and with the name of the Ethernet to which the VLAN is associated.
Mode	Use the drop-down menu to select the mode. It can be either: <ul style="list-style-type: none">• <i>Access</i>—This Ethernet interface accepts packets only from the native VLANs. If this mode is selected, the Allowed VLANs field is unavailable.• <i>Trunk</i>—The Ethernet interface allows packets from the given list of VLANs you can add to the trunk.
Access VLAN	Use this field to change the tag assigned to the native VLAN.
Allowed VLANs	This section has the following 2 options (and is only available when <i>Trunk</i> is selected from the <i>Mode</i> drop-down menu): <ul style="list-style-type: none">• <i>No VLANs</i>—Select this option if you do not wish to add any additional VLANs.• <i>Selected VLANs</i>—Select this option if you wish to add additional VLANs.

- 6 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to use the changes to the running configuration and close the dialog.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing and Configuring Ports by VLAN

A *Virtual Local Area Network* (VLAN) is a controlled network segmented by function or application rather than a traditional LAN segmentation (based on physical location). VLANs allow a greater level of

flexibility and enable changes to the network infrastructure without physically disconnecting network equipment.

To view VLAN by Port information:

- 1 Select *Network > Layer 2 Virtual LANs* from the main menu tree.
- 2 Select the *Ports by VLAN* tab.

VLAN details are displayed within the VLANs by Port tab.

SUMMIT WM3600 CONTROLLER

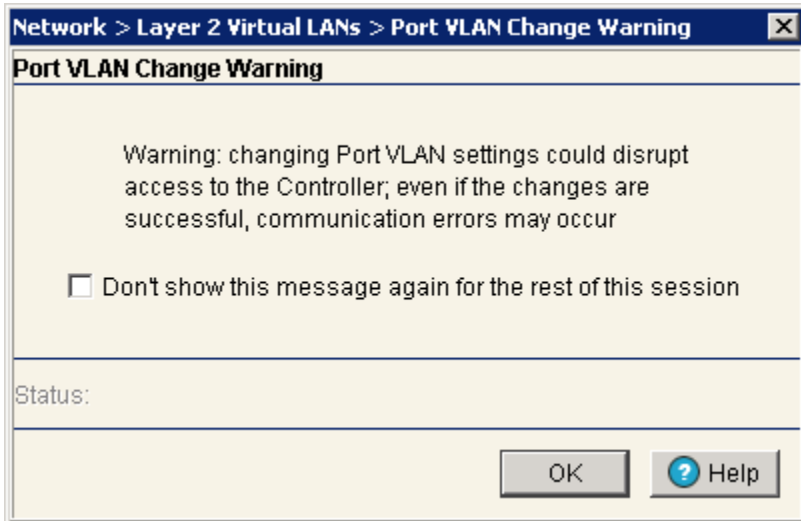
Network > Layer 2 Virtual LANs

VLANs by Port | Ports by VLAN

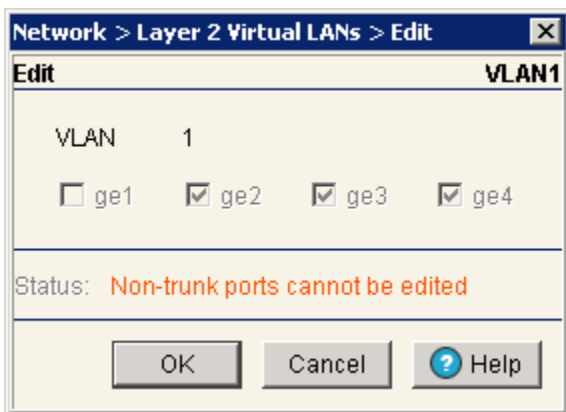
VLAN	ge1	ge2	ge3	ge4	ge5	ge6	ge7	ge8	up1
1	✓	✓	✓	✓	✓	✓	✗	✗	✓
70	✗	✗	✗	✗	✗	✗	✓	✓	✗

Buttons: Save, Logout, Refresh, Edit, Help

- 3 Highlight an existing VLAN and click the *Edit* button. The system displays a *Port VLAN Change Warning* message stating that changing VLAN designations could disrupt access to the controller.



- 4 Click *OK* to continue. A new window is displayed wherein the VLAN assignments can be modified for the selected VLAN.



NOTE

The ports available vary by controller.
On the Summit WM3600, the available ports are ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, and up1.
On the Summit WM3700, the available ports are ge1, ge2, ge3, and ge4.
On the Summit WM3400, the available ports are ge1, ge2, ge3, ge4, ge5, and up1.

- 5 Change VLAN port designations as required.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Controller Virtual Interfaces

A *Controller Virtual Interface* (SVI) is required for layer 3 (IP) access to the controller or to provide layer 3 service on a VLAN. The SVI defines which IP address is associated with each VLAN ID that the controller is connected to. An SVI is created for the default VLAN (VLAN 1) to enable remote controller administration. An SVI is also used to map VLANs to IP address ranges. This mapping determines the destination networks for controller routing.

Each IP address range (IP Address and Subnet Mask) can be mapped to one (and only one) VLAN ID. A VLAN ID does not require an IP address be defined on the controller. Each VLAN ID must be mapped to a physical port using the Layer 2 Virtual LANs configuration to communicate with the rest of the network.

Use the *Controller Virtual Interfaces* screen to view and configure VLAN interfaces. This screen contains two tabs supporting the following activities:

- [Configuring the Virtual Interface on page 121](#)
- [Viewing Virtual Interface Statistics on page 125](#)

Configuring the Virtual Interface

Use the *Configuration* screen to view and configure the virtual interface details.

- 1 Select *Network > Controller Virtual Interface* from the main tree menu.
- 2 Select the *Configuration* tab.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation tree with categories like Controller, Network, Services, Security, Management Access, and Diagnostics. The main area is titled "Network > Controller Virtual Interfaces" and has two tabs: "Configuration" and "Statistics". The "Configuration" tab is active, displaying a table of virtual interfaces.

Name	VLAN ID	DHCP Enabled	Primary IP Address	Primary Subnet Mask	Admin Status	Oper Status	Management Interface
vlan1	1	✘	10 . 255 . 108 . 36	255 . 255 . 255 . 0	Up	Up	✓
vlan70	70	✘	192 . 168 . 70 . 1	255 . 255 . 255 . 0	Up	Up	✘

Below the table is a section for "Associated Secondary IP Addresses" with columns for "IP Address" and "Subnet Mask". At the bottom of the interface are buttons for "Edit", "Delete", "Add", "Startup", "Shutdown", and "Help".

The following configuration details display in the table:

Name	Displays the name of the virtual interface.
VLAN ID	Displays the VLAN ID associated with the interface.
DHCP	Displays whether the DHCP client is enabled or not. A green check mark defines the DHCP client as enabled for the interface. A red X means the interface is disabled.
Primary IP Address	Displays the IP address for the virtual interface.
Primary Subnet Mask	Displays the subnet mask assigned for this interface.
Admin Status	Displays whether the virtual interface is operational and available to the controller.
Oper Status	Displays whether the selected Controller Virtual Interface is currently (Up) or not (Down) on the controller.

Management Interface

A green checkmark within this column defines this VLAN as currently used by the controller. This designates the interface settings used for global controller settings in case of conflicts. For example, if multiple SVIs are configured with DHCP enabled on each, the controller could have multiple domain names assigned from different DHCP servers. The one assigned over the selected Management Interface would be the only one used by the controller. This setting does not affect any of the Management Access Interfaces configured using [“Configuring Access Control” on page 533](#).

**NOTE**

The IP address on vlan1 is set to “192.168.0.1/24” by default and the on-board DHCP server will serve IPs from this IP subnet in the range 192.168.1.150-192.168.1.170. If the DSL or Cable modem that is connected to the Summit WM3400 via UP1 (vlan2100) is configured to be in the subnet, then the Summit WM3400 will not install the IP address given out by the DSL/Cable modem on vlan2100. The IP subnet on either the Summit WM3400 or the DSL/Cable modem needs to be changed to resolve the conflict.

- 3 Select a record from the table and click the *Edit* button to modify the record. For more information, see [“Modifying a Virtual Interface” on page 124](#).
- 4 Select a record from the table and click the *Delete* button to remove the configuration from the list of controller virtual interfaces.
- 5 Click the *Add* button to add a new configuration to the controller virtual interface. For more information, see [“Adding a Virtual Interface” on page 122](#).
- 6 Select an interface and click the *Startup* button to invoke the selected interface the next time the controller is booted.
- 7 Select an interface and click the *Shutdown* button to disable the selected interface.

Adding a Virtual Interface

To add a new controller virtual interface:

- 1 Select *Network > Controller Virtual Interface* from the main tree menu.
- 2 Select the *Configuration* tab.

- 3 Click the *Add* button.

Network > Switch Virtual Interfaces > Configuration

Configuration Add New

VLAN ID

Description

Primary IP Settings

Use DHCP to obtain IP Address automatically

IP Address

Subnet Mask

Set as Management Interface

Secondary IP Addresses

IP Address	Subnet Mask

Edit Delete Add

Status:

OK Cancel Help

- 4 Enter the *VLAN ID* for the controller virtual interface.
- 5 Provide a *Description* for the VLAN, representative of the VLAN's intended operation within the controller managed network.
- 6 The *Primary IP Settings* field consists of the following:
 - a Select *Use DHCP to obtain IP Address automatically* to allow DHCP to provide the IP address for the virtual interface. Selecting this option disables the IP address field.
 - b Enter the *IP Address* for the VLAN associated virtual interface.
 - c Enter the *Subnet Mask* for the IP address.
- 7 Select the *Set as Management Interface* checkbox to enable any host displayed in this VLAN to configure the controller.
- 8 Use the *Secondary IP Addresses* field to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.
Select the *Add* button (within the *Secondary IP Addresses* field) to define additional addresses from a sub screen. Choose an existing secondary address and select *Edit* or *Delete* to revise or remove a secondary address.
- 9 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to use the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

Modifying a Virtual Interface

To modify an existing virtual interface:



CAUTION

When changing from a default DHCP address to a fixed IP address, set a static route first. This is critical when the controller is being accessed from a subnet not directly connected to the controller and the default route was set from DHCP.

- 1 Select *Network > Controller Virtual Interface* from the main tree menu.
- 2 Select the *Configuration* tab and click the *Edit* button.

The screen displays with the name of the VLAN in the upper right-hand side. The VLAN ID cannot be modified and should be used to associate the VLAN ID with the description and IP address assignments defined.

- 3 If necessary, modify the *Description* of the VLAN, to make it representative of the VLAN's intended operation within the controller managed network.
- 4 Unselect the *Use DHCP to obtain IP Address automatically* checkbox to assign IP addresses manually and you do not want DHCP to provide them.
- 5 Use the *Primary IP Address* field to manually enter the IP address for the virtual interface.
- 6 Enter the *Subnet Mask* for the IP address.
- 7 Select the *Set as Management Interface* checkbox to convert the selected VLAN ID to a management interface.
- 8 Use the *Secondary IP Addresses* field to define/modify additional IP addresses to associate with VLAN IDs. The addresses provided will be used if the primary IP address is unreachable.

Select the *Add* button (within the *Secondary IP Addresses* field) to define/modify additional addresses from a sub screen. Select an existing secondary address and select *Edit* or *Delete* to revise or remove a secondary address as needed.

- 9 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to use the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing Virtual Interface Statistics

The *Statistics* screen displays information about packet level statistics and errors at the interface.

To view virtual interface statistics:

- 1 Select *Network > Controller Virtual Interface* from the main tree menu.
- 2 Select the *Statistics* tab.

The screenshot shows the Summit WM3600 Controller web interface. The main navigation tree on the left includes 'Controller', 'Network', 'Services', 'Security', 'Management Access', and 'Diagnostics'. Under 'Network', 'Controller Virtual Interfaces' is selected. The main content area shows the 'Statistics' tab for 'Controller Virtual Interfaces'. A table displays the following data:

Name	Bytes In	Packets In	Packets In Dropped	Packets In Error	Bytes Out	Packets Out	Packets Out Dropped	Packets Out Error
vian1	630522532	2183068	0	0	220768664	979192	0	0
vian70	0	0	0	0	0	0	0	0

At the bottom of the interface, there are buttons for 'Save', 'Logout', 'Refresh', 'Details', 'Graph', and 'Help'.

Refer to the following to assess the network throughput of existing virtual interfaces:

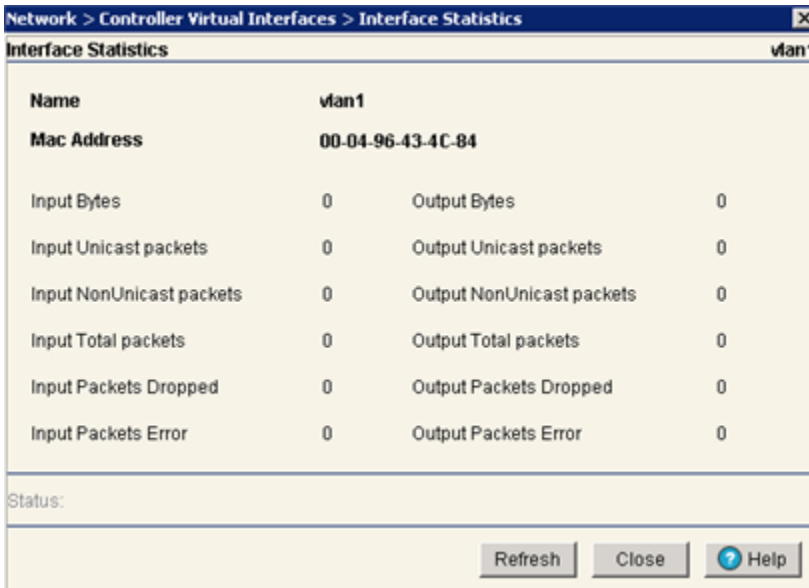
Name	Displays the user-defined interface name. The corresponding statistics are displayed along the row. The statistics are the total traffic to the interface since its creation.
Bytes In	Displays the number of bytes coming into the interface. The status is not self-updated. To view the current status, click the <i>Details</i> button.
Packets In	Displays the number of packets coming into the interface (including packets dropped, error packets, etc.)
Packets In Dropped	Displays the number of dropped packets coming into the interface. Packets are dropped if: <ul style="list-style-type: none">• The input queue for the hardware device/software module handling the interface definition is saturated/full.• Overruns occur when the interface receives packets faster than it can transfer them to a buffer.
Packets In Error	Displays the number of error packets coming into the interface. <ul style="list-style-type: none">• <i>Runt frames</i>—Packets shorter than the minimum Ethernet frame length (64 bytes).• <i>CRC errors</i>—The <i>Cyclical Redundancy Check</i> (CRC) is the 4 byte field at the end of every frame. The receiving station uses to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of frame, it is considered as a CRC error.• <i>Late collisions</i>—A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending station. Late collisions are not normal and are usually the result of out of specification cabling or a malfunctioning device.• <i>Misaligned frames</i>—A misaligned frame is a frame that somehow gets out of sync with the receiving station's receive clock recovery circuit. Misalignment is reported if the frame ends with a CRC error and extra bits are also detected.
Bytes Out	Displays the number of bytes going out on the interface.
Packets Out	Displays the number of packets going out on the interface.
Packets Out Dropped	Displays the number of dropped packets going out of the interface due to saturated output queues assigned to the interface processor or the physical device/software module. Packets can be dropped due to collisions as well.
Packets Out Error	Displays the number of error packets going out of the interface including frame forming errors or malformed packets transmitted over the interface.

- 3 Click the *Details* button to view packet level statistics of any user-defined interface. For more information, see [“Viewing Virtual Interface Statistics” on page 127](#).
- 4 Click the *Graph* button to view a graphical representation of the controller virtual interface statistics. For more information, see [“Viewing the Virtual Interface Statistics Graph” on page 128](#).

Viewing Virtual Interface Statistics

To view detailed virtual interface statistics:

- 1 Select a virtual interface from the *Statistics* tab.
- 2 Click the *Details* button.



The screenshot shows a window titled "Network > Controller Virtual Interfaces > Interface Statistics" with a close button. The window content is titled "Interface Statistics" and "vlan1". It displays a table of statistics for the interface. Below the table is a "Status:" field and three buttons: "Refresh", "Close", and "Help".

Name	vlan1		
Mac Address	00-04-96-43-4C-84		
Input Bytes	0	Output Bytes	0
Input Unicast packets	0	Output Unicast packets	0
Input NonUnicast packets	0	Output NonUnicast packets	0
Input Total packets	0	Output Total packets	0
Input Packets Dropped	0	Output Packets Dropped	0
Input Packets Error	0	Output Packets Error	0

- 3 The *Interface Statistics* screen displays the following content:

Name	Displays the title of the logical interface selected.
MAC Address	Displays physical address information associated with the interface. This address is read-only (hard-coded at the factory) and cannot be modified.
Input Bytes	Displays the number of bytes received by the interface.
Input Unicast Packets	Displays the number of unicast packets (packets directed towards the interface) received at the interface.
Input NonUnicast Packets	Displays the number of NonUnicast Packets (Multicast and Broadcast Packets) received at the interface.
Input Total Packets	Displays the total number of packets received at the interface.
Input Packets Dropped	Displays the number of packets dropped at the interface by the input Queue of the hardware unit /software module associated with the VLAN interface. Packets are dropped when the input Queue of the interface is full or unable to handle incoming traffic.
Input Packets Error	Displays the number of packets with errors at the interface. Input Packet Errors are input errors occurring due to: no buffer space/ignored packets due to broadcast storms, packets larger than maximum packet size, framing errors, input rate exceeding the receiver's data handling rate, or cyclic redundancy check errors. In all these cases, an error is reported.
Output Bytes	Displays the number of bytes transmitted from the interface.
Output Unicast Packets	Displays the number of unicast packets (packets directed towards a single destination address) transmitted from the interface.
Output NonUnicast Packets	Displays the number of unicast packets transmitted from the interface.
Output Total Packets	Displays the total number of packets transmitted from the interface.

Output Packets Dropped	Displays the number of transmitted packets dropped at the interface. Output Packets Dropped are packets dropped when the output queue of the physical device associated with interface is saturated.
Output Packets Error	Displays the number of transmitted packets with errors. Output Packet Errors are the sum of all the output packet errors, malformed packets, and misaligned packets received on an interface.

- 4 The *Status* is the current state of requests made from the applet. Requests are any “SET/GET” operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 5 Click the *Refresh* button to refresh the virtual interface statistics. Status information is not polled to the applet. Hence you have to refresh the controller to retrieve the data.
- 6 Click the *Close* button to exit the screen. Clicking *Close* does not lose any data, as there are no values configured within this screen (it is read-only).

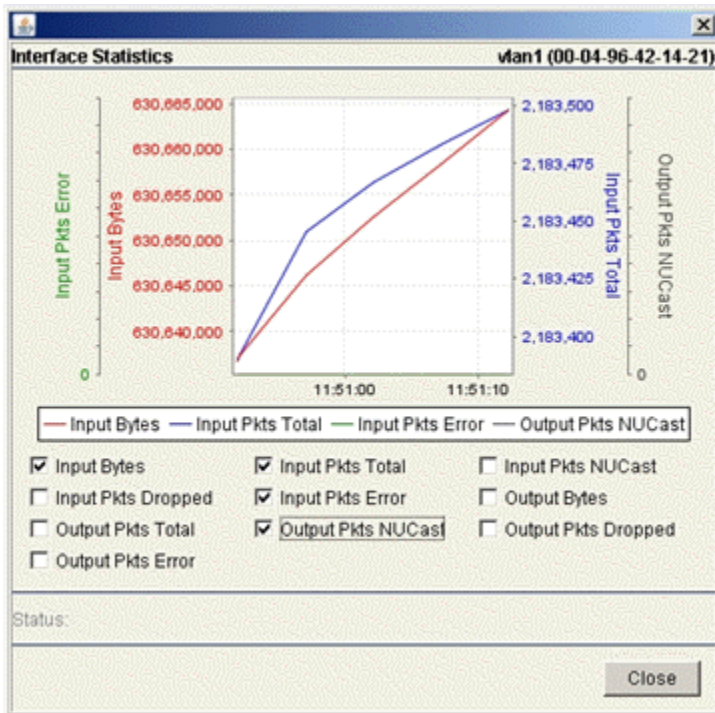
Viewing the Virtual Interface Statistics Graph

The controller Web UI continuously updates its virtual interface statistics, even when the graph is closed. Periodically display the virtual statistics graph for the latest information as network performance information is required.

To view detailed graphical statistics for a selected interface:

- 1 Select a record from the table displayed in the *Statistics* screen.
- 2 Click the *Graph* button.
- 3 The *Interface Statistics* screen displays. The *Interface Statistics* screen provides the option of viewing graphical statistics for the following parameters:
 - Input Bytes
 - Input Pkts Dropped
 - Output Pkts Total
 - Output Pkts Error
 - Input Pkts Total
 - Input Pkts Error
 - Output Pkts NUCast
 - Input Pkts NUCast
 - Output Bytes
 - Output Pkts Dropped

Select any of the above parameters by clicking on the checkbox associated with it.



NOTE

Only four parameters may be selected at any given time.

- 4 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 5 Click *Close* to close the dialog.

Viewing and Configuring Controller WLANs

A *wireless LAN (WLAN)* is a *local area network (LAN)* without wires. WLANs transfer data through the air using radio frequencies instead of cables. The WLAN screen displays a high-level overview of the WLANs created for the controller managed network. Use this data as necessary to the WLANs that are active, their VLAN assignments, updates to a WLAN's description, and their current authentication and encryption scheme. The Wireless LANs screen is partitioned into 5 tabs supporting the following configuration activities:

- [Configuring WLANs on page 130](#)
- [Viewing WLAN Statistics on page 169](#)
- [Configuring WMM on page 176](#)
- [Configuring the NAC Inclusion List on page 180](#)
- [Configuring the NAC Exclusion List on page 184](#)

Configuring WLANs

Refer to the *Configuration* screen for a high-level overview of the WLANs created for use within the controller-managed network. Use this data as necessary to keep current of active WLANs, their VLAN assignments, updates to a WLAN's description, and their current authentication and encryption schemes. Be careful to properly map BSS WLANs and security schemes.



NOTE

The Summit WM3600 supports a maximum of 32 WLANs. The Summit WM3700 supports a maximum of 256 WLANs. Summit WM3400 supports a maximum of 24 WLANs.

To configure a WLAN:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Click the *Configuration* tab.

SUMMIT® WM3600 CONTROLLER

Network > Wireless LANs

Configuration | Statistics | WMM | NAC Include | NAC Exclude

Show Filtering Options << Page 1 of 2 Go >>

Index	Enabled	ESSID	Description	VLAN	Authentication	Encryption	Independent Mode	QoS Weight	802.11w-PMF
1	✓	test-open-1x	WLAN1	1	802.1X EAP	None	✗	1	None
2	✓	test-open-hotspot	WLAN2	1	Hotspot	None	✗	1	None
3	✗	103	WLAN3	1	None	None	✗	1	None
4	✗	104	WLAN4	1	None	None	✗	1	None
5	✗	105	WLAN5	1	None	None	✗	1	None
6	✗	106	WLAN6	1	None	None	✗	1	None
7	✗	107	WLAN7	1	None	None	✗	1	None
8	✗	108	WLAN8	1	None	None	✗	1	None
9	✗	109	WLAN9	1	None	None	✗	1	None
10	✗	110	WLAN10	1	None	None	✗	1	None
11	✗	111	WLAN11	1	None	None	✗	1	None
12	✗	112	WLAN12	1	None	None	✗	1	None
13	✗	113	WLAN13	1	None	None	✗	1	None
14	✗	114	WLAN14	1	None	None	✗	1	None
15	✗	115	WLAN15	1	None	None	✗	1	None
16	✗	116	WLAN16	1	None	None	✗	1	None
17	✗	117	WLAN17	1	None	None	✗	1	None
18	✗	118	WLAN18	1	None	None	✗	1	None
19	✗	119	WLAN19	1	None	None	✗	1	None
20	✗	120	WLAN20	1	None	None	✗	1	None
21	✗	121	WLAN21	1	None	None	✗	1	None
22	✗	122	WLAN22	1	None	None	✗	1	None
23	✗	123	WLAN23	1	None	None	✗	1	None
24	✗	124	WLAN24	1	None	None	✗	1	None
25	✗	125	WLAN25	1	None	None	✗	1	None
26	✗	126	WLAN26	1	None	None	✗	1	None
27	✗	127	WLAN27	1	None	None	✗	1	None
28	✗	128	WLAN28	1	None	None	✗	1	None
29	✗	129	WLAN29	1	None	None	✗	1	None
30	✗	130	WLAN30	1	None	None	✗	1	None

Filtering is disabled Page 2 of 2 loaded.

Save Logout Refresh Edit Enable Disable Export Global Settings Help

The *Configuration* tab displays the following details:

Controller	The <i>Controller</i> field displays the IP address of the cluster member associated with each WLAN. When clustering is enabled on the controller and <i>Cluster GUI</i> is enabled, the <i>Controller</i> field will be available on the Wireless LAN screen. For information on configuring enabling <i>Cluster GUI</i> , see “Managing Clustering Using the Web UI” on page 358 .
Index	Displays the WLAN’s numerical identifier. The WLAN index range is from 1 to the maximum number of WLANs supported by the controller. An index can be helpful to differentiate a WLAN from other WLANs with similar configurations.
Enabled	Refer to the Enabled parameter to discern whether the specified WLAN is enabled or disabled. When enabled, a green check mark displays. When disabled, a red “X” displays. To enable or disable a WLAN, select it from the table and click the <i>Enable</i> or <i>Disable</i> button.
ESSID	Displays the Extended Service Set ID associated with each WLAN. Click the <i>Edit</i> button to modify the value to a new unique SSID.
Description	Displays a short description of the associated WLAN. Click the <i>Edit</i> button to modify the value the WLAN description.
VLAN(s)	Displays the name of the VLAN ID(s) of the VLAN(s) this WLAN is mapped to. The VLAN ID can be between 1 and 4094. The default mapping is to a single VLAN with VLAN ID 1.
Authentication	Displays the type of authentication used with the specified WLAN. Click the <i>Edit</i> button to modify the WLAN’s current authentication scheme. For information on configuring an authentication scheme for a WLAN, see “Configuring Authentication Types” on page 142 .
Encryption	Displays the type of wireless encryption used on the specified WLAN. When no encryption is used, the field displays “none”. Click the <i>Edit</i> button to modify the WLAN’s current encryption scheme. For information on configuring an authentication scheme for a WLAN, see “Configuring Different Encryption Types” on page 163 .
Independent Mode	Determines whether the WLAN is functioning as an independent or extended WLAN in regards its support of <i>adaptive AP</i> (AAP) operation. Independent WLANs (defined by a green checkmark) are local to an AAP and configured from the controller. Specify a WLAN as independent for no traffic to be forward to the controller. Independent WLANs behave like WLANs as used on a a standalone Access Point. Extended WLAN (defined by the default red X) are typical centralized WLANs created on the controller. Select an existing WLAN to revise its default extended mode designation if intending to use the WLAN for AAP support. For more information, see “Editing the WLAN Configuration” on page 134 .
QOS Weight	Defines the Quality of Service weight for the WLAN. WLAN QoS will be applied based on the QoS weight value with higher values representing higher priority. The range for QoS weight values is between 1 and 10 with 1 being the default value.
802.11 w-PMF	Displays the Management Frame Protection status for each WLAN. MFP can be set to None, Required, or Optional. MFP is only available on WLANs with CCMP encryption. The range is between 1000ms to 6000ms and default value is 100ms for Summit WM3400, Summit WM3600 and Summit WM3700.

- 3 Click the *Edit* button to display a screen where WLAN information, encryption, and authentication settings can be viewed or changed.

- 4 Click the *Enable* button to enable the selected WLAN. When enabled, a green check mark displays. When disabled, a red "X" displays. Enabled WLANs are displayed in a number of different controller Web UI configurations for additional configuration activities. To enable or disable a WLAN, select it from the table and click the *Enable* or *Disable* button. The *Enable* button is only available when the selected WLAN is disabled.
- 5 Click the *Disable* button to disable the selected WLAN. When enabled, a green check mark displays. When disabled, a red "X" displays. To enable or disable a WLAN, select it from the table and click the *Enable* or *Disable* button. The *Disable* button is only available when the selected WLAN is enabled.
- 6 When using clustering and the *Cluster GUI* feature is enabled, a pull-down menu will be available to select which cluster members' WLANs are displayed. To view WLANs from all cluster members, select *All* from the pull-down menu. To view WLANs from a specific cluster member, select that member's IP address from the pull-down menu.
- 7 Click the *Global Settings* button to display a screen with WLAN settings applying to all the WLANs on the system. Remember, changes made to any one value impact each WLAN.

Click *OK* to save updates to the *Global WLAN Settings* screen. Click *Cancel* to disregard changes and revert back to the previous screen. Checkbox options within the Global Settings screen include:

- MU Proxy ARP handling** Enables Proxy ARP handling for MUs. Proxy ARP is provided for MUs in PSP mode whose IP address is known. The WLAN generates an ARP reply on behalf of an MU, if the MU's IP address is known. The ARP reply contains the MAC address of the MU (not the MAC address of WLAN Module). Thus, the MU does not awaken to send ARP replies (helping to increase battery life and conserve bandwidth). If an MU goes into PSP mode without transmitting at least one packet, its Proxy ARP will not work for the MU. This option is selected by default.
- Shared-Key Authentication** Enables Shared-Key Authentication for all enabled WLANs on the system. Shared-key authentication is strongly discouraged. This option is enabled in setups where there are legacy mobile units, which can only support this authentication method.

Manual mapping of WLANs	<p>Use this option (it is selected by default) for custom WLAN to Radio mappings. When this option is disabled, the user cannot conduct Radio – WLAN mapping. Additionally, the user cannot enable WLANs with an index higher than 16. (The WLAN numbers will depend on the device on which this feature is enabled). Once the this option is enabled, the following conditions must be satisfied (to successfully disable it). No WLANs with an index higher than 16 should be enabled. With advanced WLAN mapping, the controller evenly distributes the enabled WLANs to BSSIDs. Additionally, the Radio – WLAN mapping should conform to the following:</p> <p>BSS ID 1—Possible WLANs 1,5,9,13 BSS ID 2—Possible WLANs 2,6,10,14 BSS ID 3—Possible WLANs 3,7,11,15 BSS ID 4—Possible WLANs 4, 8, 12,16</p> <p>If the above conditions are not satisfied, disabling this option will fail.</p>
Enable WLAN Bandwidth Settings	Select this option to enable WLAN bandwidth settings. WLAN bandwidth settings ensures quality of service for applications regardless of network load. This option is selected by default.
MU Rate Limiting UP	Enter an upstream rate limit in kbps for all MUs associated with the controller across all WLANs.
MU Rate Limiting Down	Enter a downstream rate limit in kbps for all MUs associated with the controller across all WLANs.
MU Load Balance Mode	Configure a method for distributing traffic across MUs using the <i>MU Load Balancing Mode</i> . Select <i>Count</i> to set load balancing based on number of MUs. Select <i>By Throughput</i> to set load balancing based on total throughput of MUs.
Hotspot Voucher Logo Name	Enter the name of the image that is used on each Hotspot Voucher generated for each guest user. Use this to include your organization's logo as a part of the generated Hotspot Voucher.
Hotspot Voucher Title	Enter a title that is displayed on each Hotspot Voucher generated for each guest user. Use this to include any information or your organization's Name as a part of the generated Hotspot Voucher.
Max Events Before Email Alert	This value sets the number of adoption/unadoption events that must occur before an email alert is sent. Set this value in the range 1-10000.
Email Alert Time Period	This value sets the time duration in minutes that must expire before an email is sent again for continuous adoption/unadoption events. Set a value in the range of 1-1440 minutes.
Email Alert Per Radio Initial Count	This value sets the number of initialization events for which emails are sent. When a radio initializes, it might cycle through multiple adoption/unadoption before being adopted. This value configures the number of adoption and unadoption events for which emails will be sent when the radio is initializing.

Editing the WLAN Configuration

Security measures for the controller and its WLANs are critical. Use the available controller security options to protect each WLAN from wireless vulnerabilities, and secure the transmission of RF packets between WLANs and the MU traffic they support.

The user has the capability of configuring separate security policies for each WLAN. Each security policy can be configured based on the authentication (Kerberos, 802.1x EAP, Hotspot) and /or encryption (WEP, KeyGuard, WPA/WPA2-TKIP, or WPA2/CCMP) scheme.

All of the default WLANs are available for modification when the user accesses the Wireless LANs screen. However, the WLAN requires an authentication or encryption scheme be applied before it can begin securing the data traffic within the controller-managed wireless network. The *Edit* screen provides a mean of modifying the existing WLANs SSID, description, VLAN ID assignment, inter-WLAN communication definition, and encryption and authentication scheme. To edit WLAN configuration settings:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Select a WLAN to modify from the table.

4 Click the *Edit* button.

Network > Wireless LANs > Edit WLAN1

Edit

Configuration

ESSID: Description:

Deny Static MU
 Enable URL Logging
 Independent Mode
 Client Bridge Backhaul

Enter a list VLAN ID: <input type="text" value="10"/> <input type="checkbox"/> Dynamic Assignment <input type="button" value="Assign Multiple VLANs"/>	Enter a list of IP Filter Rules In filters: <input type="text"/> Out filters: <input type="text"/>	802.11w-PMF: <input type="text" value="None"/> SA Query Max Timeout: <input type="text" value="1000"/> (100 - 6000 msec) SA Query Retry Timeout: <input type="text" value="201"/> (10 - 1500 msec)
---	--	--

Authentication

802.1X EAP
 Kerberos
 Hotspot
 MAC Authentication
 No Authentication

Encryption

WEP 64
 WEP 128
 KeyGuard
 WPAWPA2-TKIP
 WPA2-CCMP

Advanced

Accounting Mode: <input type="text" value="Off"/>	MU to MU Traffic: <input type="text" value="Allow Packets"/>	
<input checked="" type="checkbox"/> Answer Broadcast ESS	MU Idle Time: <input type="text" value="1800"/> seconds	
<input type="checkbox"/> Use Voice Prioritization	Access Category: <input type="text" value="Automatic/WMM"/>	
<input type="checkbox"/> Enable SVP	MCast Addr 1: <input type="text" value="00 - 00 - 00 - 00 - 00 - 00"/>	
<input type="checkbox"/> Secure Beacon	MCast Addr 2: <input type="text" value="00 - 00 - 00 - 00 - 00 - 00"/>	
QOS Weight: <input type="text" value="1"/>	NAC Mode: <input type="text" value="None"/>	

Status:

The Wireless LANs Edit screen is divided into the following user-configurable fields:

- Controller IP
 - Configuration
 - Authentication
 - Encryption
 - Advanced
- 5 The *Controller* field displays the IP address of the cluster member associated with each WLAN. When clustering is enabled on the controller and Cluster GUI is enabled, the *Controller* field will be available on the Wireless LAN screen. For information on configuring enabling Cluster GUI, see [“Managing Clustering Using the Web UI” on page 358](#).
- 6 Refer to the *Configuration* field to define the following WLAN values

ESSID	Displays the <i>Extended Service Set ID</i> (ESSID) associated with each WLAN. If changing the ESSID, ensure the value used is unique.
Description	If editing an existing WLAN, ensure its description is updated accordingly to best describe the intended function of the WLAN.
Deny Static MU	Enabling this option provides WLAN based configuration to allow only traffic from those mobile units whose IP is present in the layer 3 entity table. If the IP entry is not present in the layer 3 entity table, the event will be logged and the packet dropped.
Enable URL Logging	Enable URL Logging to log all HTTP GET requests. Along with the URL, a mobile unit IP address will also be logged.
Independent Mode (AAP Only)	Determines whether the WLAN is functioning as an independent or extended WLAN in regards its support of <i>adaptive AP</i> (AAP) operation. Select the checkbox to designate the WLAN as independent and prevent traffic from being forwarded to the controller. Independent WLANs behave like WLANs as used on a standalone Access Point. Leave this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the controller). For an overview of AAP and how it is configured and deployed using the controller and Access Point, see “Adaptive AP Overview” on page 595 .
VLAN ID	Displays the VLAN ID of VLANs assigned to WLANs. By default, all WLANs created are assigned to VLAN 1.
Dynamic Assignment	With any authentication method that involves a RADIUS server, the RADIUS server may be configured to include a VLAN ID attribute in its “ACCESS Accept” response. This VLAN, instead of the configured VLAN(s) on this WLAN, will be assigned to the mobile unit. Enabling this check mark will enable controller to take VLAN ID from RADIUS response. When disabled, controller will ignore the VLAN ID from RADIUS response.
Assign Multiple VLANs	Click this button when it is desirable to assign multiple VLANs to this WLAN. For more information, see “Assigning Multiple VLANs per WLAN” on page 140 .
802.11w-PMF	On WLANs with CCMP encryption enabled, choose an 802.11w-PMF mode from the pull-down menu. Available options are: <ul style="list-style-type: none">● None● Optional● Required
SA Query Max Timeout	Define the maximum time (in milliseconds) before an SA Query is timed out. The valid timeout range is between 100 msec and 6000 msec with a default value of 1000 msec.

SA Query Retry Timeout	Define the maximum number of retries before an SA Query is timed out. The valid retry range is between 10 and 1500 retries with a default value of 201 retries.
------------------------	---



NOTE

When configuring wireless settings for Adaptive APs, all configuration must be done through the controller and not from the AP management console. Making changes directly in the AP management console can lead to unstable operation of the Adaptive AP.



NOTE

For a Radius supported VLAN to function, the “Dynamic Assignment” checkbox must be enabled for the WLAN supporting the VLAN.



NOTE

If the WLAN is to support AAP, the Independent Mode (AAP Only) checkbox must be selected. Additionally, the Access Point must have its auto discovery option enabled to be discovered by the controller. For information on configuring an Access Point for AAP support, see [“Adaptive AP Configuration” on page 606](#)

7 Refer to the *Authentication* field to select amongst the following options:

802.1X EAP	A RADIUS server is used to authenticate users. For detailed information on configuring EAP for the WLAN, see “Configuring 802.1x EAP” on page 142 .
Kerberos	A Kerberos server is used to authenticate users. For detailed information on configuring Kerberos for the WLAN, see “Configuring Kerberos” on page 143 .
Hotspot	A Hotspot is used to authenticate users in a unique network segment (hotspot). The attributes of both the hotspot and the RADIUS Server are required. For more information, see “Configuring Hotspots” on page 144 .
MAC Authentication	The controller uses a RADIUS server to see if a target MAC address is allowed on the network. The attributes of the RADIUS Server are required. For more information, see “Configuring MAC Authentication” on page 154
No Authentication	When selected, no Authentication is used and transmissions are made (in the open) without security unless an encryption scheme is used. This setting is not recommended when data protection is important.

8 Refer to the *Encryption* field to select among the following options:

WEP 64	Use the WEP 64 checkbox to enable the <i>Wired Equivalent Privacy</i> (WEP) protocol with a 40-bit key. WEP is available in two encryption modes: 40 bit (also called WEP 64) and 104 bit (also called WEP 128). The 104-bit encryption mode provides a longer algorithm that takes longer to decode than that of the 40-bit encryption mode. For detailed information on configuring WEP 64 for the WLAN, see “Configuring WEP 64” on page 163 .
--------	---

WEP 128	Use the WEP 128 checkbox to enable the <i>Wired Equivalent Privacy</i> (WEP) protocol with a 104-bit key. WEP is available in two encryption modes: WEP 64 (using a 40-bit key) and WEP 128 (using a 104-bit key). WEP 128 encryption mode provides a longer algorithm that takes longer to decode than that of the WEP 64 encryption mode. For detailed information on configuring WEP 128 for the WLAN, see “Configuring WEP 128 / KeyGuard” on page 165.
KeyGuard	Uses a proprietary encryption mechanism to protect data. For detailed information on configuring KeyGuard for the WLAN, see “Configuring WEP 128 / KeyGuard” on page 165.
WPA-WPA2-TKIP	Use the WPA-TKIP checkbox to enable <i>Wi-Fi Protected Access</i> (WPA) with <i>Temporal Key Integrity Protocol</i> (TKIP). For detailed information on configuring TKIP for the WLAN, see “Configuring WPA/WPA2 using TKIP and CCMP” on page 166.
WPA2-CCMP	WPA2 is a newer 802.11i standard that provides even stronger wireless security than Wi-Fi Protected Access (WPA) and WEP. CCMP is the security standard used by the <i>Advanced Encryption Standard</i> (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a <i>Message Integrity Check</i> (MIC) using the proven <i>Cipher Block Chaining</i> (CBC) technique. Changing just one bit in a message produces a totally different result. For detailed information on configuring CCMP for the WLAN, see “Configuring WPA/WPA2 using TKIP and CCMP” on page 166.

9 Refer to the *Advanced* field for the following information:

Accounting Mode	<p>If using a Syslog server to conduct accounting for the controller, select the Syslog option from the <i>Accounting Mode</i> drop-down menu. Once selected, a <i>Syslog Config</i> button is enabled on the bottom of the Network > Wireless LANs > Edit screen. Use this sub screen to provide the Syslog Server IP address and port for the Syslog Server performing the accounting function.</p> <p>If either Hotspot, MAC Authentication, or 802.1x EAP have been selected from within the <i>Authentication</i> field, a <i>Radius Config</i> button is enabled (on the bottom of the screen) allowing the user to define a Primary and Secondary RADIUS Accounting Server IP address, port, shared secret password, and timeout and retry. Define these accounting settings as required for the controller.</p> <p>The default Accounting Mode setting is <i>Off</i>.</p>
Answer Broadcast ESS	Select this checkbox to allow the WLAN to respond to probes for broadcast ESS.
Use Voice Prioritization	Select the <i>Use Voice Prioritization</i> option if Voice is used on the WLAN.
Enable SVP	Enabling SVP (<i>Spectralink Voice Prioritization</i>) allows the controller to identify and prioritize traffic from Spectralink/Polycomm phones.
Secure Beacon	Closed system is the secure beacon feature for not answering broadcast SSID. This option still allows MU to MU communication within the WLAN.
QoS Weight	Sets the Quality of Service weight for the WLAN. WLAN QoS will be applied based on the QoS weight value with the higher values given priority. The default value for the weight is 1.
MU to MU Traffic	<p>Allows frames from one MU (where the destination MAC is of another MU) are controlled to a second MU. Use the drop-down menu to select one of the following options:</p> <ul style="list-style-type: none"> • <i>Drop Packets</i>—This restricts MU to MU communication based on the WLAN’s configuration • <i>Allow Packets</i>—This allows MU to MU communication based on the WLAN’s configuration

MU Idle Time	Set the MUs idle time limit in seconds. The default value is 1800 seconds.
Access Category	Displays the Access Category for the intended traffic. The Access Categories are the different WLAN-WMM options available to the radio. The Access Category types are: <ul style="list-style-type: none"> • <i>Automatic/WMM</i>—Optimized for WMM • <i>Voice</i>—Optimized for voice traffic. Voice packets receive priority. • <i>Video</i>—Optimized for video traffic. Video packets receive priority. • <i>Normal</i>—Optimized for normal traffic • <i>Low</i>—Optimized for background traffic
MCast Addr 1	The address provided takes packets (where the first 4 bytes match the first 4 bytes of the mask) and sends them immediately over the air instead of waiting for the DTIM period. Any multicast/broadcast that does not match this mask will go out only on DTIM Intervals.
MCast Addr 2	The second address also takes packets (where the first 4 bytes match the first 4 bytes of the mask) and sends them immediately over the air instead of waiting for the DTIM period. Any multicast/broadcast that does not match this mask will go out only on DTIM Intervals.
NAC Mode	Using Network Access Control (NAC), the controller only grants access to specific network resources. NAC restricts access to only compliant and validated devices (printers, phones, PDAs, etc.), thereby limiting the risk of emerging security risks. NAC performs an authorization check for users and MUs without a NAC agent, and verifies an MU's compliance with the network security policy. The controller supports only the EAP/802.1x type of NAC. However, the controller can bypass NAC for MUs without NAC 802.1x support. For the implications of using the include and exclude with NAC, see “Configuring the NAC Inclusion List” on page 180 , “Configuring the NAC Exclusion List” on page 184 and “Configuring NAC Server Support” on page 160 .

- 10 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 11 Click the *Radius...* button (when RADIUS is selected as the accounting mode) to configure an external or internal primary and secondary RADIUS and NAC server. For more information, see [“Configuring External RADIUS Server Support” on page 155](#).
- 12 Select the *Syslog* button (when Syslog is selected as the accounting mode) to view controller syslog accounting details. To enable syslog, select the *Syslog* option from the *Accounting Mode* drop-down menu. Use this sub screen to provide the Syslog Server IP address and port for the Syslog Server performing the accounting function.
- 13 If clustering and the *Cluster GUI* feature is enabled, the *Apply to Cluster* feature will be available. Click the *Apply to Cluster* button to apply the WLAN settings to all members in the cluster.
- 14 Click *OK* to use the changes to the running configuration and close the dialog.
- 15 Click *Cancel* to close the dialog without committing updates to the running configuration.

Assigning Multiple VLANs per WLAN

The controller allows the mapping of a WLAN to more than one VLAN. When an MU associates with a WLAN, it is assigned a VLAN in such a way that users are load balanced across VLANs. The VLAN is assigned from the pool representative of the WLAN. The controller tracks the number of MUs per VLAN, and assigns the least used/loaded VLAN to the MU. This number is tracked on a per-WLAN basis.

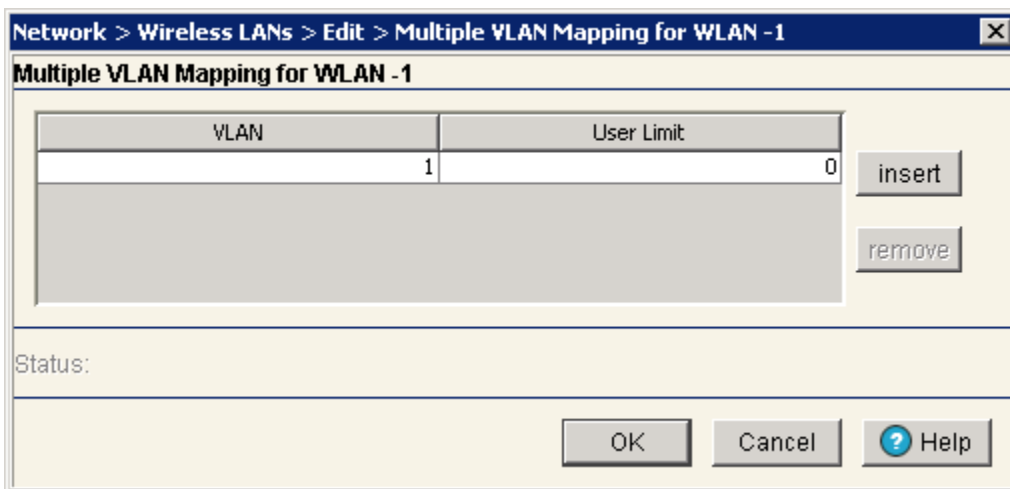
To assign multiple VLANs to a WLAN:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button. A WLAN screen displays with the WLAN's existing configuration.
- 3 Select the *VLAN* radio button from the Configuration screen to change the VLAN designation for this WLAN.

By default, all WLANs are initially assigned to VLAN 1.

- 4 Select the *Dynamic Assignment* checkbox for a user-based VLAN assignment with RADIUS for this WLAN.
- 5 Select the *Assign Multiple VLAN(s)* button to map a WLAN to more than one VLAN. This displays the Multiple VLAN Mapping screen.
- 6 Configure the *Multiple VLAN Mapping for WLAN* table as required to add or remove multiple VLANs for the selected WLAN.

Multiple VLANs per WLAN are mapped (by default) to a regular VLAN and are not supported on an adaptive AP. Refer to [“Editing the WLAN Configuration” on page 134](#) to select and define an independent VLAN for adaptive AP support.



VLAN	Displays the VLANs currently mapped to the WLAN. By default, VLAN 1 is configured for any selected WLAN.
User Limit	Displays the user limit configured for the mapped VLAN. The maximum allowed user limit is 4096 per VLAN.

- 7 Click the *Insert* button to add the VLAN using the criteria described above.
- 8 Select a row from the Multiple VLAN Mapping table and click the *Remove* button to delete the mapping of a VLAN to a WLAN.
- 9 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to use the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

**NOTE**

In a cluster environment with multiple controllers, ensure that the VLAN list is consistent across all controllers.

Configuring Authentication Types

Refer to the following to configure the WLAN authentication options available on the controller:

- [Configuring 802.1x EAP on page 142](#)
- [Configuring Kerberos on page 143](#)
- [Configuring Hotspots on page 144](#)
 - [Configuring an Internal Hotspot on page 146](#)
 - [Configuring External Hotspot on page 150](#)
 - [Configuring Advanced Hotspot on page 152](#)
- [Configuring MAC Authentication on page 154](#)

Configuring 802.1x EAP. The IEEE 802.1x standard ties the 802.1x EAP authentication protocol to both wired and wireless LAN applications.

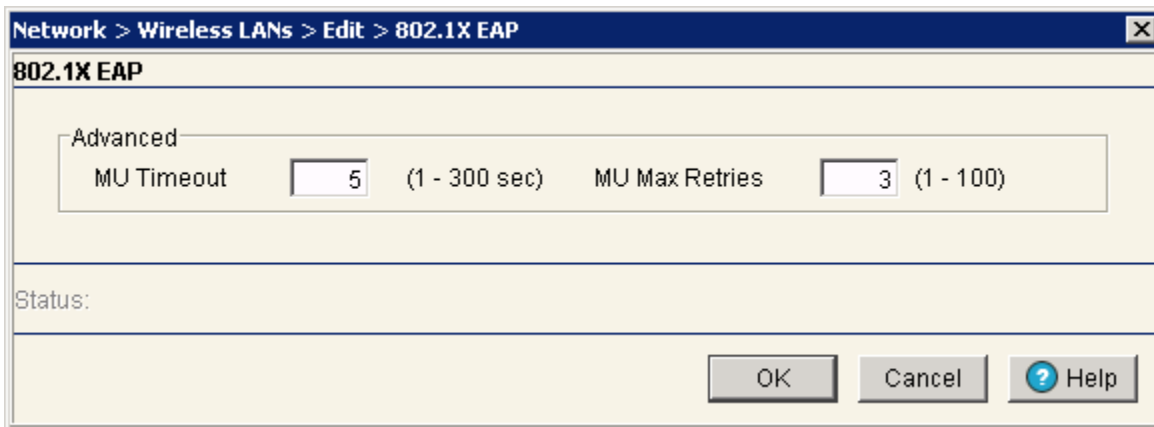
The EAP process begins when an unauthenticated supplicant (MU) tries to connect with an authenticator (in this case, the authentication server). The controller passes EAP packets from the client to an authentication server on the wired side of the controller. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the MU's identity.

**NOTE**

As part of the EAP configuration process, ensure a primary and optional secondary RADIUS server have been properly configured to authenticate the users requesting access to the EAP protected WLAN. For more information on configuring RADIUS Server support for the EAP 802.1x WLAN, see [“Configuring External RADIUS Server Support” on page 155](#).

To configure an 802.1x EAP authentication scheme for a WLAN:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button. A WLAN screen displays with the WLAN's existing configuration. Refer to the *Authentication* and *Encryption* columns to assess the WLAN's existing security configuration.
- 3 Select the *802.1X EAP* button from within the *Authentication* field. The *Radius Config...* button on the bottom of the screen will become enabled. Ensure a primary and optional secondary RADIUS Server have been configured to authenticate users requesting access to the EAP 802.1x supported WLAN. For more information, see [“Configuring External RADIUS Server Support” on page 155](#).
- 4 Click the *Config* button to the right of the 802.1X EAP checkbox. The 802.1x EAP screen displays.



- 5 Configure the *Advanced* field as required to define MU timeout and retry information for the authentication server.

MU Timeout	Define the time (between 1–60 seconds) for the controller’s retransmission of EAP-Request packets. The default is 5 seconds.
MU Max Retries	Specify the maximum number of times the controller retransmits an EAP-Request frame to the client before it times out the authentication session. The default is 3 retries, with a maximum of 100 supported.

- 6 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to use the changes to the running configuration and close the dialog.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Kerberos. Kerberos (designed and developed by MIT) provides strong authentication for client/server applications using secret-key cryptography. Using Kerberos, an MU must prove its identity to a server (and vice versa) across an insecure network connection. Once an MU and server prove their identity, they can encrypt all communications to assure privacy and data integrity.



CAUTION

Kerberos makes no provisions for host security. Kerberos assumes that it is running on a trusted host with an untrusted network. If host security is compromised, Kerberos is compromised as well.

To configure a Kerberos authentication scheme for a WLAN:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab.
- 3 Click the *Edit* button.
A WLAN screen displays with the WLAN’s existing configuration. Refer to the *Authentication* and *Encryption* columns to assess the WLAN’s existing security configuration.
- 4 Select the *Kerberos* button from within the *Authentication* field.

**NOTE**

Kerberos requires at least one encryption scheme be enabled (WEP 128 or other). If neither WEP 128 or KeyGuard is enabled, WEP 128 will automatically be enabled for use with Kerberos.

- Click the *Config...* button to the right of the Kerberos checkbox. The *Kerberos* screen displays.

Kerberos			
Realm Name	<input type="text"/>		
Password	<input type="password"/>		
	Primary KDC	Backup KDC	
Server IP Addr	<input type="text" value="0 . 0 . 0 . 0"/>	<input type="text" value="0 . 0 . 0 . 0"/>	
Port	<input type="text" value="88"/>	<input type="text" value="88"/>	
Status:	<input type="text"/>		

- Specify a case-sensitive *Realm Name*.

The realm name is the name domain/realm name of the KDC Server. A realm name functions similarly to a DNS domain name. In theory, the realm name is arbitrary. However, in practice a Kerberos realm is named by uppercasing the DNS domain name associated with hosts in the realm.

- Provide the password required to effectively update Kerberos authentication credentials.

- Enter a *Server IP Addr* (IP address) for the Primary and (if necessary) Backup KDC.

Specify a numerical (non-DNS) IP address for the Primary *Key Distribution Center* (KDC). The KDC implements an Authentication Service and a Ticket Granting Service, whereby an authorized user is granted a ticket encrypted with the user's password. The KDC has a copy of every user password provided. Optionally, specify a numerical (non-DNS) IP address for a backup KDC. Backup KDCs are often referred to as slave servers.

- Specify the *Ports* on which the Primary and Backup KDCs reside.

The default port number for Kerberos Key Distribution Centers is port 88.

- Refer to the *Status* field for the current state of requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

- Click *OK* to use the changes to the running configuration and close the dialog.

- Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Hotspots. A hotspot is essentially a Web page granting user access to the Internet (in this case within a controller managed WLAN). With the influx of Wi-Fi enabled mobile devices (laptops, PDAs, etc.), hotspots are common and can be found at many airports, hotels, and college campuses.

The controller enables hotspot operators to provide user authentication and accounting without a special client application. The controller uses a traditional Internet browser as a secure authentication device. Rather than rely on built-in 802.11 security features to control association privileges, configure a WLAN with no WEP (an open network). The controller issues an IP address using a DHCP server, authenticates the user, and grants the user access to the Internet.

The hotspot feature supports both internal and external RADIUS servers. It also supports the following three HTTP redirection options to satisfy various customer configurations:

- Simple internal pre-built Web-pages.
- External Web-pages
- Customized internal Web page (using the Advanced feature in hotspot configuration)

When a user visits a public hotspot and wants to browse a Web page, they can boot up their laptop and associate with the local Wi-Fi network by entering the correct SSID. They then start a browser. The hotspot access controller forces this un-authenticated user to a Welcome page from the hotspot Operator that allows the user to log in with a username and password. This form of IP-Redirection requires no special software on the client.

To configure a hotspot, create a WLAN ESSID and select Hotspot as the authentication scheme from the WLAN Authentication menu. This is simply another way to authenticate a WLAN user, as it would be impractical to authenticate visitors using 802.1x authentications. Having enabled a hotspot, you will need to configure it. There are two parts to the hotspot configuration process:

- Setting up the Hotspot Web pages
- Setting up the RADIUS server.

Controller Hotspot Redirection. The controller uses destination network address translation to redirect user traffic from a default home page to the login page. Specifically, when the controller receives an HTTP Web page request from the user (when the client first launches its browser after connecting to the WLAN), a protocol stack on the controller intercepts the request and sends back an HTTP response after modifying the network and port address in the packet (thereby acting like a proxy between the User and the website they are trying to access).

To configure hotspot support:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button.
A WLAN screen displays with the WLAN's existing configuration. Refer to the *Authentication* and *Encryption* columns to assess the WLAN's existing security configuration.
- 3 Select the *Hotspot* button from within the *Authentication* field. The *Radius Config...* button on the bottom of the screen becomes enabled. Ensure a primary and optional secondary RADIUS Server have been configured to authenticate users requesting access to the hotspot supported WLAN. For more information, see "[Configuring External RADIUS Server Support](#)" on page 155.
- 4 Click the *Config* button to the right of the Hotspot checkbox.
A *Hotspot* screen displays, allowing the user to define one of the three available hotspot types.
- 5 Use the drop-down menu at the top of the screen to define whether this WLAN's Web pages are:
 - *Internal*—five HTML pages with basic functionality are made available on the switch's onboard HTTP server. The HTML pages are pre-created to collect login credentials through *Login.htm*, send them to a Radius server and display a *Welcome.htm* or a *Faliure.htm* depending on the result of the authentication attempt. If there is a disruption in service or connection to the wireless controller is lost for any reason, a *NoService.htm* page is displayed. For more information, see "[Configuring an Internal Hotspot](#)" on page 146.
 - *External*—a customer may wish to host their own external Web server using advanced Web content (using XML, Flash). Use the *External* option to point the controller to an external hotspot. For more information, see "[Configuring External Hotspot](#)" on page 150.
 - *Advanced*—a customer may wish to use advanced Web content (XML, Flash) but might not have (or would not want to use) an external Web server, choosing instead to host the Web pages on the

controller's HTTP Web server. Selecting the Advanced option allows for the importing the Web pages from an external source (like an FTP server) and hosting them on the controller. For more information, see [“Configuring Advanced Hotspot” on page 152](#).

**NOTE**

The appearance of the Hotspot screen differs depending on which option is selected from the drop-down menu. You may want to research the options available before deciding which hotspot option to select.

**NOTE**

As part of the hotspot configuration process, ensure a primary and optional secondary RADIUS Server have been properly configured to authenticate the users requesting access to the hotspot supported WLAN. For more information on configuring RADIUS Server support for the hotspot-supported WLAN, see [“Configuring External RADIUS Server Support” on page 155](#).

Configuring an Internal Hotspot. Using the Internal option means the user develops the hotspot using the three HTML pages made available on the controller's onboard HTTP server. The HTML pages are pre-created to collect login credentials through Login.htm, send them to a RADIUS server and display a Welcome.htm or a Faliure.htm depending on the result of the authentication attempt.

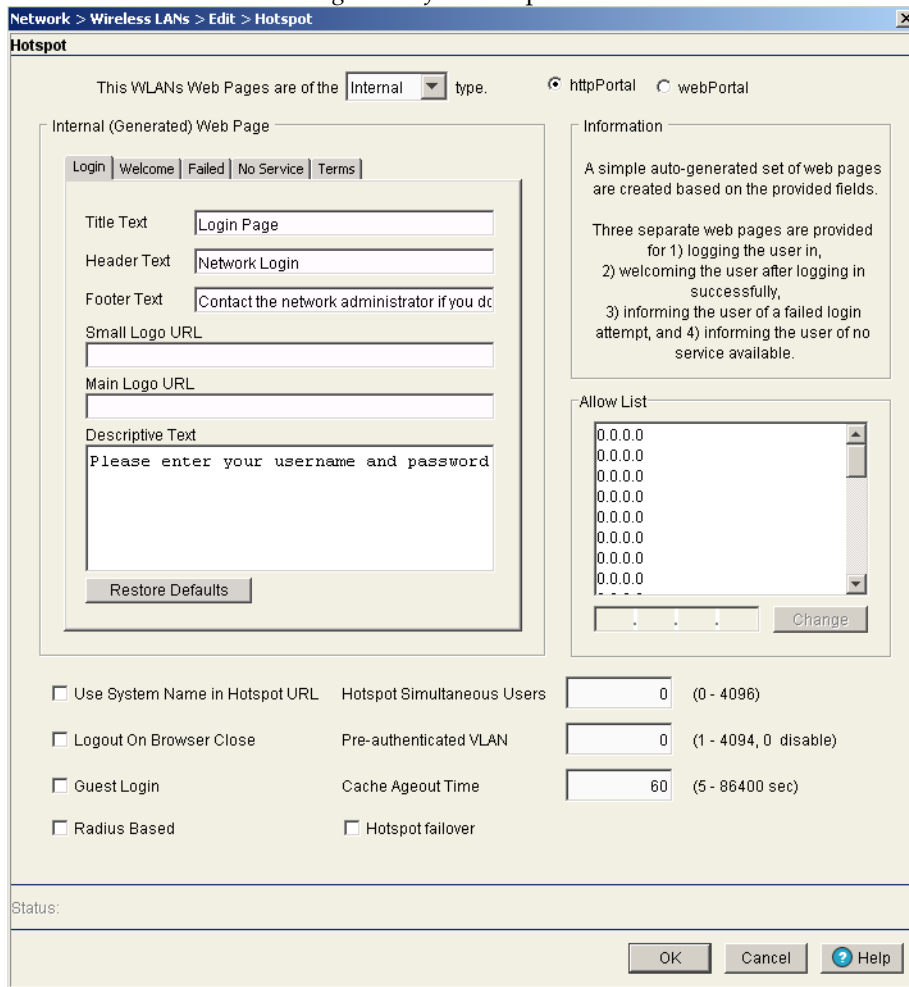
**NOTE**

When using an internal hotspot, ensure that traffic can pass on TCP port 444 between the controller's internal webserver and the hotspot clients.

To create a hotspot maintained by the controller's own internal resources:

- 1 Select *Network > Wireless LANs* from the main menu tree. Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button.

- 3 Select the *Hotspot* button from within the *Authentication* field. Ensure *Internal* is selected from within the *This WLAN's Web Pages are of the* drop-down menu.



- 4 Click the *Login* tab and enter the title, header, footer Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when users log in to the controller-maintained hotspot.

Title Text	Displays the HTML text displayed on the Welcome page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Header Text	Displays the HTML header displayed on the Failed page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Footer Text	Displays the HTML footer text displayed on the Failed page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Small Logo URL	Displays the URL for a small logo image displayed on the Failed page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Main Logo URL	Displays the URL for the main logo image displayed on the Failed page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.

Descriptive Text	Specify any additional text containing instructions or information for the users who access the Failed page. This option is only available if <i>Internal</i> is chosen from the drop-down menu above. The default text is: "Either the username and password are invalid, or service is unavailable at this time."
------------------	---

- 5 Click the *Welcome* tab and enter the title, header, footer Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when users successfully authenticate with the controller-maintained hotspot.

Title Text	The Title Text specifies the HTML title text displayed on the Welcome page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
------------	--

Header Text	The Header Text is the HTML header text displayed on the Welcome page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
-------------	---

Footer Text	The Footer Text is the HTML footer text displayed on the Welcome page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
-------------	---

Small Logo URL	The Small Logo URL is the URL for a small logo image displayed on the Welcome page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
----------------	--

Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on the Welcome page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
---------------	--

Descriptive Text	Specify any additional text containing instructions or information for the users who access the Welcome page on the internal Web server. This option is only available if <i>Internal</i> is chosen from the pull-down menu above. The default text is: "You now have network access. Click the disconnect link on right when you want to end this session."
------------------	--

- 6 Click the *Failed* tab and enter the title, header, footer Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when users fail authentication with the controller-maintained hotspot.

Title Text	The Title Text is the HTML title displayed on the Failed page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
------------	---

Header Text	The Header Text specifies the HTML header displayed on the Failed page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
-------------	--

Footer Text	The Footer Text is the HTML footer text displayed on the Failed page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
-------------	--

Small Logo URL	The Small Logo URL is the URL for a small logo image displayed on the Failed page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
----------------	---

Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on the Failed page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
---------------	---

Descriptive Text	Specify any additional text containing instructions or information for the users who access the Failed page on the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above. The default text is: "Either the username and password are invalid, or service is unavailable at this time."
------------------	--

-
- 7 Click the *No Service* tab and enter the title, header, footer Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when the AP loses connection with the wireless controller or with the AAA server.

Title Text	The Title Text is the HTML title displayed on the No Service page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Header Text	The Header Text specifies the HTML header displayed on the No Service page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Footer Text	The Footer Text is the HTML footer text displayed on the No Service page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Small Logo URL	The Small Logo URL is the URL for a small logo image displayed on the No Service page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on the No Service page when using the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Descriptive Text	Specify any additional text containing instructions or information for the users who access the No Service page on the internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above. The default text is: "Service is unavailable at this time."

- 8 Click the *Terms* tab to set the terms and conditions for display to the user.

Title Text	Specifies the terms and conditions title.
Descriptive Text	Defines the terms and conditions.

- 9 Click the *Restore Defaults* button to revert to the default settings in the Internal (Generated) Web Page.

- 10 Refer to the *Allow List* field, and enter any IP address (for internal or external websites) that may be accessed by the Hotspot user without authentication.



NOTE

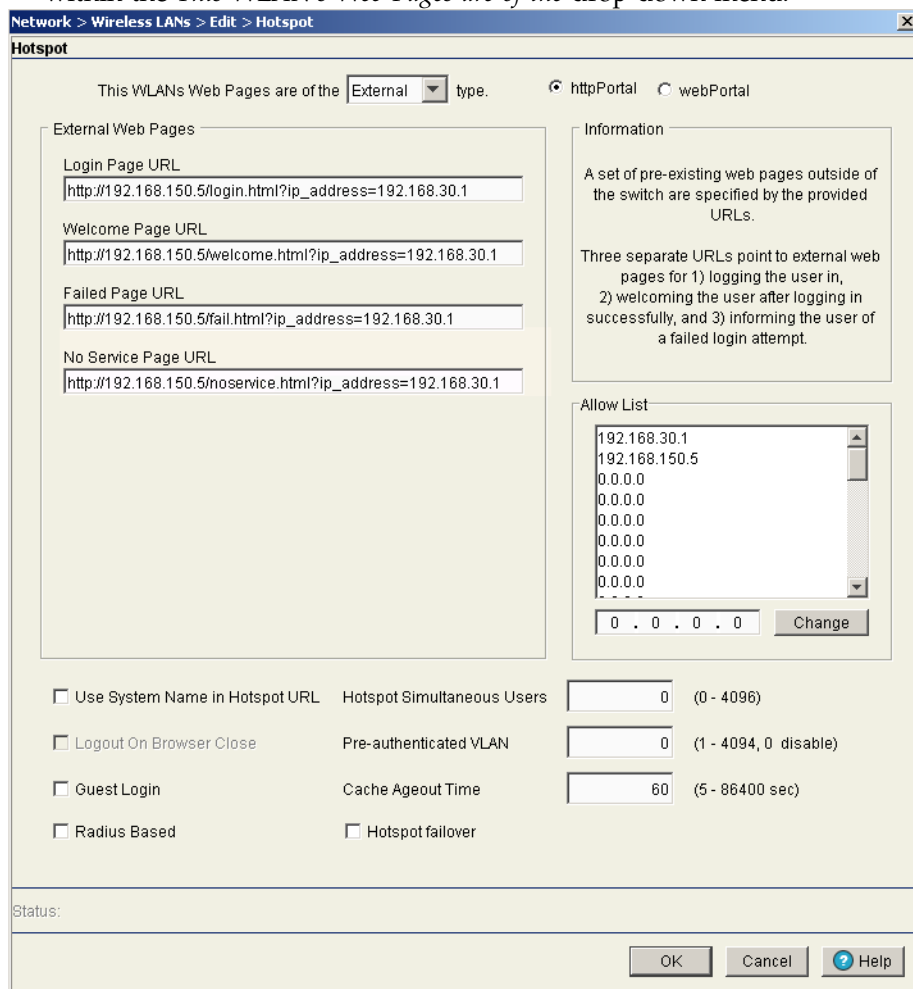
In multi-controller hotspot environments if a single controller's internal pages are configured for authentication on the other controllers, those controllers will redirect to their own internal pages instead. In these environments, it is recommended to use an external server for all of the controllers.

- 11 Check the *Use System Name in Hotspot URL* to use the *System Name* specified on the main Controller configuration screen as part of the hotspot address.
- 12 Check the *Logout on Browser Close* button to log out hotspot users from the network when they close their web browsers.
- 13 Specify the maximum *Hotspot Simultaneous Users* to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
- 14 Enter a value in the *Pre-authenticated VLAN* field to configure a default VLAN to be used until the user gets authorized. Specify the VLAN within the range <1-4096>.
- 15 Enter a value in seconds in the *Cache Ageout Time* field. This is the time in seconds to age out the hotspot data ready state after the MU disassociation.
- 16 Check the *Guest Login* checkbox to allow the guest login option.
- 17 Check the *Radius Based* checkbox to provide the user a radius authenticated login option. When unchecked, RADIUS authentication is not available for hotspot user validation.

- 18 Check the *Hotspot failover* checkbox to enable the hotspot failover option. Hotspot failover is a feature that displays the No Service page when an authentication server/a critical resource is not available when a user tries to access resources using the hotspot.
- 19 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller. Click *OK* to use the changes to the running configuration and close the dialog.
- 20 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring External Hotspot. Selecting the external option entails hosting your own external Web server using advanced Web content (using XML, Flash). To create a hotspot maintained by an external server:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button.
- 3 Select the *Hotspot* button from within the Authentication field. Ensure *External* is selected from within the *This WLAN's Web Pages are of the* drop-down menu.



- 4 Refer to the *External Web Pages* field and provide the Login, Welcome, and Failed Page URLs used by the external Web server to support the hotspot.

Login Page URL	<p>Define the complete URL for the location of the Login page. The Login screen will prompt the hotspot user for a username and password to access the Welcome page. For example, the Login page URL can be the following:</p> <p><code>http://192.168.150.5/login.html?ip_address=192.168.30.1</code>. Here, 192.168.150.5 is the Web server IP address and 192.168.30.1 is the controller IP address.</p>
Welcome Page URL	<p>Define the complete URL for the location of the Welcome page. The Welcome page assumes that the hotspot user has logged in successfully and can access the Internet. Ensure that RADIUS server port number is included in the URL using the following format:</p> <p><code>https://192.168.0.70:444/wlan2/login.html</code></p>
Failed Page URL	<p>Define the complete URL for the location of the Failed page. The Failed screen assumes that the hotspot authentication attempt has failed, you are not allowed to access the Internet and you need to provide correct login information to access the Web. Ensure that RADIUS server port number is included in the URL using the following format:</p> <p><code>https://192.168.0.70:444/wlan2/login.html</code></p>
No Service Page URL	<p>Define the complete URL for the location of the No Service page. The No Service page assumes that the hotspot user has logged in successfully. This page is displayed when the AP is disconnected from a critical resource such as its AAA server or the wireless controller to which it is adopted. For example, the No Service page URL can be the following:</p> <p><code>http://192.168.150.5/noservice.html?ip_address=192.168.30.1</code>. Here, 192.168.150.5 is the Web server IP address and 192.168.30.1 is the switch IP address.</p>

- 5 Refer to the *Allow List* field, and enter any IP address (for internal or external websites) that may be accessed by the Hotspot user without authentication.



NOTE

When using hotspot features in a cluster environment, additional steps must be taken when specifying the external URLs. In order for the browser to return the login information correctly, the IP address and port must be specified as part of the URL in the following format:

`http://external_url<login | welcome | fail>.html?ip_address=a.b.c.d&port=x`

- 6 Check the *Use System Name in Hotspot URL* to use the *System Name* specified on the main Controller configuration screen as part of the hotspot address.
- 7 Specify the maximum *Hotspot Simultaneous Users* to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
- 8 Check the *Logout on Browser Close* button to logout hotspot users from the network when they close their web browsers.
- 9 Enter a value in the *Pre-authenticated VLAN* field to configure a default VLAN to be used until the user gets authorized. Specify the VLAN within the range <1-4096>.
- 10 Enter a value in seconds in the *Cache Ageout Time* field. This is the time in seconds to age out the hotspot data ready state after the MU disassociation.
- 11 Check the *Guest Login* checkbox to allow the guest login option.
- 12 Check the *Radius Based* checkbox to provide the user a radius authenticated login option.
- 13 Check the *Hotspot failover* checkbox to enable the hotspot failover option.

- 14 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 15 Click *OK* to use the changes to the running configuration and close the dialog.
- 16 Click *Cancel* to close the dialog without committing updates to the running configuration.



NOTE

While using the External web pages option:

- Configure the Internal Web pages for a particular WLAN.
 - Copy the Internal Web pages corresponding to the WLAN from the controller to the external Web server.
 - Change the WLAN Web pages option from “Internal” to “External”.
 - Enter the URL of the external Web server in the “Login Page URL”, “Welcome Page URL”, and “Failed Page URL” fields of the External Web pages screen.
-

Configuring Advanced Hotspot. A customer may wish to use advanced Web content (XML, Flash) but might not have (or would not want to use) an external Web server, choosing instead to host the Web pages on the controller's HTTP Web server. Selecting the *Advanced* option allows for importing the Web pages from an external source (like an FTP server) and hosting them on the controller.

To use the Advanced option to define the hotspot:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab.
- 3 Click the *Edit* button.
- 4 Select the *Hotspot* button from within the *Authentication* field.

Ensure *Advanced* is selected from within the *This WLAN's Web Pages are of the* drop-down menu.

Network > Wireless LANs > Edit > Hotspot

Hotspot

This WLAN's Web Pages are of the **Advanced** type. httpPortal webPortal

Advanced Web-Auth Pages

Advanced Hotspot must be configured using either the CLI or other advanced operation. See your documentation for more details about setting up Advanced Hotspot web pages.

Information

A custom-developed directory full of web page content, including subdirectories, can be copied in and out of the switch. File transfers occur immediately (not when "OK" is pressed).

There are minimal requirements that the custom web pages must comply with in order to work. Refer to this device's documentation for more details.

Source

File:

Using: **FTP** Port:

IP Address:

User ID:

Password:

Path:

Install

Allow List

0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0

Change

Use System Name in Hotspot URL Hotspot Simultaneous Users: (0 - 4096)

Logout On Browser Close Pre-authenticated VLAN: (1 - 4094, 0 disable)

Guest Login Cache Ageout Time: (5 - 86400 sec)

Radius Based Hotspot failover

Status:

OK **Cancel** **Help**

Once the properties of the advanced hotspot have been defined, the file can be installed on the controller and used to support the hotspot. The following parameters are required to upload the file:

- a Specify a source hotspot configuration file. The file used at startup automatically displays within the *File* parameter.
 - b Refer to the *Using* drop-down menu to configure whether the hotspot file transfer is conducted using FTP or TFTP.
 - c Enter the *IP Address* of the server or system receiving the source hotspot configuration. Ensure that the IP address is valid or risk jeopardizing the success of the file transfer.
 - d If using FTP, enter the *User ID* credentials required to transfer the configuration file from an FTP server.
 - e If using FTP, enter the *Password* required to send the configuration file from an FTP server.
 - f Specify the appropriate *Path* name to the hotspot configuration on the local system disk or server.
 - g Once the location and settings for the advanced hotspot configuration have been defined, click the *Install* button to use the hotspot configuration with the controller.
- 5 Refer to the *Allow List* field, and enter any IP address (for internal or external websites) that may be accessed by the Hotspot user without authentication.

- 6 Check the *Use System Name in Hotspot URL* to use the *System Name* specified on the main Controller configuration screen as part of the hotspot address.
- 7 Specify the maximum *Hotspot Simultaneous Users* to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
- 8 Check the *Logout on Browser Close* button to log out hotspot users from the network when they close their web browsers.
- 9 Enter a value in the *Pre-authenticated VLAN* field to configure a default VLAN to be used until the user gets authorized. Specify the VLAN within the range <1-4096>.
- 10 Enter a value in seconds in the *Cache Ageout Time* field. This is the time in seconds to age out the hotspot data ready state after the MU disassociation.
- 11 Check the *Guest Login* checkbox to allow the guest login option.
- 12 Check the *Radius Based* checkbox to provide the user a radius authenticated login option.
- 13 Check the *Hotspot failover* checkbox to enable the hotspot failover option.
- 14 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 15 Click *OK* to use the changes to the running configuration and close the dialog.
- 16 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring MAC Authentication. The MAC Authentication option allows the user to configure a RADIUS server for user authentication with the range of MAC addressees defined as allowed or denied access to the controller managed network.



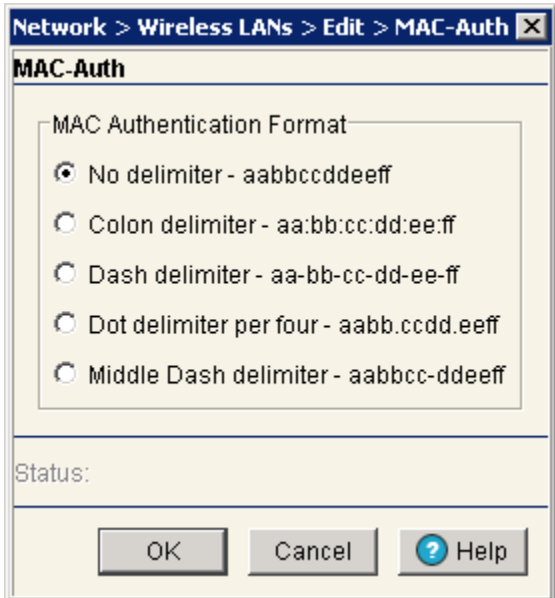
NOTE

As part of the MAC Authentication process, ensure a primary and optional secondary RADIUS Server have been properly configured to authenticate the users requesting access to the ACL supported WLAN. For more information on configuring RADIUS Server support for the MAC Authentication supported WLAN, see [“Configuring External RADIUS Server Support” on page 155](#).

To configure the format of MAC addresses used in MAC Authentications:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab.
- 3 Click the *Edit* button.
- 4 Select the *MAC Authentication* button from within the Authentication field.
This enables the *Radius* button at the bottom of the *Network > Wireless LANs > Edit* screen.

- 5 Click the Config button next to the *MAC Authentication* option to open a dialogue where the format of MAC Addresses can be configured.



The MAC Authentication Format setting determines the text format that MAC addresses are transmitted when using MAC-Auth authentication

- 6 Select a format for MAC Addresses used in MAC Authentication:
 - *No delimiter*: The 12 digit MAC Address is in a format with no spaces or delimiters.
 - *Colon delimiter*: The 12 digit MAC Address is in a format separated by colons after every pair.
 - *Dash delimiter*: The 12 digit MAC Address is in a format separated by dashes after every pair.
 - *Dot delimiter per four*: The 12 digit MAC Address is in a format separated by periods after every four digits.
 - *Middle Dash delimiter*: The 12 digit MAC Address is in a format separated in the middle by a dash.
- 7 Click *OK* to use the changes to the running configuration and close the dialog.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring External RADIUS Server Support. If either the EAP 802.1x, Hotspot, or Dynamic MAC ACL options have been selected as an authentication scheme for a WLAN, the *Radius Config...* button at the bottom of the Network > Wireless LANs > Edit becomes enabled. The *Radius Configuration* screen provides users the option of defining an external primary and secondary RADIUS Server as well as a NAC Server if you do not use the controller’s resident RADIUS Server.



NOTE

If using the controller’s local RADIUS Server for user authentication instead of an external primary or secondary RADIUS Server, see [“Configuring the RADIUS Server” on page 489](#). The controller’s local RADIUS Server provides an easy setup option and offers a high degree of security and accountability.

The controller ships with a default configuration defining the local Radius Server as the primary authentication source (default users are admin with superuser privileges and operator with monitor privileges). No secondary authentication source is specified. However, Extreme Networks recommends using an external Radius Server as the primary user authentication source and the local controller

Radius Server as the secondary user authentication source. To use an external Radius Server as either a primary or secondary authentication source, it must be specified appropriately.

To configure an external RADIUS Server for EAP 802.1x, Hotspot, or Dynamic MAC ACL WLAN support:



NOTE

To optimally use an external RADIUS Server with the controller, Extreme Networks recommends defining specific external Server attributes to best utilize user privilege values for specific controller permissions. For information on defining the external RADIUS Server configuration, see [“Configuring an External RADIUS Server for Optimal Controller Support”](#) on page 159.

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab.
- 3 Click the *Edit* button.
- 4 Select either the *EAP 802.1x*, *Hotspot*, or *Dynamic MAC ACL* button from within the *Authentication* field. This enables the *Radius...* button at the bottom of the *Network > Wireless LANs > Edit* screen.

- 5 Select the *Radius...* button. The *Radius Configuration* screen displays for defining an external RADIUS or NAC Server.

Radius Configuration

Radius and NAC Configuration

Radius | NAC

	Primary	Secondary
RADIUS Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
RADIUS Port	1812	1812
RADIUS Shared Secret	*****	*****
Server Timeout	5 (1-300 secs)	
Server Retries	3 (1-100 retries)	<input type="checkbox"/> Dynamic Authorization

Enable radius proxy

Realm Name Strip Realm

Accounting

	Primary	Secondary
Accounting Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
Accounting Port	1813	1813
Accounting Shared Secret	*****	*****
Accounting Timeout	5 (1-300 secs)	
Accounting Retries	6 (1-100 retries)	
Accounting Mode	Start-Stop	Interval <input type="text" value="60"/>

Re-authentication

Re-authentication Period (30-65535 sec)

Advanced

Authentication Protocol PAP CHAP DSCP/TOS

Status:

OK Cancel Help

The *Radius Configuration* screen contains tabs for defining both the RADIUS and NAC server settings. For NAC overview and configuration information, see [“Configuring NAC Server Support”](#) on page 160.

- 6 Refer to the *Server* field and define the following credentials for a primary and secondary RADIUS server.

RADIUS Server Address	Enter the IP address of the primary and secondary server acting as the RADIUS user authentication data source.
RADIUS Port	Enter the TCP/IP port number for the primary and secondary server acting as the RADIUS user authentication data source. The default port is 1812.
RADIUS Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary RADIUS server.
Server Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the controller to time out on a request to the primary or secondary server.
Server Retries	Enter a value between 1 and 100 to indicate the number of times the controller attempts to reach the primary or secondary RADIUS server before giving up.
Dynamic Authorization	Check this option to enable the RADIUS Dynamic Authorization function. RADIUS Dynamic Authorization enables the administrator to send the disconnect and change of authorization packets to the controller (NAS) for wired hosts.

**NOTE**

The RADIUS or NAC server's Timeout and Retries should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fall back to the secondary server will not work.

- 7 Refer to the *Accounting* field and define the following credentials for a primary and secondary RADIUS Server.

Accounting Server Address	Enter the IP address of the primary and secondary server acting as the RADIUS accounting server.
Accounting Port	Enter the TCP/IP port number for the primary and secondary server acting as the RADIUS accounting data source. The default port is 1813.
Accounting Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary RADIUS accounting server.
Accounting Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the controller to time out a request to the primary or secondary accounting server.
Accounting Retries	Enter a value between 1 and 100 to indicate the number of times the controller attempts to reach the primary or secondary RADIUS accounting server before giving up.
Accounting Mode	Use the Accounting Mode drop-down menu to define the accounting mode as either Start-Stop, Stop Only, or Start-Interim-Stop. Define the interval (in seconds) used with the selected accounting mode.

- 8 Select the *Re-authentication* checkbox to force a periodic re-authentication with the RADIUS server. Periodic repetition of the authentication process provides ongoing security for currently authorized connections. Define an interval between 30 and 65535 seconds.
- 9 Refer to the *Advanced* field to define the authentication protocol used with the RADIUS Server.

PAP	PAP— <i>Password Authentication Protocol</i> sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized.
-----	---

CHAP	CHAP is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
DSCP/TOS	Optionally mark packets with a <i>DiffServ CodePoint</i> (DSCP) in its header. The DSCP value is stored in the first 6 bits of the Type of Service (ToS) field that is part of the standard IP header. The DCSP values are associated with a forwarding treatment called <i>Per Hop Behaviors</i> (PHB). Service can be provisioned (if necessary) by assigning a DCSP point code from 1–6.

- 10 Click *OK* to save the changes made to this screen.
- 11 Click *Cancel* to revert back to the last saved configuration and move back to the *Network > Wireless LANs > Edit* screen.

Configuring an External RADIUS Server for Optimal Controller Support. The controller's external RADIUS Server should be configured with Extreme Networks Controller specific attributes to best utilize the user privilege values assignable by the RADIUS Server. The following two values should be configured on the external Server for optimal use with the controller:

- Extreme Networks user privilege values
- User login source

Configuring Extreme Networks Specific RADIUS Server User Privilege Values. The following recommended RADIUS Server user privilege settings specify access privilege levels for those accessing the controller managed network. To define user privilege values, assign the following attributes in the external RADIUS Server:

- 1 Set the attribute number to 1 and its type as "integer."
- 2 Define the following possible decimal values for user access permissions:
 - a Set the *Monitor Role* value to 1 (read-only access to the controller).
 - b Set the *Helpdesk Role* value to 2 (helpdesk/support access to the controller).
 - c Set the *Nwadmin Role* value to 4 (wired and wireless access to the controller).
 - d Set the *Sysadmin Role* value to 8 (system administrator access).
 - e Set the *WebAdmin Role* value to 16 (guest user application access).
 - f Set the *Superuser Role* value to 32768 (grants full read/write access to the controller).
- 3 Specify multiple privileges (for a single user) by specifying different attributes as needed. The privilege values can be *ORed* and specified once. For example, if a user needs monitor (read-only) and helpdesk access, configure the RADIUS Server with two attributes. Once with a value 1 for monitor access and then with a value 2 for the helpdesk role.
Multiple roles can also be defined by configuring the RADIUS Server with attribute 1 and value 3 (or monitor value 1 and helpdesk value 2).



NOTE

If user privilege attributes are not defined for the RADIUS Server, users will be authenticated with a default privilege role of 1 (Monitor read-only access).

Configuring the User Login Sources. The following recommended RADIUS Server user login sources specify the location (ssh/telnet/console/Web) from which users are allowed controller access. If login access permissions are not defined (restricted), users will be allowed to log in from each interface.

To define login source access locations:

- 1 Set the attribute number to 100 and its type as “integer.”
- 2 Define the following possible decimal values for login sources:
 - a Set the *Console Access* value to 128 (user is allowed login privileges only from console).
 - b Set the *Telnet Access* value to 64 (user is allowed login privileges only from a Telnet session).
 - c Set the *SSH Access* value to 32 (user is allowed login privileges only from ssh session).
 - d Set the *Web Access* value to 16 (user is allowed login privileges only from Web/applet).
- 3 Specify multiple access sources by using different values. The privilege values can be ORed and specified once. For example, if a user needs access from both the console and Web, configure the RADIUS Server with the 100 attribute twice, once with value 128 for console, and next with value 16 for Web access.

Configuring NAC Server Support. There is an increasing proliferation of insecure devices (laptops, mobile computers, PDA, smart-phones, etc.) accessing WiFi networks. These devices often lack proper anti-virus software and can potentially infect the network they access. Device compliance per an organization’s security policy must be enforced using NAC. A typical security compliance check entails verifying the right operating system patches, anti-virus software, etc.

NAC is a continuous process for evaluating MU credentials, mitigating security issues, admitting MUs to the network, and monitoring MUs for compliance with globally-maintained standards and policies. If an MU is not in compliance, network access is restricted by quarantining the MU.

Using NAC, the controller hardware and software grants access to specific network devices. NAC performs a user and MU authorization check for devices without a NAC agent. NAC verifies an MU’s compliance with the controller’s security policy. The controller supports only EAP/802.1x NAC. However, the controller provides a mean to bypass NAC authentication for MUs without NAC 802.1x support (printers, phones, PDAs, etc.).

For a NAC configuration example using the controller CLI, see [“Configuring the NAC Inclusion List” on page 180](#) or [“Configuring the NAC Exclusion List” on page 184](#).

- *None*—NAC disabled, no NAC is conducted. An MU can only be authenticated by a RADIUS server.
- *Do NAC except exclude list*—An MU NAC check is conducted except for those in the exclude-list. Devices in the exclude-list will not have any NAC checks.
- *Bypass NAC except include list*—An MU NAC check is conducted only for those MUs in the include-list.

To configure NAC Server support:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed with the *Configuration* tab.
- 3 Click the *Edit* button.
- 4 Select either the *EAP 802.1x*, *Hotspot*, or *Dynamic MAC ACL* button from within the *Authentication* field.

This enables the *Radius* button at the bottom of the *Network > Wireless LANs > Edit* screen.

- 5 Click the *Radius* button.

The *Radius Configuration* screen displays (with the *Radius* tab displayed by default) for defining an external RADIUS or NAC Server.

- 6 Select the NAC tab to configure NAC support.

Radius Configuration

Radius and NAC Configuration

Radius | **NAC**

	Primary	Secondary
NAC Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
NAC Server Port	1812	1812
NAC Shared Secret	*****	*****
Server Timeout	5 (1-300 secs)	
Server Retries	3 (1-100 retries)	

Enable radius proxy

Realm Name Strip Realm

Accounting

	Primary	Secondary
Accounting Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
Accounting Port	1813	1813
Accounting Shared Secret	*****	*****
Accounting Timeout	5 (1-300 secs)	
Accounting Retries	6 (1-100 retries)	
Accounting Mode	Start-Stop	Interval
		60

Re-authentication

Re-authentication Period 3600 (30-65535 sec)

Advanced

Authentication Protocol PAP CHAP DSCP/TOS 0

Status:

OK Cancel ? Help

- 7 Refer to the *Server* field and define the following credentials for a primary and secondary NAC server.

NAC Server Address Enter the IP address of the primary and secondary NAC server.

NAC Server Port	Enter the TCP/IP port number for the primary and secondary server. The default port is 1812.
NAC Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary NAC server.
Server Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the controller to time out on a request to the primary or secondary NAC server.
Server Retries	Enter a value between 1 and 100 to indicate the number of times the controller attempts to reach the primary or secondary server before giving up.



CAUTION

The server's Timeout and Retries should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fall back to the secondary server will not work.

8 Refer to the *Accounting* field and define the following credentials for a primary and secondary NAC Server.

Accounting Server Address	Enter the IP address of the primary and secondary server acting as the NAC accounting server.
Accounting Port	Enter the TCP/IP port number for the primary and secondary server acting as the NAC accounting data source. The default port is 1813.
Accounting Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary NAC accounting server.
Accounting Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the controller to time out a request to the primary or secondary accounting server.
Accounting Retries	Enter a value between 1 and 100 to indicate the number of times the controller attempts to reach the primary or secondary NAC accounting server before giving up.
Accounting Mode	Use the <i>Accounting Mode</i> drop-down menu to define the accounting mode as either <i>Start-Stop</i> , <i>Stop Only</i> , or <i>Start-Interim-Stop</i> . Define the interval (in seconds) used with the selected accounting mode.

9 Select the *Re-authentication* checkbox to force a periodic re-authentication with the NAC server.

Periodic repetition of the authentication process provides ongoing security for currently authorized connections. Define an interval between 30 and 65535 seconds.

10 Refer to the *Advanced* field to define the authentication protocol used with the NAC Server.

PAP	PAP— <i>Password Authentication Protocol</i> sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized.
CHAP	CHAP is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
DSCP/TOS	Optionally mark packets with a <i>DiffServ CodePoint</i> (DSCP) in its header. The DSCP value is stored in the first 6 bits of the Type of Service (ToS) field that is part of the standard IP header. The DCSP values are associated with a forwarding treatment called <i>Per Hop Behaviors</i> (PHB). Service can be provisioned (if necessary) by assigning a DCSP point code from 1–6.

-
- 11 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
 - 12 Click *OK* to use the changes to the running configuration and close the dialog.
 - 13 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Different Encryption Types

To configure the WLAN data encryption options available on the controller, refer to the following:

- [Configuring WEP 64 on page 163](#)
- [Configuring WEP 128 / KeyGuard on page 165](#)
- [Configuring WPA/WPA2 using TKIP and CCMP on page 166](#)

Configuring WEP 64. *Wired Equivalent Privacy (WEP)* is a security protocol specified in the *IEEE Wireless Fidelity (Wi-Fi)* standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP 64 is a less robust encryption scheme than WEP 128 (shorter WEP algorithm for a hacker to duplicate), but WEP 64 may be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP 64:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button.
A WLAN screen displays with the WLAN's existing configuration. Refer to the *Authentication* and *Encryption* columns to assess the WLAN's existing security configuration.
- 3 Select the *WEP 64* button from within the *Encryption* field.
- 4 Click the *Config* button to the right of the WEP 64 checkbox.

The WEP 64 screen displays.

- 5 Specify a 4 to 32 character *Pass Key* and click the *Generate* button.

The pass key can be any alphanumeric string. The controller, other routers, and MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Extreme Networks adapters need to use WEP keys manually configured as hexadecimal numbers.

- 6 Use the *Key #1-4* areas to specify key numbers.

The key can be either a hexadecimal or ASCII. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length or 5 ASCII characters. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for WEP 64 include:

Key 1	1011121314
Key 2	2021222324
Key 3	3031323334
Key 4	4041424344

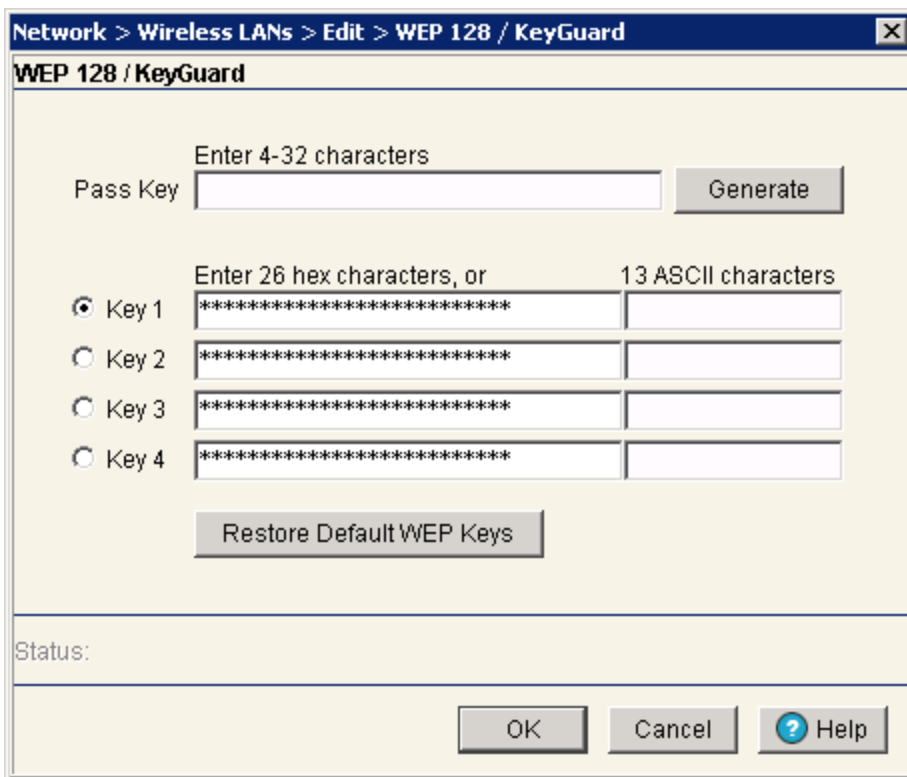
- 7 If you feel it necessary to restore the WEP algorithm back to its default settings, click the *Restore Default WEP Keys* button. This may be the case if you feel that the latest defined WEP algorithm has been compromised and no longer provides its former measure of data security.
- 8 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 9 Click *OK* to use the changes to the running configuration and close the dialog.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring WEP 128 / KeyGuard. WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys. WEP 128 may be all that a small-business user needs for the simple encryption of wireless data.

KeyGuard is an enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

To configure WEP 128 or KeyGuard:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button.
A WLAN screen displays with the WLAN's existing configuration. Refer to the *Authentication and Encryption* columns to assess the WLAN's existing security configuration.
- 3 Select either the *WEP 128* or *KeyGuard* button from within the Encryption field.
- 4 Click the *Config* button to the right of the WEP 128 and KeyGuard checkboxes.
The *WEP 128 / KeyGuard* screen displays.



- 5 Specify a 4 to 32 character *Pass Key* and click the *Generate* button.
The pass key can be any alphanumeric string. The controller and Extreme Networks MUs use the algorithm to convert an ASCII string to the same hexadecimal number. MUs without Extreme Networks adapters need to use WEP keys manually configured as hexadecimal numbers.
- 6 Use the *Key #1-4* areas to specify key numbers.
The key can be either a hexadecimal or ASCII. The keys are 26 hexadecimal characters in length or 13 ASCII characters. Select one of these keys for activation by clicking its radio button.

Default (hexadecimal) keys for WEP 128 and KeyGuard include:

Key 1	101112131415161718191A1B1C
Key 2	202122232425262728292A2B2C
Key 3	303132333435363738393A3B3C
Key 4	404142434445464748494A4B4C

- 7 If you feel it necessary to restore the WEP algorithm back to its default settings, click the *Restore Default WEP Keys* button. This may be the case if you feel that the latest defined WEP algorithm has been compromised and no longer provides its former measure of data security.
- 8 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 9 Click *OK* to use the changes to the running configuration and close the dialog.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring WPA/WPA2 using TKIP and CCMP. *Wi-Fi Protected Access (WPA)* is a robust encryption scheme specified in the *IEEE Wireless Fidelity (Wi-Fi)* standard, 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

WPA's encryption method is *Temporal Key Integrity Protocol (TKIP)*. TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector. WPA also provides strong user authentication based on 802.1x EAP.

WPA2 is a newer 802.11i standard that provides even stronger wireless security than WPA and WEP. CCMP is the security standard used by the *Advanced Encryption Standard (AES)*. AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check (MIC)* using the proven *Cipher Block Chaining (CBC)* technique. Changing just one bit in a message produces a totally different result.

WPA2-CCMP is based on the concept of a *Robust Security Network (RSN)*, which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the controller provides.

To configure WPA/WPA2-TKIP/CCMP encryption:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select an existing WLAN from those displayed within the *Configuration* tab and click the *Edit* button. A WLAN screen displays with the WLAN's existing configuration. Refer to the *Authentication* and *Encryption* columns to assess the WLAN's existing security configuration.
- 3 Select either the *WPA/WPA2-TKIP* or *WPA2-CCMP* button from within the *Encryption* field.
- 4 Click the *Config* button to the right of the *WPA/WPA2-TKIP* and *WPA2-CCMP* checkboxes.

The *WPA/WPA2-TKIP/CCMP* screen displays. This single screen can be used to configure either WPA/WPA2-TKIP, or WPA-CCMP.

- 5 Select the *Broadcast Key Rotation* checkbox to enable periodically changing the broadcast key for this WLAN.

Only broadcast key changes when required by associated MUs to reduce the transmissions of sensitive key information. This value is enabled by default.

- 6 Refer to the *Update broadcast keys every* field to specify a time period (in seconds) for broadcasting encryption-key changes to MUs.

Set key broadcasts to a shorter interval (at least 60 seconds) for tighter security on wireless connections. Set key broadcasts to a longer interval (at most, 86400 seconds) to extend key times for wireless connections. The default is 7200 seconds.

- 7 Configure the *Key Settings* field as needed to set an ASCII Passphrase and key values.

ASCII Passphrase	To use an ASCII passphrase (and not a hexadecimal value), select the checkbox and enter an alphanumeric string of 8 to 63 characters. The alphanumeric string allows character spaces. The controller converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.
256-bit Key	To use a hexadecimal value (and not an ASCII passphrase), select the checkbox and enter 16 hexadecimal characters into each of the four fields displayed.



NOTE

The Web UI does not support saving passphrases in encrypted format. To save passphrases in an encrypted format, configure the passphrases using the Command Line Interface. Refer to the Summit WM3000 Controller CLI Reference Guide for details on configuring passphrases using the CLI.

Default (hexadecimal) 256-bit keys for WPA/TKIP include:

- 1011121314151617
- 18191A1B1C1D1E1F
- 2021222324252627
- 28292A2B2C2D2E2F

8 Optionally select one of the following from within the *Fast Roaming (8021x only)* field.

PMK Caching	Select <i>Pairwise Master Key (PMK)</i> caching to store Pairwise Master Key derived from 802.1x authentication between a client device and its authenticator. When a client roams between devices, the client's credentials no longer need to be completely reauthenticated (a process that can take up to 100 milliseconds). In the instance of a voice session, the connection would likely be terminated if not using a PMK. PMK cache entries are stored for a finite amount of time, as configured on the wireless client.
Opportunistic Key Caching	<i>Opportunistic Key Caching</i> allows the controller to use a PMK derived with a client on one Access Port/Point with the same client when it roams over to another Access Port/Point. Upon roaming, the client does not have to conduct 802.1x authentication and can start sending/receiving data sooner.
Pre-Authentication	Selecting the <i>Pre-Authentication</i> option enables an associated MU to carry out an 802.1x authentication with another controller (or device) before it roams to it. This enables the roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. This is only supported when 802.1x EAP authentication is enabled.

9 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

10 Click *OK* to use the changes to the running configuration and close the dialog.

11 Click *Cancel* to close the dialog without committing updates to the running configuration.

This feature allows using a combination of WEP encryption and 802.11i encryption on a per WLAN basis. This is done by creating WLANs with the same SSID but with different BSSIDs and security cipher combinations. The APs broadcast different beacons for the same SSID. The MUs associate with the AP based on its configuration of SSID, BSSID, and security cipher.

This feature supports the following combinations of security ciphers:

- WEP 64 and WPA/WPA2-TKIP
- WEP 64 and WPA-CCMP
- WEP 128 and WPA/WPA2-TKIP
- WEP 128 and WPA-CCMP
- WPA-CCMP and WPA/WPA2-TKIP

These security cipher combinations are available on a per WLAN basis.

The following are the limitations of this feature:

- You should make sure that the WLANs created with the same SSIDs are grouped into different WLAN groups. This is because WLANs with common SSID should have unique BSSIDs.
- WEP 64 and TKIP/CCMP ciphers can not be part of the same WLAN group.
- When WEP 128/TKIP and CCMP ciphers are grouped in the same WLAN group, the BC/MC encryption is downgraded to WEP 128/TKIP. So in scenarios where 'N only' MUs are present they

may not be able to associate as those MUs do not support WEP 128/TKIP. In such cases WLANs with WEP 128/TKIP cipher suites should be in a different WLAN group than those WLANs with CCMP cipher suites.

- When downgrading the firmware on the AP, WLANs with same SSIDs are not supported by the old version of the firmware image and hence there could be errors while configuring the AP after booting up with image. Only the first WLAN with the common SSID may get created.
- When exporting the configuration to an AP, which does not support this feature there could be errors while configuring the AP. Only the first WLAN with the common SSID may get created.

Viewing WLAN Statistics

The *Statistics* screen displays read-only statistics for each WLAN. Use this information to assess if configuration changes are required to improve network performance. If a more detailed set of WLAN statistics is required, select a WLAN from the table and click the *Details* button.

To view WLAN configuration details:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Click the *Statistics* tab.

The screenshot shows the 'Network > Wireless LANs' configuration page in the Summit WM3600 Controller. The 'Statistics' tab is selected, showing a table of WLAN statistics. The table has the following data:

Index	ESSID	Description	VLAN	MUs	Throughput Mbps	Avg Mbps	% Non-UNI	Retries
1	test-open-1x	WLAN1	1	0	0	0	100	0
2	test-open-hotspot	WLAN2	1	0	0	0	100	0

The interface also includes a left-hand navigation menu with options like 'Controller', 'Network', 'Services', 'Security', etc. The top navigation bar shows 'Configuration', 'Statistics', 'WMM', 'NAC Include', and 'NAC Exclude'. The bottom bar contains buttons for 'Save', 'Logout', 'Refresh', 'Details', 'Graph', 'Controller Statistics', and 'Help'.

3 Refer to the following details displayed within the table:

Last 30s	Click the <i>Last 30s</i> radio button to display statistics for the WLAN over the last 30 seconds. This option is helpful when troubleshooting issues as they actually occur.
Last Hr	Click the <i>Last Hr</i> radio button to display statistics for the WLAN over the last 1 hour. This metric is helpful in baselining events over a one hour interval.
Index	The Idx (or index) is a numerical identifier used to differentiate the WLAN from other WLANs that may have similar characteristics.
ESSID	The SSID is the <i>Extended Service Set ID</i> (ESSID) for the selected WLAN.
Description	The Description item contains a brief description of the WLAN. Use the description (along with the index) to differentiate the WLAN from others with similar attributes.
VLAN	The VLAN parameter displays the name of the VLAN the WLAN is associated with.
MUs	Lists the number of MUs associated with the WLAN.
Throughput Mbps	Throughput Mbps is the average throughput in Mbps on the selected WLAN. The Rx value is the average throughput in Mbps for packets received on the selected WLAN. The Tx value is the average throughput for packets sent on the selected WLAN.
Avg BPS	Displays the average bit speed in Mbps for the selected WLAN. This includes all packets sent and received.
% Non-UNI	Displays the percentage of the total packets for the selected WLAN that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries for all MUs associated with the selected WLAN.

4 To view WLAN statistics in greater detail, select a WLAN and click the *Statistics* button. For more information, see [“Viewing WLAN Statistics in Detail” on page 170](#).



NOTE

When using mesh-enabled WLAN statistics, no statistics are shown. This is because WLAN statistics are generated by mobile unit traffic for that particular WLAN. In a mesh configuration, there are typically no mobile units associated and therefore no statistical information to display.

5 To view WLAN statistics in a graphical format, select a WLAN and click the *Graph* button. For more information, see [“Viewing WLAN Statistics in a Graphical Format” on page 173](#).

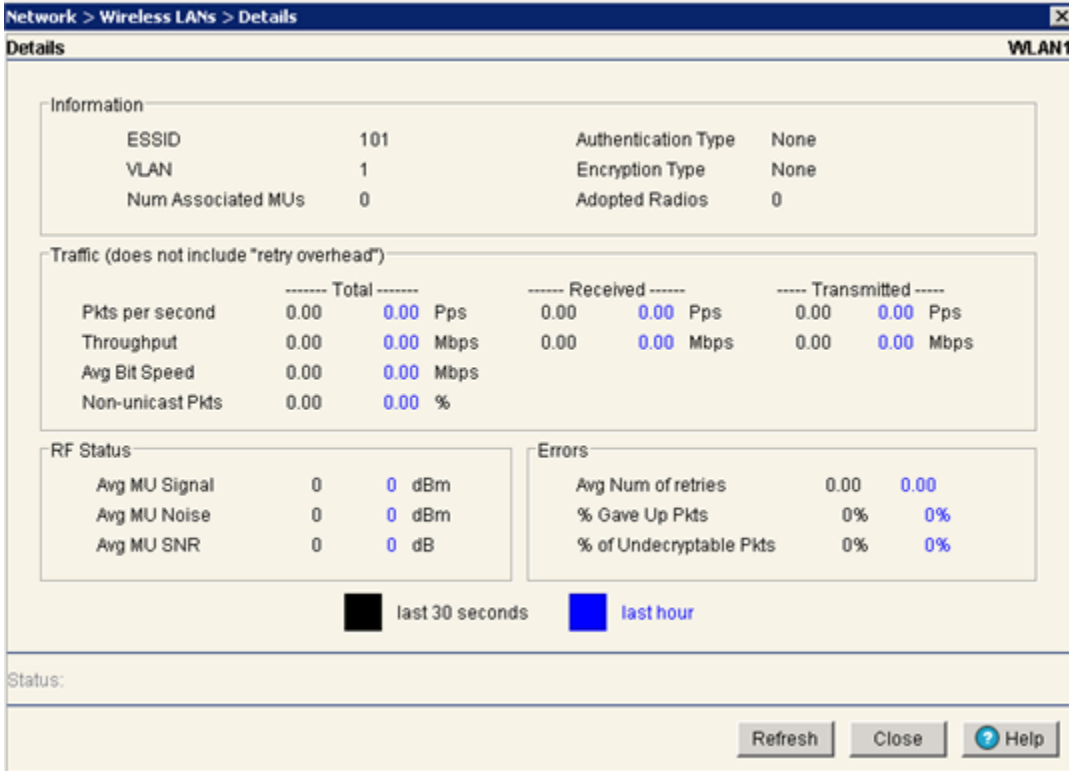
6 To view WLAN packet data rates and retry counts, select a WLAN and click the *Controller Statistics* button. For more information, see [“Viewing WLAN Controller Statistics” on page 174](#).

Viewing WLAN Statistics in Detail

When the WLAN Statistics screen does not supply adequate information for an individual WLAN, the *Details* screen is recommended for displaying more granular information for a single WLAN. Use this information to discern if a WLAN requires modification to meet network expectations.

To view detailed statistics for a WLAN:

- 1 Select a *Network > Wireless LANs* from the main menu tree.
- 2 Click the *Statistics* tab.
- 3 Select a WLAN from the table displayed in the Statistics screen and click the *Details* button.



The *Details* screen displays the WLAN statistics of the selected WLAN. The *Details* screen contains the following fields:

- Information
- Traffic
- RF Status
- Errors

Information in *black* represents the statistics from the last 30 seconds and information in *blue* represents statistics from the last hour.

- 4 Refer to the *Information* field for the following information:

ESSID	Displays the <i>Extended Service Set ID</i> (ESSID) for the selected WLAN.
VLAN	Displays the name of the VLAN the WLAN is associated with.
Num Associated MUs	Displays the total number of MUs currently associated with the selected WLAN.
Authentication Type	Displays the authentication method deployed on the WLAN.
Encryption Type	Displays the encryption type deployed on the selected WLAN.
Adopted Radios	Displays the radios adopted by the selected WLAN.

5 Refer to the *Traffic* field for the following information (both received and transmitted):

Pkts per second	Displays the average total packets per second that cross the selected WLAN. The Rx column displays the average total packets per second received on the selected WLAN. The Tx column displays the average total packets per second sent on the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Throughput	Displays the average throughput in Mbps on the selected WLAN. The Rx column displays the average throughput in Mbps for packets received on the selected WLAN. The Tx column displays the average throughput for packets sent on the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Avg Bit Speed	Displays the average bit speed in Mbps on the selected WLAN. This includes all packets sent and received. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Non-unicast Pkts	Displays the percentage of the total packets for the selected WLAN that are non-unicast. Non-unicast packets include broadcast and multicast packets. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.

6 Refer to the *RF Status* field for the following information:

Avg MU Signal	Displays the average RF signal strength in dBm for all MUs associated with the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Avg MU Noise	Displays the average RF noise for all MUs associated with the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Avg MU SNR	Displays the average <i>Signal to Noise Ratio</i> (SNR) for all MUs associated with the selected WLAN. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7 Refer to the *Errors* field for the following information:

Average Number of Retries	Displays the average number of retries for all MUs associated with the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
% Gave Up Pkts	Displays the percentage of packets the controller gave up on for all MUs associated with the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
% Non-decryptable Pkts	Displays the percentage of undecryptable packets for all MUs associated with the selected WLAN. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistic for the last hour.

8 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

9 Click *OK* to use the changes to the running configuration and close the dialog.

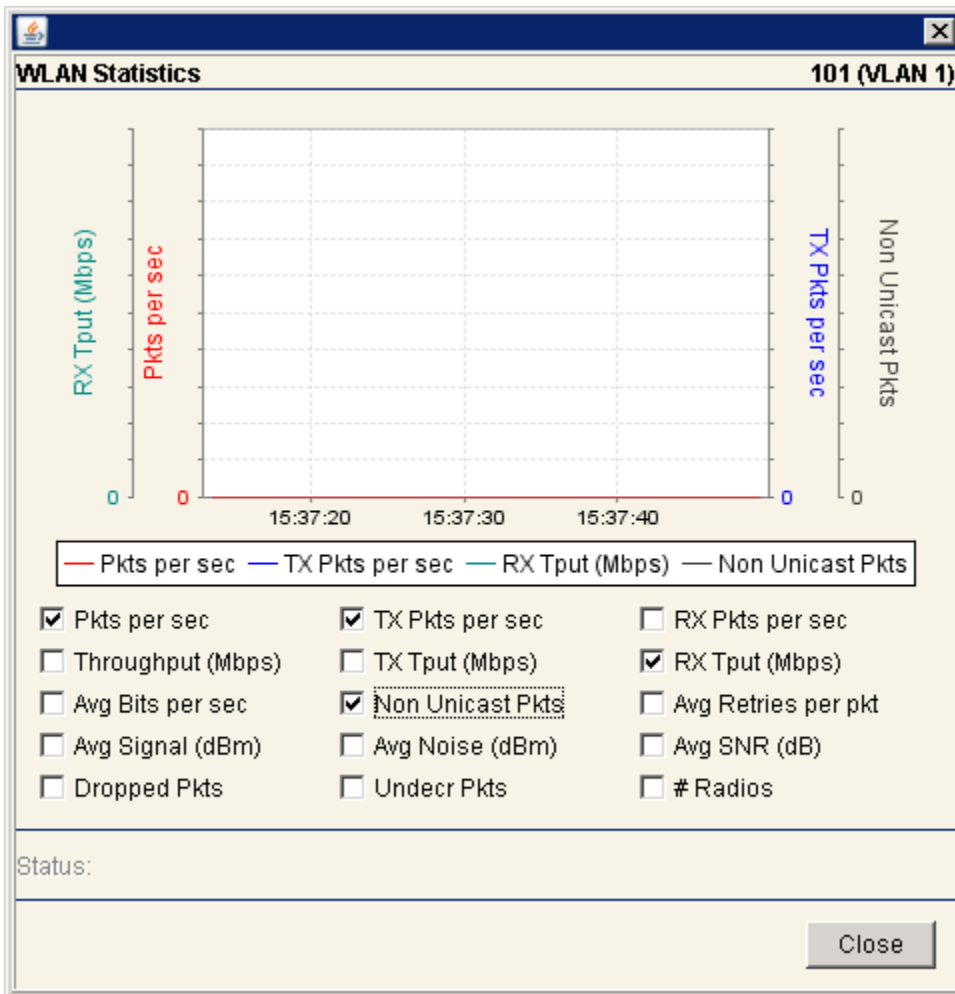
10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing WLAN Statistics in a Graphical Format

The controller Web UI continuously collects WLAN statistics even when the graph is not displayed. Periodically display the WLAN statistics graph for the latest WLAN throughput and performance information.

To view detailed graphical statistics for a WLAN:

- 1 Select a WLAN from the table displayed in the *Statistics* screen.
- 2 Click the *Graph* button.



The *WLAN Statistics* screen displays for the select port. The *WLAN Statistics* screen provides the option of viewing the graphical statistics of the following parameters:

- Pkts per sec
- Throughput (Mbps)
- Avg Bits per sec
- Avg Signal (dBm)
- Dropped Pkts
- TX Pkts per sec
- TX Tput (Mbps)
- NUcast Pkts
- Avg Noise (dBm)
- Undecr Pkts
- RX Pkts per sec
- RX Tput (Mbps)
- Avg Retries per pkt
- Avg SNR (dB)
- # Radios



NOTE

You cannot select (and send) more than four parameters at any given time.

- 3 Select any of the above listed parameters by clicking on the checkbox associated with it.
- 4 Click the *Close* button to exit the screen.

Viewing WLAN Controller Statistics

The *Controller Statistics* screen displays the sum of all WLAN statistics. The *Controller Statistics* screen is optimal for displaying a snapshot of overall WLAN traffic on your controller.

To view detailed statistics for a WLAN:

- 1 Select a *Network > Wireless LANs* from the main menu tree.
- 2 Click the *Statistics* tab.

- 3 Select a WLAN from the table displayed in the *Statistics screen* and click the *Controller Statistics* button.

The screenshot shows a window titled "Network > Wireless LANs > Controller Statistics". Inside, there are two tables: "Packet Rates" and "Retry Counts".

Packet Rates			Retry Counts	
Rates (Mbps)	Tx packets	Rx packets	Retries	Packets
1.0	0	0	0	0
2.0	0	0	1	0
5.5	0	0	2	0
6.0	0	0	3	0
9.0	0	0	4	0
11.0	0	0	5	0
12.0	0	0	6	0
18.0	0	0	7	0
22.0	0	0	8	0
24.0	0	0	9	0
36.0	0	0	10	0
48.0	0	0	11	0
54.0	0	0	12	0
			13	0
			14	0
			15	0

Below the tables is a "Status:" field. At the bottom right are buttons for "Refresh", "Close", and "Help".

- 4 Refer to the *Packet Rates* field to review the number of packets both transmitted (Tx) and received (Rx) at data rates from 1.0 to 54.0 Mbps. If a large number of packets are sent and received at a slower data rate, then perhaps the controller is not adequately positioned or configured to support the MUs within that WLAN.



NOTE

The Extreme Networks Wireless Management Suite (WMS) is recommended to plan the deployment of the controller. Extreme Networks WMS can help optimize the positioning and configuration of a controller in respect to a WLAN's MU throughput requirements. For more information, refer to the Extreme Networks website.

- 5 Refer to the *Retry Counts* field to review the number of packets requiring retransmission from the controller.
- 6 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *Refresh* to update the Packet Rate and Retry Count data displayed within the screen.

8 Click *Close* to close the dialog and return to the Network > Wireless LANs > Statistics screen.

Configuring WMM

Use the *WMM* tab to review a WLAN's current index (numerical identifier), SSID, description, current enabled/disabled designation, and Access Category.

To view existing WMM Settings:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Click the *WMM* tab.

SUMMIT® WM3600 CONTROLLER

Network > Wireless LANs

Configuration | Statistics | **WMM** | NAC Include | NAC Exclude

Show Filtering Options

Idx	SSID	Description	WLAN enabled	WMM enabled	Access	AIFSN	Transmit Ops	ECW Min	ECW Max	Max Retries
1/1	test-o...	WLAN1	✓	✓	Best Effort	3	0	4	10	0
1/2	test-o...	WLAN1	✓	✓	Background	7	0	4	10	0
1/3	test-o...	WLAN1	✓	✓	Video	2	94	3	4	0
1/4	test-o...	WLAN1	✓	✓	Voice	2	47	2	3	0
2/1	test-o...	WLAN2	✓	✓	Best Effort	3	0	4	10	0
2/2	test-o...	WLAN2	✓	✓	Background	7	0	4	10	0
2/3	test-o...	WLAN2	✓	✓	Video	2	94	3	4	0
2/4	test-o...	WLAN2	✓	✓	Voice	2	47	2	3	0
3/1	103	WLAN3	✗	✓	Best Effort	3	0	4	10	0
3/2	103	WLAN3	✗	✓	Background	7	0	4	10	0
3/3	103	WLAN3	✗	✓	Video	2	94	3	4	0
3/4	103	WLAN3	✗	✓	Voice	2	47	2	3	0
4/1	104	WLAN4	✗	✓	Best Effort	3	0	4	10	0
4/2	104	WLAN4	✗	✓	Background	7	0	4	10	0
4/3	104	WLAN4	✗	✓	Video	2	94	3	4	0
4/4	104	WLAN4	✗	✓	Voice	2	47	2	3	0
5/1	105	WLAN5	✗	✓	Best Effort	3	0	4	10	0
5/2	105	WLAN5	✗	✓	Background	7	0	4	10	0
5/3	105	WLAN5	✗	✓	Video	2	94	3	4	0
5/4	105	WLAN5	✗	✓	Voice	2	47	2	3	0
6/1	106	WLAN6	✗	✓	Best Effort	3	0	4	10	0
6/2	106	WLAN6	✗	✓	Background	7	0	4	10	0
6/3	106	WLAN6	✗	✓	Video	2	94	3	4	0
6/4	106	WLAN6	✗	✓	Voice	2	47	2	3	0
7/1	107	WLAN7	✗	✓	Best Effort	3	0	4	10	0
7/2	107	WLAN7	✗	✓	Background	7	0	4	10	0
7/3	107	WLAN7	✗	✓	Video	2	94	3	4	0
7/4	107	WLAN7	✗	✓	Voice	2	47	2	3	0
8/1	108	WLAN8	✗	✓	Best Effort	3	0	4	10	0
8/2	108	WLAN8	✗	✓	Background	7	0	4	10	0

Filtering is disabled

Buttons: Save, Logout, Refresh, Edit, GoS Mappings, Help

The *WMM* tab displays the following information:

- Idx** Displays the WLANs numerical identifier. This field is displayed in a two part format. The first number is the WLAN index and the second number is a sub-index corresponding to the access category. Click the *Edit* button to modify this property.
The available WLAN index range is from 1-24 for Summit WM3400.
- SSID** Displays the Service Set ID (SSID) associated with each WLAN.
- Description** Displays a brief description of the WLAN.

WLAN enabled	Displays the status of the WLAN. A Green check defines the WLAN as enabled and a Red "X" means it is disabled. The enable/disable setting can be defined using the <i>WLAN Configuration</i> screen.
WMM enabled	Displays WLAN-WMM status. It can be enabled (for a WLAN) from the WLAN Configurations Edit screen by selecting the Enable WMM checkbox.
Access	Displays the Access Category for the intended radio traffic. Access Categories are the different WLAN-WMM options available. The four Access Category types are: <ul style="list-style-type: none"> • <i>Background</i>—Optimized for background traffic • <i>Best-effort</i>—Optimized for best effort traffic • <i>Video</i>—Optimized for video traffic • <i>Voice</i>—Optimized for voice traffic
AIFSN	Displays the current <i>Arbitrary Inter-frame Space Number (AIFSN)</i> . Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access.
Transmit Ops	Displays the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number.
ECW Min	The ECW Min is combined with the ECW Max to make the Contention screen. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
ECW Max	The ECW Max is combined with the ECW Min to make the Contention screen. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
Max Retries	Displays the maximum number of retries for each WMM index.

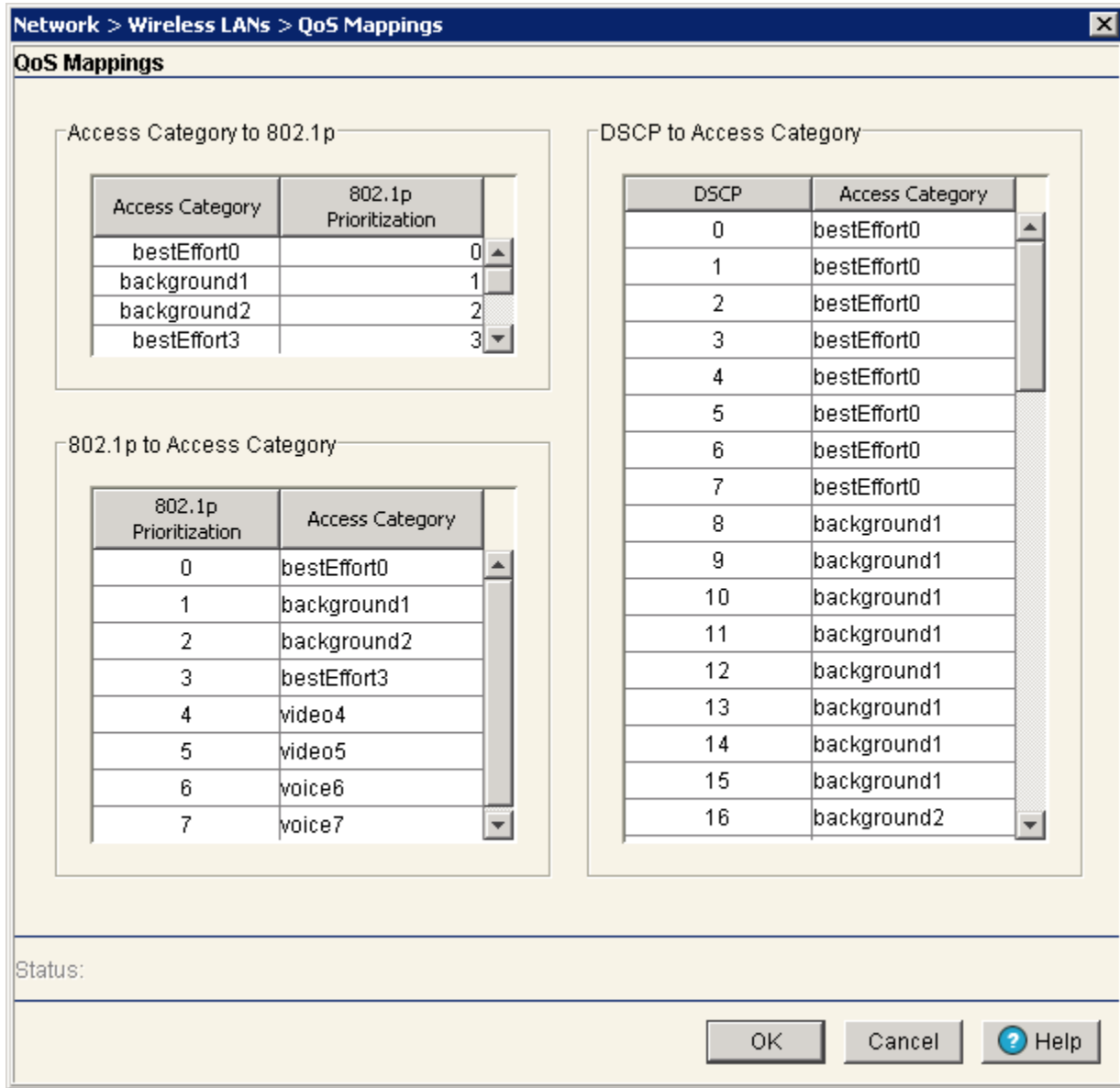


NOTE

When using an Altitude 4700 Series Access Point in Adaptive AP Mode, you must enable WMM on the associated WLAN in order to achieve the highest data rates available.

- 3 Click the *Edit* button to display a screen used to modify the WMM parameters. For more information, see [“Editing WMM Settings” on page 179](#).

- 4 Select the *QoS Mappings* button to revise the existing mappings of access category to 802.1p and DSCP to access category settings.



With a drastic increase in bandwidth absorbing network traffic (VOIP, multimedia, etc.), the importance of data prioritization is critical to effective network management.

Refer to the following fields within the *QoS Mapping* screen to optionally revise the existing settings in respect to the data traffic requirements for this WLAN.

- Access Category to 802.1p Optionally revise the *802.1p Prioritization* for each access category to prioritize the network traffic expected on this WLAN.
- 802.1p to Access Category Set the access category accordingly in respect to its importance for this WLAN's target network traffic.

DSCP to Access Category

Set the access category accordingly in respect to its DSCP importance for this WLAN's target network traffic.

Differentiated Services Code Point (DSCP) is a field in an IP packet that enables different levels of service to be assigned to network traffic. This is achieved by marking each packet on the network with a DSCP code and appropriating to it the corresponding level of service or priority. QoS enabled programs request a specific service type for a traffic flow through the generic QoS (GQoS) application programming interface (API).

Editing WMM Settings

WLAN WMM configuration affects your upstream traffic parameters. Use “[Configuring WMM](#)” on [page 227](#) to configure downstream traffic parameters. Use the WMM Edit screen to modify existing Access Category settings for the WLAN selected within the WMM screen. This could be necessary in instances when data traffic has changed and high-priority traffic (video and voice) must be accounted for by modifying AIFSN Transmit Ops and CW values.

To edit existing WMM Settings:

- 1 Select *Network Setup > WLAN Setup* from the main menu tree.
- 2 Click the *WMM* tab.
- 3 Select an Access Category from the table and click the *Edit* button to launch a dialog with WMM configuration for that radio.

Network > Wireless LANs > Edit WMM

Edit WMM

SSID: 101

Access Category: Best Effort

AIFSN: 3 (2 - 15)

Transmit Ops: 0 (0 - 65535)

ECW Min.: 4 (0 - 15)

ECW Max.: 10 (0 - 15)

Max Retries: 0 (0 - 15)

Use DSCP Use 802.1p
(applies to all of this WLAN)

Status:

OK Cancel Help

- 4 Refer to the *Edit WMM* screen for the following information:

SSID

Displays the *Service Set ID* (SSID) associated with the selected WMM index. This SSID is read-only and cannot be modified within this screen.

Access Category	Displays the Access Category for the intended radio traffic. The Access Categories are the different WLAN-WMM options available to the radio. The four Access Category types are: <ul style="list-style-type: none"> • <i>Background</i>—Optimized for background traffic. • <i>Best-effort</i>—Optimized for best effort traffic. • <i>Video</i>—Optimized for video traffic. Video traffic receives priority. • <i>Voice</i>—Optimized for voice traffic. Voice traffic receives priority.
AIFSN	Defines the current <i>Arbitrary Inter-frame Space Number</i> (AIFSN). Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before trying to access the medium.
Transmit Ops	Defines the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number.
ECW Minimum	The ECW Minimum is combined with the ECW Maximum to make the Contention screen. From this range, a random number is selected for the back off mechanism. Select a lower value for high priority traffic.
ECW Maximum	The ECW Maximum is combined with the ECW Minimum to make the Contention screen. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic
Max Retries	Defines a maximum number of retries for each Access Category.
Use DSCP or 802.1p	Selects the DSCP or 802.1p radio buttons to choose between DSCP and 802.1p.

- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring the NAC Inclusion List

Using NAC, the controller acts as an enforcement entity before allowing MU access to specific network resources. NAC performs an MU host integrity check wherein an MU sends host integrity information to the NAC server. The NAC server configuration is defined on the controller on a per WLAN basis. NAC verifies an MU's compliance with the NAC server's security policy (not the controller).

For a NAC configuration example using the controller CLI, see [“NAC Configuration Examples Using the Controller CLI” on page 188](#).

An include list is a list of MAC addresses configured for a WLAN. During EAP authentication, the EAP server (RADIUS or NAC server) is determined based on the MU's MAC address.

- All non-802.1x devices are partitioned into a WLAN (separate from a 802.1x enabled WLAN).
- Communication between devices in a 802.1x supported WLAN and a non 802.1x supported WLAN is achieved by merging the WLANs within the same VLAN.

The controller uses the include list to add devices that are NAC supported. The following explains how authentication is achieved using 802.1x. The controller authenticates 802.1x enabled devices using one of the following:

- *NAC Agent*—NAC support is added in the controller to allow the controller to communicate with a LAN enforcer (a laptop with a NAC agent installed).

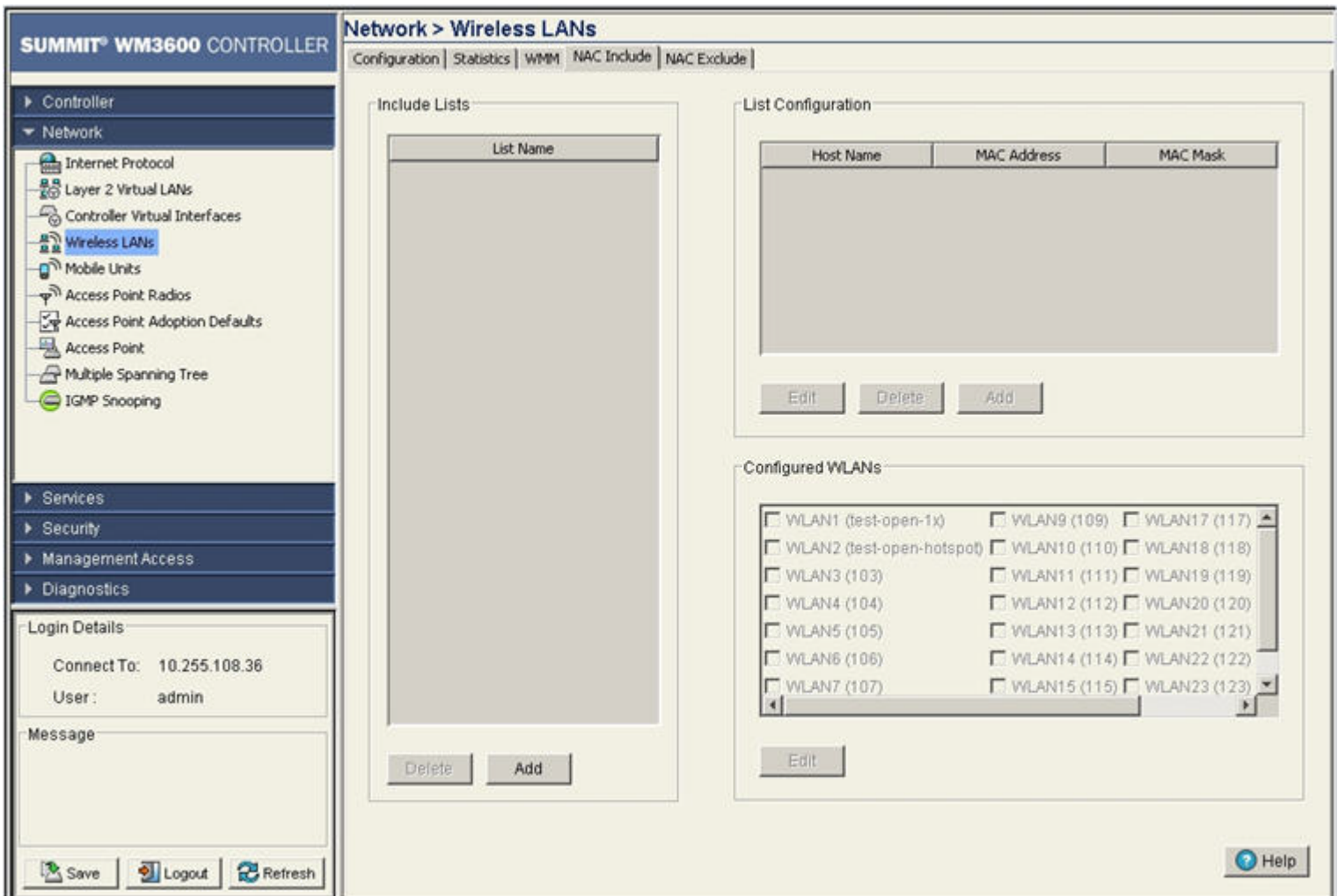
- *No NAC Agent*—NAC support is achieved using an exclude list. For more information, see [“Configuring the NAC Exclusion List” on page 184](#).

By default, a WLAN is NAC disabled. Each WLAN can be configured to:

- Conduct a NAC check for MU's connecting to the WLAN as well as perform an additional exclude function, by attaching an exclude list to the WLAN.
- Do not perform NAC validation for MUs connecting to the WLAN.
- Include a few MUs for NAC validation and bypass the rest of the MUs.

To view the attributes of a NAC Include list:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Include List Configuration* tab to view and configure NAC enabled devices.



- 3 The *Include Lists* field displays the list of devices that can be included on a WLAN (a printer for example).

Use the *Add* button to add a device for configuration on a WLAN. A maximum of 6 MAC addresses are allowed per device. For more information, see [“Adding an Include List to a WLAN” on page 182](#).

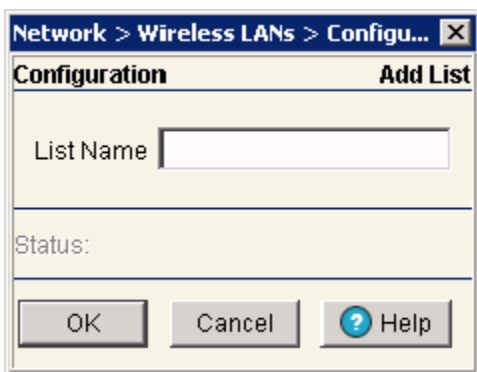
The *List Configuration* field displays a list of MAC addresses that can be included on a WLAN. You can add more than one device in this list. For example, printer 1, printer 2, etc.

- 4 Use the *Add* button (within the *List Configuration* field) to add more than one device to the WLAN. You can create 32 lists (both include and exclude combined together) and 64 MAC entries per list. For more information, see [“Configuring Devices on the Include List” on page 182](#).
- 5 The *Configured WLANs* field displays available WLANs. Associate a list item (within the *Include Lists* field) with as many WLANs as required.
For information on mapping NAC Include list items with WLANs, see [“Mapping Include List Items to WLANs” on page 183](#).
- 6 To delete a device (and its configuration), select it from the *Include Lists* and click the *Delete* button.
- 7 Use the *Edit* button in the *List Configuration* section to modify the devices parameters.
- 8 To delete any list configuration for a particular device, select the row from the *List Configuration* section and click the *Delete* button.

Adding an Include List to a WLAN

To add a device to a WLAN’s include list configuration:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Include* tab to view and configure NAC Include enabled devices.
- 3 Click the *Add* button in the *Include Lists* area.



- 4 Enter the name of the device to include for NAC authentication.
- 5 Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to save the new configuration and close the dialog window.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Devices on the Include List

To add a multiple number of devices for a single device type:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Include* tab to view and configure all the NAC Include enabled devices.

- 3 Click the *Add* button within the *List Configuration* area.

The screenshot shows a dialog box titled "Network > Wireless LANs > Configuration" with a close button (X) in the top right corner. The dialog has two tabs: "Configuration" (selected) and "Add Host". Under the "Configuration" tab, there are four input fields: "List Name" (containing "Printers"), "Host Name" (empty), "MAC Address" (containing five dashes), and "MAC Mask" (containing five dashes). Below these fields is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

The *List Name* field displays the name of the device list used. This parameter is read-only.

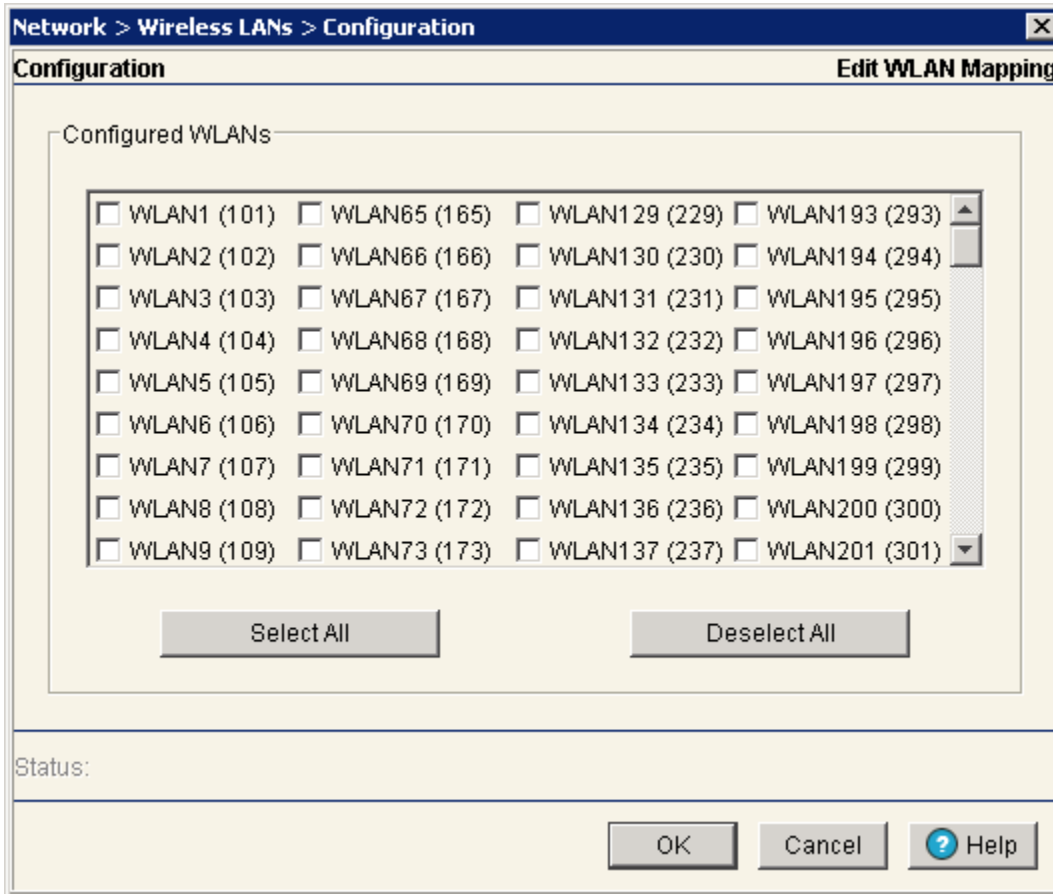
- 4 Enter the *Host Name* for the device you wish to add.
- 5 Enter a valid *MAC Address* of the device you wish to add.
- 6 Optionally, enter the *MAC Mask* for the device you wish to add.
- 7 Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to save and add the new configuration and close the dialog window.
- 9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Mapping Include List Items to WLANs

To assign include list items to one or more WLANs:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Include* tab to view NAC Included devices.

- 3 Select an item from the Include List's *List Name* field and click the *Edit* button (within the *Configured WLANs* field).



- 4 Map the selected list item with as many WLANs as needed (be selecting the WLAN's checkbox). Use the *Select All* button to associate each WLAN with the selected list item.
- 5 To remove the WLAN Mappings, select the *Deselect All* button to clear the mappings.
- 6 Refer to the *Status* field for a display of the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to save and add the new configuration and close the dialog window.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring the NAC Exclusion List

The controller provides a means to bypass NAC for 802.1x devices without a NAC agent.

A list of MAC addresses (called an exclusion list) can be added to each WLAN. Each has a separate configuration for the RADIUS server (which only conducts EAP authentication). An exclusion list is a global index-based configuration. An exclusion list can be configured and associated to any WLAN.

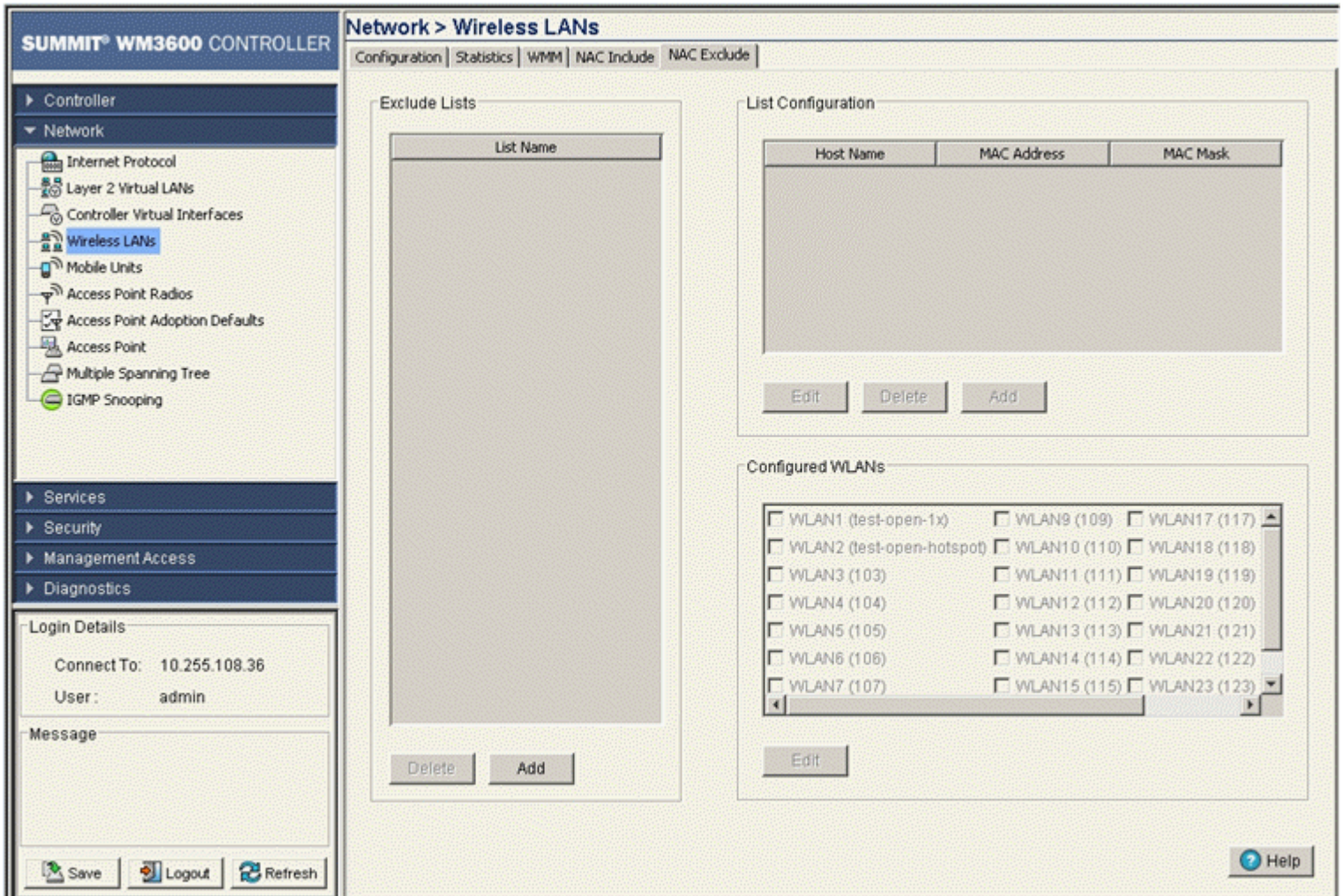
If a device's MAC address is not present in an exclusion list, it will go through the NAC server (LAN enforcer) and thereby a 802.1x host integrity check. For every WLAN configuration, there are two separate EAP servers (RADIUS and NAC).

Whenever a host entry is added or deleted from/to the list, the associated WLAN is updated and de-authenticated. The de-authenticated MU can be re-authenticated once it receives the de-authentication information from the WLAN.

For a NAC configuration example using the controller CLI, see [“NAC Configuration Examples Using the Controller CLI”](#) on page 188.

To view the attributes of a NAC exclusion list:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Exclude* tab to view and configure all the NAC include enabled devices.



The *Exclude Lists* field displays a list of devices that can be excluded from a WLAN.

- 3 Use the *Add* button to add a device that can be excluded on a WLAN. For more information, see [“Adding an Exclude List to the WLAN”](#) on page 186.

The *List Configuration* field displays a list of MAC addresses that can be excluded from a WLAN. You can add more than one device to this list.

- 4 Use the *Add* button (within the *List Configuration* field) to add devices excluded from NAC compliance on a WLAN. You can create up to 32 lists (both include and exclude combined together) and 64 MAC entries maximum per list. For more information, see [“Configuring Devices on the Exclude List”](#) on page 186.

- 5 The *Configured WLANs* field displays the available controller WLANs. Associate a list item in the *Exclude Lists* field with multiple WLANs.

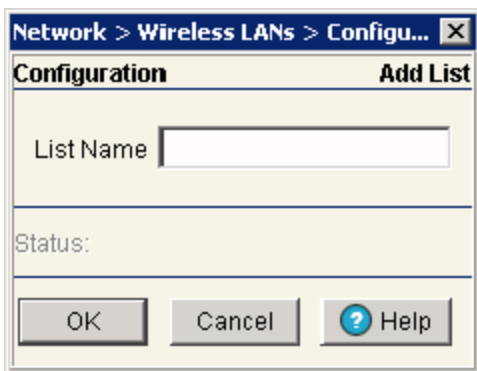
For information on mapping NAC Exclude list's items to WLANs, see [“Mapping Exclude List Items to WLANs” on page 187](#).

- 6 To delete a device, select a device from the *Exclude List* and click the *Delete* button.
- 7 Use the *Edit* button to modify devices parameters.
- 8 To delete a list configuration for a device, select a row from the *List Configuration* field and click the *Delete* button.

Adding an Exclude List to the WLAN

To exclude a device from a WLAN:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Exclude* tab to view NAC exclude devices.
- 3 Click the *Add* button in the *Exclude Lists* field.



- 4 Enter the name of the device that you wish to exclude for NAC authentication.
- 5 Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to save and add the new configuration and close the dialog window.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Devices on the Exclude List

To add more than one device for a particular type of device in the include list:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Exclude* tab to view and configure all the NAC exclude devices.

- 3 Click the *Add* button in the *List Configuration* field.

The screenshot shows a dialog box titled "Network > Wireless LANs > Configuration". It has two tabs: "Configuration" and "Add Host". The "Configuration" tab is active and contains the following fields:

- List Name: WildAPs
- Host Name: (empty)
- MAC Address: - - - - -
- MAC Mask: - - - - -

Below the fields is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

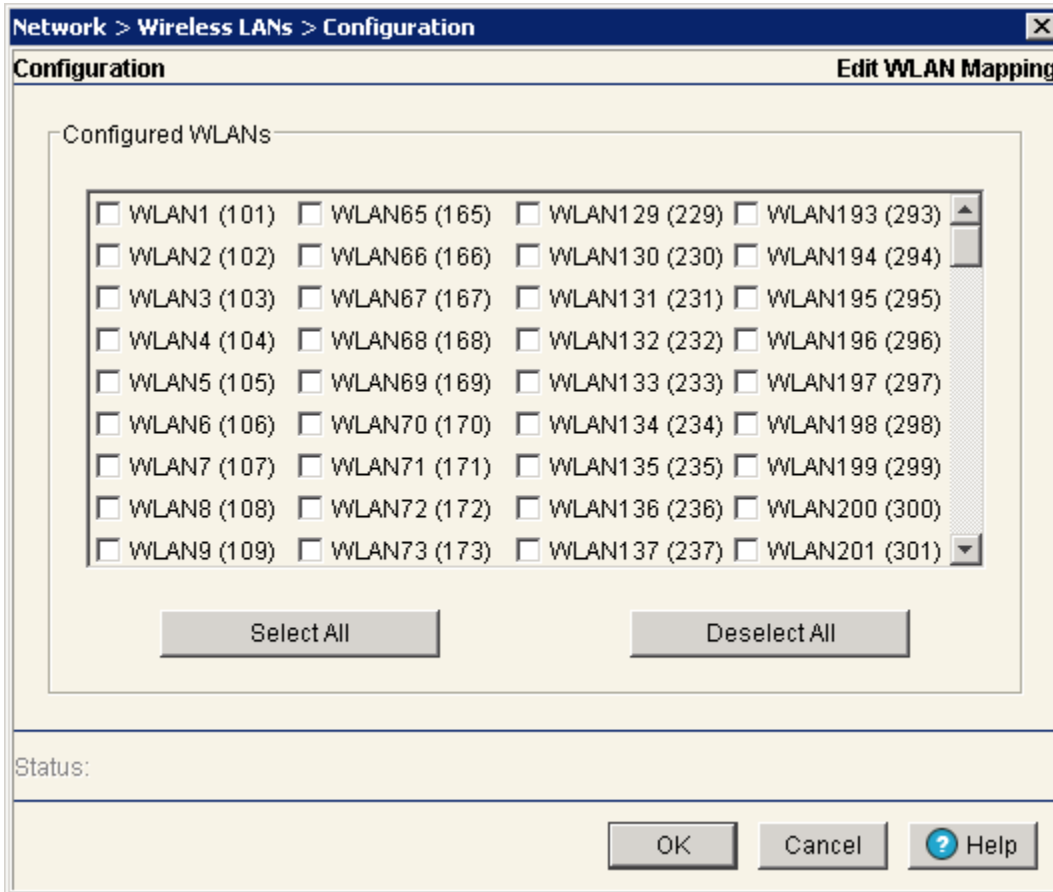
- 4 The *List Name* displays the read-only name of the list for which you wish to add more devices.
- 5 Enter the *Host Name* for the device you wish to add for the selected exclude list.
- 6 Enter a valid *MAC Address* for the device you wish to add.
- 7 Optionally, enter the *MAC Mask* for the device you wish to add.
- 8 Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 9 Click *OK* to save and add the new configuration, and close the dialog window.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Mapping Exclude List Items to WLANs

To assign exclude list items to one or more WLANs:

- 1 Select *Network > Wireless LANs* from the main menu tree.
- 2 Select the *NAC Exclude* tab to view NAC excluded devices.

- 3 Select an item from the Exclude List's *List Name* field and click the *Edit* button (within the *Configured WLANs* field).



- 4 Map the selected list item with as many WLANs as needed (be selecting the WLAN's checkbox). Use the *Select All* button to associate each WLAN with the selected list item.
- 5 To remove the WLAN Mappings, select the *Deselect All* button to clear the mappings.
- 6 Refer to the *Status* field for a display of the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The *Status* field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to save and add the new configuration and close the dialog window.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

NAC Configuration Examples Using the Controller CLI

The following are NAC include list, exclude list, and WLAN configuration examples using the controller CLI interface.

Creating an Include List

Since few devices require NAC, Extreme Networks recommends using the “bypass-nac-except-include-list” option. Refer to the commands below to create a NAC Include List:

- 1 Create a NAC include list.

```
WMController (config-wireless) #client include-list Desktop
WMController (config-wireless-client-list) #
```



NOTE

The instance changes from (config-wireless) to (config-wireless-client-list).

- 2 Add a host entry to the include list. This adds a specified MAC entry/MAC range into the client’s include list.

```
WMController(config-wireless-client-list) #station pc1 AA:BB:CC:DD:EE:FF
WMController(config-wireless-client-list) #
```

- 3 Associate the include list to a WLAN. This adds the client’s include list into the WLAN.

```
WMController(config-wireless-client-list) #wlan 1
WMController(config-wireless-client-list) #
```

Creating an Exclude List

To create a NAC Exclude List:

- 1 Define the NAC include list.

```
WMController(config-wireless) #client exclude-list Desktop
WMController(config-wireless-client-list) #
```

- 2 Add a host entry into the exclude list.

```
WMController(config-wireless-client-list) #station pc10 AB:BC:CD:DE:EF:FA
WMController(config-wireless-client-list) #
```

- 3 Associate the exclude list to a WLAN.

```
WMController(config-wireless-client-list) #wlan 1
WMController(config-wireless-client-list) #
```

Configuring the WLAN for NAC

Many handheld devices are required to bypass NAC, and a few laptops and desktops are required to be NAC validated.

- 1 Set the NAC mode for WLAN. A NAC validation is conducted for station entries in the include list. The station entries are authenticated using the RADIUS server.

```
WMController(config-wireless) #wlan 1 nac-mode bypass-nac-except-include-list
WMController (config-wireless) #
```

- 2 Configure the WLAN’s NAC server settings.

- a Configure the NAC Server’s IP address.

```
WMController(config-wireless) #wlan 1 nac-server primary 192.168.1.10
WMController(config-wireless) #
```

- b Configure the NAC Server’s RADIUS Key.

```
WMController(config-wireless) #wlan 1 nac-server primary radius-key my-secret
```

```
WMController(config-wireless) #
```

**NOTE**

Configure the secondary NAC server for redundancy.

- c** Configure the secondary NAC server's IP address.

```
WMController(config-wireless) #wlan 1 nac-server secondary 192.168.1.20
WMController(config-wireless) #
```

- d** Configure the secondary NAC Server's RADIUS Key.

```
WMController(config-wireless) #wlan 1 nac-server secondary radius-key my secret-2
WMController(config-wireless) #
```

- 3** MUs not NAC authenticated use RADIUS for authentication. To configure the WLAN's RADIUS settings:

- a** Configure the RADIUS server's IP address.

```
WMController(config-wireless) #wlan 1 radius-server primary 192.168.1.30
WMController(config-wireless) #
```

- b** Configure the server's RADIUS Key

```
WMController(config-wireless) #wlan 1 radius-server primary radius-key my-rad-secret
WMController(config-wireless) #
```

- c** Configure the secondary RADIUS server's IP address.

```
WMController(config-wireless) #wlan 1 radius-server secondary 192.168.1.40
WMController(config-wireless) #
```

- d** Configure the secondary server's RADIUS Key.

```
WMController (config-wireless) #wlan 1 radius-server secondary radius-key my-rad-
secret-2
WMController (config-wireless) #
```

- 4** Configure the NAC server's timeout and re-transmit settings. The timeout parameter configures the duration for which the controller waits for a response from the RADIUS server before attempting a retry. This is a global setting for both the primary and secondary server.

The re-transmit parameter defines the number of retries a controller attempts before dis-associating the MU.

```
WMController(config-wireless) #wlan 1 nac-server timeout 30 retransmit 10
WMController(config-wireless) #
```

- 5** Configure WLAN for EAP authentication and define the encryption type.

```
WMController(config-wireless) #wlan 1 authentication-type eap
WMController(config-wireless) #wlan 1 encryption-type wep128
WMController(config-wireless) #wlan 1 ssid wlan-1
```

Viewing Associated MU Details

The *Mobile Units* screen displays read-only device information for MUs interoperating with the controller managed network. The *Mobile Units* screen consists of the following tabs:

- [Viewing MU Status on page 191](#)
- [Configuring Mobile Units on page 195](#)

- Viewing MU Statistics on page 196
- Viewing MU Voice Statistics on page 202



NOTE

The Extreme Networks Wireless Management Suite (WMS) is a recommended utility to plan the deployment of the controller and view its configuration once operational. Extreme Networks WMS can help optimize controller positioning and configuration in respect to a WLAN's MU throughput requirements and can help detect rogue devices. For more information, refer to the Extreme Networks website.

Viewing MU Status

To view MU Status in detail:

- 1 Select *Network > Mobile Units* from the main menu tree.
- 2 Click the *Status* tab.

SUMMIT® WM3600 CONTROLLER

Network > Mobile Units

Status | Configuration | Statistics | Voice Statistics

Show Filtering Options View By Page View all Page 1 of 1 Go

Station Index	MAC Address	MAC Name	IP Address	Ready	Session Timeout	Power Save	WLAN	VLAN	Tunn	Radio Index	Radio Type
1	00-09-5B-41-58-4C		10.255.108.181	✓	unlimited	✗	4	1	-	4	802.11a
2	00-1D-6A-0E-7E-FD		10.255.108.180	✓	unlimited	✗	6	1	-	3	802.11bg

Filtering is disabled Page 1 of 1 loaded.

Details Disconnect Export Edit MAC Name dot11k Help

Save Logout Refresh

Login Details
Connect To: 10.255.108.36
User: admin

Message

The *Status* screen displays the following read-only device information for MUs interoperating within the controller managed network.

Station Index	Displays a numerical device recognition identifier for a specific MU.
MAC Address	Each MU has a unique <i>Media Access Control</i> (MAC) address through which it is identified. This address is burned into the ROM of the MU.
MAC Name	Displays the MAC name associated with each MU's MAC Address. The MAC Name is a user-created name used to identify individual mobile unit MAC Addresses with a user-friendly name.
IP Address	Displays the unique IP address for the MU. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
Ready	Displays whether the MU is ready for controller interoperation. Values are Yes and No.
Session Timeout	Displays the session timeout values for each of the listed MUs.
Power Save	Displays the current (read-only) <i>Power-Save-Poll</i> (PSP) state of the MU. The <i>Power Save</i> field has two potential settings. PSP indicates that the MU is operating in Power Save Protocol mode. In PSP, the MU runs enough power to check for beacons and is otherwise inactive. CAM indicates that the MU is continuously aware of all radio traffic. CAM is recommended for MUs frequently transmitting with the controller's Access Ports/Points for periods of two hours or greater.
WLAN	Displays the name of the WLAN the MU's associated AP is connect to.
VLAN	Displays the specific VLAN the target MU is mapped to.
Tunnel	Displays the tunnel the target MU is mapped to.
Radio Index	The Radio Index is a numerical device recognition identifier for MU radios. The index is helpful to differentiate device radios when a particular MU has more than one radio.
Radio Type	The Radio Type defines the radio used by the adopted MU. The controller supports 802.11a and 802.11g single radio MUs as well as dual radio 802.11ab, 802.11bg, 802.11an, and 802.11bgn MUs.

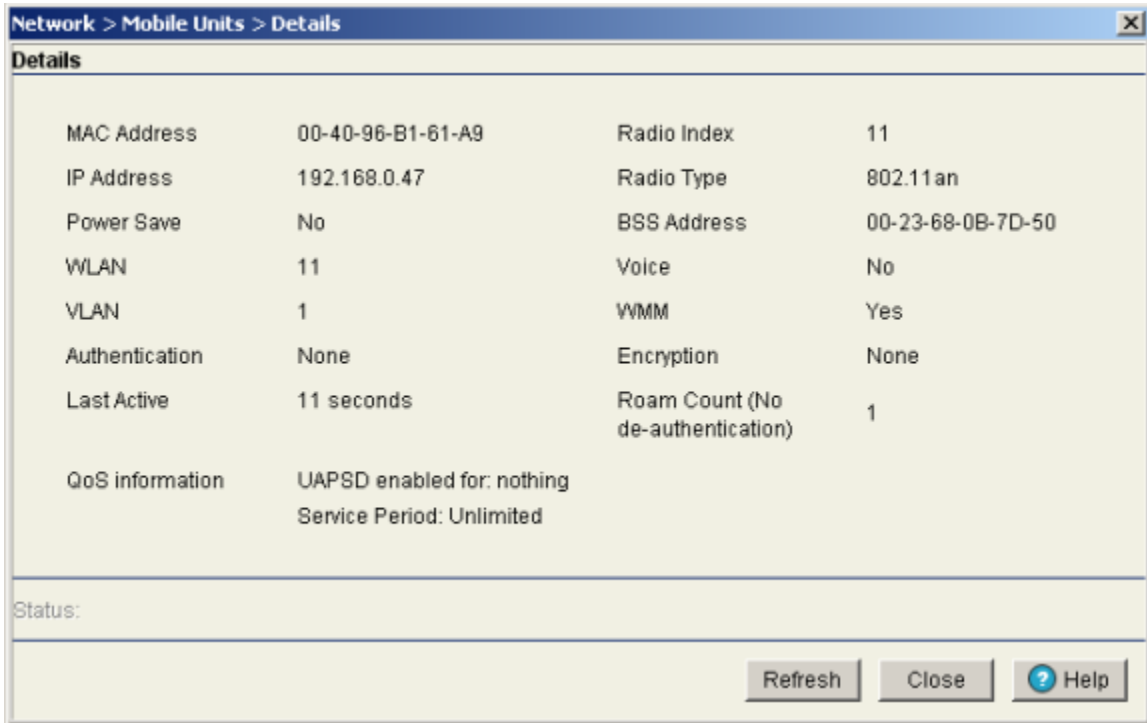
- 3 Click the *Details* button to launch a screen with additional information about the selected MU. For more information, see [“Viewing MU Details” on page 192](#)
- 4 Highlight an MU from those listed and click the *Disconnect* button to remove the MU from the list of currently associated devices.
Be aware that disconnected MUs will often become immediately re-connected to the controller. Ensure that disconnected MUs are permanently removed from controller association.
- 5 Click the *Export* button to export the content of the table to a *Comma Separated Values* file (CSV).
- 6 Click the *Edit MAC Name* button and it will open a window where you can associate a name with the selected MU's MAC Address. The MAC Name is a user-created name used to identify individual mobile unit MAC Addresses with a user-friendly name or description.
- 7 Click the *dot11k* button and it will open a new window where you can configure 802.11k Radio Resource Management services.

Viewing MU Details

The *MUs Details* screen displays read-only MU transmit and receive statistics.

To view MU Details:

- 1 Select a *Network > Mobile Units* from the main menu tree.
- 2 Click the *Status* tab.
- 3 Select an MU from the table in the *Status* screen and click the *Details* button.



4 Refer to the following read-only MUs transmit and receive statistics:

MAC Address	Displays the Hardware or Media Access Control (MAC) address for the MU.
IP Address	Displays the unique IP address for the MU. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
Power Save	Displays the current PSP state of the MU. This field has two potential settings. PSP indicates if the MU is operating in PSP mode. In PSP, the MU runs enough power to check for beacons, and is otherwise inactive. CAM indicates that the MU is continuously aware of all radio traffic. CAM is recommended for MUs transmitting frequently.
WLAN	Displays of the WLAN the MU is currently associated with.
VLAN	Displays the VLAN parameter for the name of the VLAN the MU is currently mapped to.
Authentication	Displays the authentication method used by the MU to get connected to the WLAN.
Last Active	Displays the time the MU last interoperated with the controller.
QoS Information	Displays the WMM power save (UAPSD) parameters used by this MU.
Radio Index	Displays a numerical identifier used to associate a particular Radio with a set of statistics. The Index is helpful for distinguishing a particular radio from other MU radios with similar configurations.
Radio Type	Displays the radio type used by the adopted MU. The controller supports 802.11b, 802.11bg and 802.11bgn MUs as well as 802.11a and 802.11an MUs.
BSS Address	Displays the MU's BSSID.

Voice	Displays whether or not the MU is a voice capable device. Traffic from a voice enabled MU is handled differently than traffic from MUs without this capability. MUs grouped to particular WLANs can be prioritized to transmit and receive voice traffic over data traffic.
WMM	Displays WMM usage status for the MU, including the Access Category currently in use. Use this information to assess whether the MU is using the correct WMM settings in relation to the operation of the controller.
Encryption	Displays the encryption type used by the MU for transmitting or receiving data frames on this WLAN.
Roam Count	Refer to the Roam Count value to assess the number of times the MU has roamed from the controller.

- 5 Click the *Refresh* button to update the MU Statistics to their latest values.
- 6 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

Assigning MAC Names

The *Edit MAC Name* screen allows you to associate a name with the selected MU's MAC Address.

To edit a MAC Name:

- 1 Select a *Network > Mobile Units* from the main menu tree.
- 2 Click the *Status* tab.
- 3 Select an MU from the table in the *Status* screen and click the *Edit MAC Name* button.
- 4 The *MAC Address* field displays the MAC Address for the selected MU, which will be associated by the MAC Name.
- 5 Enter a *MAC Name* to associate with the selected MU's MAC Address. The MAC Name is a user-created name used to identify individual mobile unit MAC Addresses with a user-friendly name.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.

Configuring 802.11k Radio Resource Management

The *dot11k* screen allows you to enable 802.11k Radio Resource Management for MUs.

The RRM (WLAN Radio Resource Measurement) service enables MUs to understand the radio environment in which they exist. It enables them to observe and gather data on radio link performance and on the radio environment there by enabling adjustment of MUs operation to better suit the radio environment. The RRM capability needs to be advertised through Beacons. The Wireless Controller shall send out a Beacon request to RRM capable MUs, and it should be able to process received Beacon reports. The Beacon request is sent to RRM capable MUs in active mode with specified measurement duration as and when they are triggered. If an MU refuses/ rejects/ does not send the report, then the request is retried after an expiry of specified duration. In case of further refuse/reject, retry until a maximum retry limit. The Maximum Beacon requests sent out to an MU in this case are limited to three.

To enable 802.11k on an MU:

- 1 Select a *Network > Mobile Units* from the main menu tree.
- 2 Click the *Status* tab.
- 3 Select an MU from the table in the *Status* screen and click the *dot11k* button.
- 4 Check the *Trigger Beacon Request* box to enable Radio Resource Management services on the selected MU.

- 5 In the *Measurement Duration* field, enter a time interval between 500-1000 (in K-us) to specify how often the Radio Resource Measurement services will poll the selected MU for traffic information.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.

Configuring Mobile Units

The *Mobile Units Configuration* screen lets you view MAC Address to MAC Name associations as well as creating new MAC Address to MAC Name associations.

To configure Mobile Unit settings:

- 1 Select *Network > Mobile Units* from the main menu tree.
- 2 Click the *Configuration* tab.

The screenshot shows the 'SUMMIT WM3600 CONTROLLER' interface. The left sidebar contains a navigation tree with 'Network > Mobile Units' selected. The main content area is titled 'Network > Mobile Units' and has tabs for 'Status', 'Configuration', 'Statistics', and 'Voice Statistics'. The 'Configuration' tab is active. Below the tabs, there are options for 'Show Filtering Options', 'View By Page', and 'View all'. A table with the following columns is displayed: 'Controller', 'Station Index', 'MAC Address', and 'MAC Name'. The table is currently empty. Below the table, there is a message: 'Filtering is disabled Page 1 of 1 loaded.' At the bottom of the interface, there are buttons for 'Add', 'Delete', 'Apply', 'Revert', and 'Help'. A message at the bottom of the table area reads: 'Double Click on Table cell "MAC Name" to edit, press RETURN after each edit, when done press APPLY button or use ESCAPE/REVERT button to abort.'

- 3 The MU table displays the following information:

Controller

The *Controller* field displays the IP address of the cluster member associated with each MU. When clustering is enabled on the controller and Cluster GUI is enabled, the *Controller* field will be available on the MU Configuration screen. For information on configuring enabling Cluster GUI, see Managing Clustering Using the Applet.(link missing)

Station Index	The <i>Station Index</i> is a numerical device recognition identifier for a specific MU.
MAC Address	Each MU has a unique Media Access Control (<i>MAC</i>) address through which it is identified. This address is burned into the ROM of the MU.
MAC Name	The <i>MAC Name</i> is a user-created name used to identify individual mobile unit MAC Addresses with a user-friendly name. To edit an existing entry, double-click the <i>MAC Name</i> and type in the new name.

- When using clustering and the *Cluster GUI* feature is enabled, a pull-down menu will be available to select which cluster members' MUs are displayed. To view MUs from all cluster members, select *All* from the pull-down menu. To view MUs from a specific cluster member, select that member's IP address from the pull-down menu.
- To add a MAC address to MU association, click the *Add* button. For more information on adding an association, see "[MAC Naming of Mobile Units](#)".
- To remove a *MAC Name* association, select the item from the table and click the *Delete* button.
- If changes have been made to the MU table, click the *Apply* button to save the changes to the running configuration.

MAC Naming of Mobile Units

To configure Mobile Unit settings:

- Select *Network > Mobile Units* from the main menu tree.
- Click the *Configuration* tab.

- Enter the MAC Address and MAC Name for the MU being added to the list:

MAC Address	Each MU has a unique Media Access Control (<i>MAC</i>) address through which it is identified. This address is burned into the ROM of the MU.
MAC Name	The <i>MAC Name</i> is a user-created name used to identify individual mobile unit MAC Addresses with a user-friendly name.

- Click *OK* to use the changes to the running configuration and close the dialog.
- Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing MU Statistics

The *Statistics* screen displays read-only statistics for each MU. Use this information to assess if configuration changes are required to improve network performance. If a more detailed set of MU statistics is required, select an MU from the table and click the *Details* button.



NOTE

The Summit WM3400 supports a maximum of 192 MUs. The Summit WM3600 supports a maximum of 4096 MUs. The Summit WM3700 supports 8192 MUs.

To view MU statistics details:

- 1 Select *Network > Mobile Units* from the main menu tree.
- 2 Click the *Statistics* tab.

SUMMIT® WM3600 CONTROLLER

Network > Mobile Units

Status | Configuration | **Statistics** | Voice Statistics

Last 30s Last Hr

[Show Filtering Options](#)

Radio Index	AP Type	MAC Address	MAC Name	WLAN	Throughput Mbps	Bit Speed (Avg.)	% Non Unicast	Retries
4	AP3510	00-09-5B-41-5...			4 0.0	1.0	n/a	0.0
3	AP3510	00-1D-6A-0E-7...			6 0.0	27.5	n/a	0.0

Filtering is disabled

- 3 Select the *Last 30s* checkbox to display MU statistics gathered over the last 30 seconds. This option is helpful for assessing MU performance trends in real-time.
- 4 Select the *Last HR* checkbox to display MU statistics gathered over the last hour. This option is helpful for assessing performance trends over a measurable period.
- 5 Refer to the following details as displayed within the *MU Statistics* table:

Radio Index	Displays a numerical identifier used to associate a particular Radio with a set of statistics. The Index is helpful for distinguishing the radio from other radios with a similar configuration.
-------------	--

AP Type	Displays the type of Access Port detected. The controllers support AP4600 Series Access Ports, AP3510 and AP3550 model Access Points, and AP4700 Series Access Points.
MAC Address	Displays the Hardware or <i>Media Access Control</i> (MAC) address for the MU. The MAC address is hard coded at the factory and cannot be modified.
MAC Name	Displays the MAC name associated with each MU's MAC address. The MAC name is a user-created name used to identify individual mobile unit MAC addresses with a user-friendly name.
WLAN	Displays the name of the WLAN the MU is currently associated with. Use this information to determine if the MU/WLAN placement best suits the intended operation and MU coverage area.
Throughput Mbps	Displays the average throughput in Mbps between the selected MU and the Access Port/Point. The Rx column displays the average throughput in Mbps for packets received on the selected MU from the Access Port/Point. The Tx column displays the average throughput for packets sent on the selected MU from the Access Port/Point.
Bit Speed (Avg.) Mbps	Displays the average bit speed in Mbps for the selected MU. This includes all packets sent and received.
% Non Unicast	Displays the percentage of the total packets for the selected MU that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.

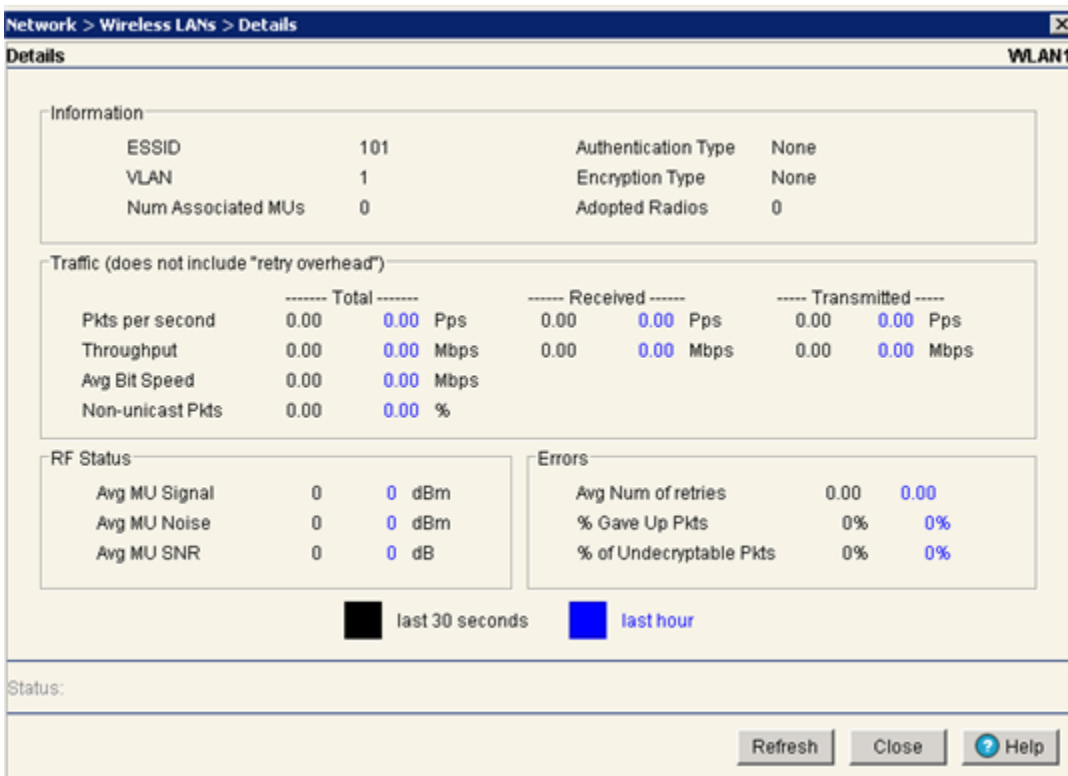
- 6 Click the *Details* button to launch a screen with additional information about the selected MU. For more information, see [“Viewing MU Statistics in Detail” on page 198](#).
- 7 Click the *Graph* button to launch a graph with pictorial information about the selected MU in a graphical format. For more information, see [“View an MU Statistics Graph” on page 200](#).
- 8 Click the *Export* button to export the content of the table to a *Comma Separated Values* file (CSV).

Viewing MU Statistics in Detail

The MU Statistics *Details* screen displays additional device address and performance information for the selected MU. Use the WMM information to assess if poor MU performance can be attributed to an inaccurate WMM setting for the type of data transmitted. To view the MU Statistics details:

- 1 Select a *Network > Mobile Units* from the main menu tree.
- 2 Click the *Statistics* tab.

3 Select an MU from the table displayed in the *Statistics* screen and click the *Details* button.



The *Details* screen displays WLAN statistics for the selected WLAN, including:

- Information
- Traffic
- RF Status
- Errors

Information in black represents the statistics from the last 30 seconds and information in blue represents statistics from the last hour. Use both sets of data to trend statistics in real time versus a measurable period (1 hour).

4 Refer to the *Information* field for the following information:

ESSID	Displays the Extended Service Set ID (ESSID) for the selected WLAN.
VLAN	Displays the VLAN the WLAN is associated with.
Num Associated MUs	Displays the total number of MUs currently associated with the selected WLAN.
Authentication Type	Displays the method of authentication currently active on the WLAN.
Encryption Type	Displays the method of authentication currently active on the WLAN.
Adopted Radios	Displays the number of radios adopted by the WLAN.

5 Refer to the *Traffic* field for the following information:

Pkts per second	Displays the average packets per second received by the MU. The Rx column displays the average packets per second received on the selected MU. The Tx column displays the average packets per second sent on the selected MU.
-----------------	---

Throughput	Displays the average throughput in Mbps between the MU and the Access Port/Point. The Rx column displays the average throughput in Mbps for packets received on the selected MU from the Access Port/Point. The Tx column displays the average throughput for packets sent on the selected MU from the Access Port/Point.
Avg. Bit Speed	Displays the average bit speed in Mbps on the selected MU. This includes all packets sent and received.
% Non-unicast pkts	Displays the percentage of the total packets for the MU that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.

6 Refer to the *RF Status* field for the following information:

Avg MU Signal	Displays the RF signal strength in dBm for the selected MU.
Avg MU Noise	Displays the RF noise for the selected MU.
Avg MU SNR	Displays the <i>Signal to Noise Ratio</i> (SNR) for the selected MU. The Signal to Noise Ratio is an indication of overall RF performance on the wireless network.

7 Refer to the *Errors* field for the following information:

Avg Num of Retries	Displays the average number of retries for the selected MU. Use this information to assess potential performance issues.
% Gave Up Pkts	Displays the percentage of packets the controller gave up on for the selected MU.
% of Undecryptable Pkts	Displays the percentage of undecryptable packets (packets that could not be processed) for the selected MU.

8 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

9 Click *Cancel* to close the dialog without committing updates to the running configuration.

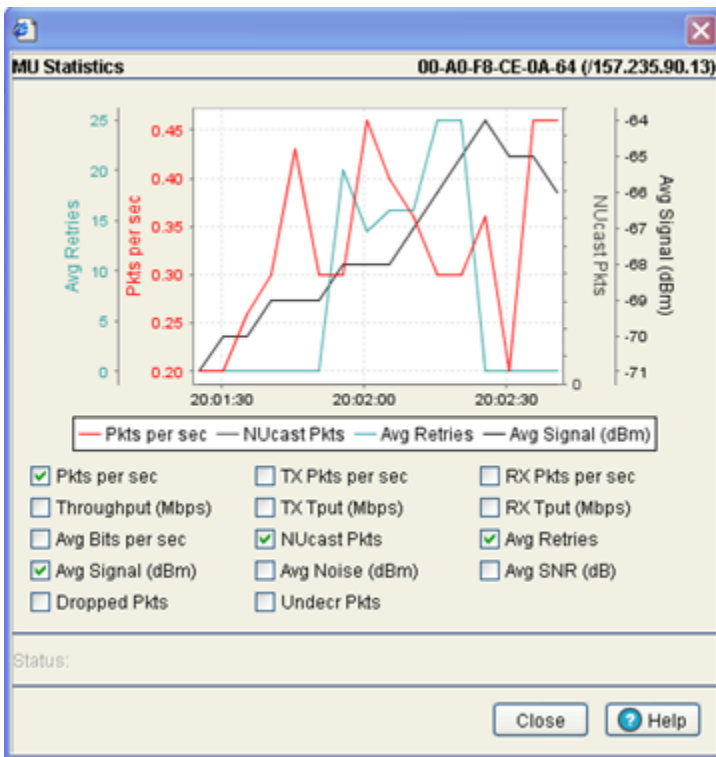
View an MU Statistics Graph

The *MU Statistics* tab has an option for displaying detailed MU statistics for individual MUs in a graphical format. This information can be used for comparison purposes to chart MU and overall controller performance.

To view the MU Statistics in a graphical format:

- 1 Select a *Network > Mobile Units* from the main menu tree.
- 2 Click the *Statistics* tab.

- 3 Select an MU from the table displayed in the *Statistics* screen and click the *Graph* button.

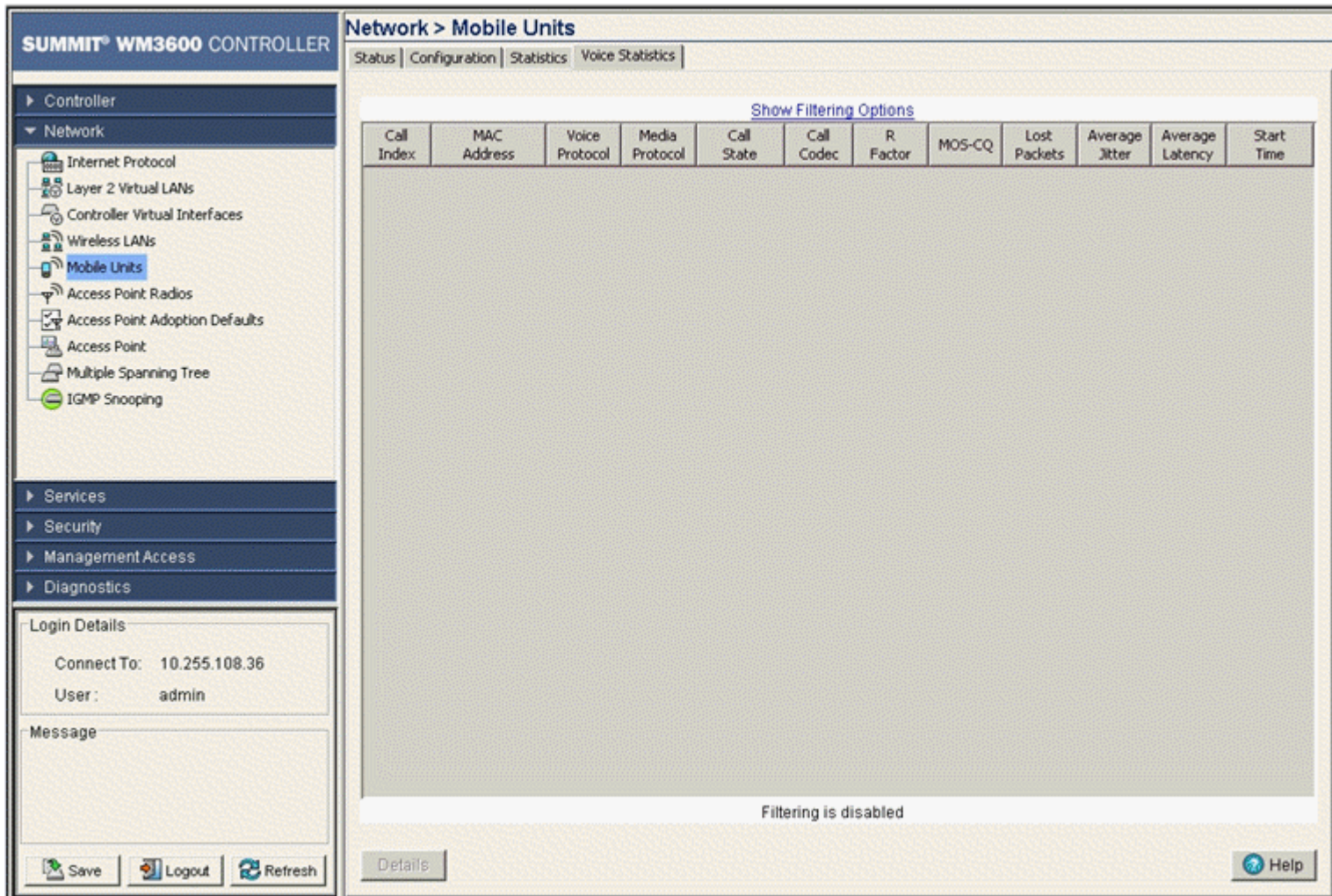


- 4 Select a checkbox to display that metric charted within the graph. Do not select more than four checkboxes at any one time.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *Close* to close the dialog without committing updates to the running configuration. Voice Statistics tab is not mentioned.

Viewing MU Voice Statistics

To view MU Voice Statistics details:

- 1 Select *Network > Mobile Units* from the main menu tree.
- 2 Click the *Voice Statistics* tab.



The Voice Statistics table displays the following information:

Call Index	Displays the numerical identifier assigned to each Access Port.
MAC Address	Displays MAC Address
Voice Protocol	Displays which voice protocol is being used for the selected call. Voice protocols include: <ul style="list-style-type: none"> • SIP • TPSEC • Spectralink • H.323
Media Protocol	Displays the Media Transport Protocol supported by the controller managed voice call.

Call State	<p>Displays the call state of the voice supported call supported by the controller. Terminated calls are not displayed. States include:</p> <p>Initiated—Call has begun but has not yet been accepted by the call's destination.</p> <p>Accepted—Call has been initiated and accepted by the destination, but not yet established as a two way voice session supported by the controller.</p> <p>Established—Call initiated, accepted by the destination, and in progress as a voice session supported by the controller.</p>
Call Codec	Displays the codec in use for the active calls.
R Factor	Displays the average call quality using the R Factor scale. The R Factor method rates voice quality on a scale of 0 to 120 with a higher score being better. If the R Factor score is lower than 70 it is likely that users will not be satisfied with the voice quality of calls.
MOS-CQ	Displays the average call quality using the Mean Opinion Score (MOS) call quality scale. The MOS scale rates call quality on a scale of 1-5 with higher scores being better. If the MOS score is lower than 3.5 it is likely that users will not be satisfied with the voice quality of calls.
Lost Packets	Displays the total number of voice packets lost for each MU.
Average Jitter	Displays the average jitter time for calls on the displayed MUs. Jitter is delays on the network that can result in a lag in conversations. A jitter score higher than 150ms is likely to be noticed by end users during a call.
Average Latency	Displays the average latency in milliseconds for calls on the selected MUs.
Start Time	Displays the start time for this call. This is the timestamp for the call as it is supported by the controller.

Viewing Access Port/Point Information

The *Access Points* screen displays a high-level overview of the APs created for use within the controller managed network. Use this data as necessary to check all the APs that are active, their VLAN assignments, updates to AP descriptions as well as their current authentication and encryption schemes.



NOTE

Up to 256 Access Points/Ports are supported by the Summit WM3600. Up to 1024 Access Points/Ports are supported by the Summit WM3700 controller. Up to 6 Access Points/Ports are supported by the Summit WM3400 controller. The actual number of Access Ports adoptable by a controller is defined based on Access Port or Adaptive AP licenses and on a per platform basis.



NOTE

The Extreme Networks Wireless Management Suite (WMS) is a recommended utility to plan the deployment of the controller and view its configuration once operational. Extreme Networks WMS can help optimize the positioning and configuration of a controller and Access Ports/Points in respect to a WLAN's MU throughput requirements. For more information, refer to the Extreme Networks website.

The Access Points screen consists of the following tabs:

- [Configuring Access Port/Point Radios on page 204](#)
- [Viewing AP Statistics on page 221](#)
- [Configuring WLAN Assignment on page 225](#)
- [Configuring WMM on page 227](#)
- [Configuring Access Point Radio Bandwidth on page 230](#)
- [Configuring Radio Groups for MU Load Balancing on page 231](#)
- [Viewing Active Calls \(AC\) Statistics on page 234](#)

Configuring Access Port/Point Radios

Refer to the *Configuration* tab to view existing radio configurations available to the controller. After reviewing the radios listed, you have the option of editing a radio's properties, deleting a radio, adding a new radio, resetting a radio, scanning available channels, or exporting a radio.

To view Access Point Radio configuration details:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Configuration* tab.

The screenshot shows the Summit WM3600 Controller web interface. The main content area is titled "Network > Access Point Radios" and includes several tabs: Configuration, Statistics, WLAN Assignment, WMM, Bandwidth, Group, VCAC Statistics, Mesh Statistics, Smart RF, and Voice Statistics. A note states: "Unconfigured radios are automatically adopted, use 'Global Settings' to change this option." Below this is a table with the following data:

Index	Description	AP Type	Type	Adopted	Parent AP MAC Address	MAC Address	State	VLAN
1	RADIO1	AP46X0	802.11bgn	✘	00-04-96-44-51-8C			
2	RADIO2	AP46X0	802.11an	✘	00-04-96-44-51-8C			
3	RADIO3	AP3510	802.11bg	✔	00-04-96-43-50-70	00-04-96-43-50-00	Normal	None
4	RADIO4	AP3510	802.11a	✔	00-04-96-43-50-70	00-04-96-43-50-C0	Normal	None

Below the table, it says "Filtering is disabled Page 1 of 1 loaded." At the bottom of the main content area, there are buttons for "Edit", "Delete", "Add", "Tools >", and "AP Mesh".

The "Properties" section at the bottom of the screenshot shows the following fields:

Property	Value
Desired Channel	--
Desired Power (dBm)	--
Placement	--
Secondary Channel	--
AP Manufacturer	--
BSSIDs	--
AP IP Address	--
Actual Channel	--
Actual Power	--
Last Adopted	--
Voice Calls	--

3 Refer to the table for the following information:

Controller	Displays the IP address of the cluster member associated with each Access Port/Point radio. When clustering is enabled on the controller and Cluster GUI is enabled, the <i>Controller</i> field will be available on the Access Port/Point radio configuration screen. For information on configuring enabling Cluster GUI, see "Managing Clustering Using the Web UI" on page 358.
Index	Displays the numerical index (device identifier) used with the device radio. Use this index (along with the radio name) to differentiate the radio from other device radios.
Description	Displays a user-assigned name for the radio.
AP Type	Use the Type to identify whether the radio is 802.11bg and 802.11bgn or 802.11a and 802.11an.
Type	Use the Type to identify whether the radio is 802.11b, 802.11bg and 802.11bn or 802.11a and 802.11an.

Adopted	Displays the radio's adoption status. If the radio is adopted, a green check displays. If the radio is not adopted, a red X displays.
Parent AP MAC Address	Displays the Access Port/Point's Ethernet MAC (the device MAC address that is printed on the casing of the unit). Do not confuse this BSSID MAC with the Access Port/Point's Ethernet MAC address.
MAC Address	The Base Radio MAC is the radio's first MAC address when it is adopted by the Controller.
State	Displays the radio's current operational mode. If the radio is set as a Detector AP, the state is "Detector", otherwise the state is "Normal".
VLAN	Displays the name of the VLAN currently used with each Access Port/Point radio.

4 Refer to the *Properties* field for the following:

Desired Channel	When the radio's channel is configured statically, the Actual Channel and Desired Channel are the same. If using ACS (<i>Automatic Channel Selection</i>), the controller selects a channel for the radio. The Desired Channel displays "ACS" and the Actual channel displays the channel selected for the radio. When set to Random, the applet determines the channel's designation.
Actual Channel	When the radio's channel is configured statically, the Actual Channel and Desired Channel are the same. If using ACS (<i>Automatic Channel Selection</i>), the controller selects a channel for the radio. The Desired channel displays "ACS" and the Actual Channel displays the channel selected for the radio.
Desired Power (dBm)	Displays the configured power setting in dBm for the selected radio. In most cases, the Desired Power and Actual Power are the same unless the desired power level would put the radio's output power outside the accepted regulatory compliance range.
Actual Power	Displays the current power level in dBm for the selected radio. In most cases, the Desired Power and Actual Power are the same unless the desired power level would put the radio's output power outside the accepted regulatory compliance range.
Placement	When the radio is adopted using the default configuration, the power for the radio can be defined as "Indoor" or "Outdoor." However, some countries have restrictions for the use of outdoor radios. If using a value of "Outdoor", verify if it is in compliance with the country of operation's regulatory restrictions.
AP Manufacturer	Displays the company name that manufactured the Access Point.
BSSIDs	Displays the Basic Service Set IDs.
Secondary Channel	Displays the channel number of a secondary channel. 802.11 n specification allows the use of two channels for radios when a 40-MHz channel bandwidth is selected. A 40-MHz channel can be considered to consist of two 20-MHz channels referred to as "primary" and "secondary". The primary channel is used for n clients who only support 20-MHz channels and legacy clients. Using two channels improves the performance of the wireless connection.
Last Adopted	Displays the time this radio was last adopted by the controller.
AP IP Address Mask	Displays the net mask address associated with the selected Access Port IP Address.
Voice Calls	Displays the current number of active voice calls for the selected radio.

5 Click the *Edit* button to launch a screen used to configure radio-specific parameters. For more information, see ["Editing AP Settings" on page 212](#).

6 Click the *Delete* button to remove a radio. However, before a radio can be removed, the radio's BSS mapping must be removed.

-
- 7 Click the *Add* button to add a radio. The radio must be added before the radio can be adopted. For more information, see [“Adding APs” on page 219](#).
 - 8 Click the *Reset* button to reset an individual radio.
 - 9 Click the *Tools >* button to display a submenu with *Reset*, *Run ACS*, and *Export* options.
Select the *Reset* option to reset the Access Port/Point radio. Select the *Run ACS Now* option to scan all channels and discover which radios are adopted and on what channel. ACS then analyzes the radios' channels and moves the radio to the channel where it is least likely to have interference from the other radios. Use the *Export* option to move the contents of the table to a *Comma Separated Values* file (CSV).
 - 10 Select an AP from the table and click the *AP Mesh* button to configure a mesh network.
 - 11 When using clustering and the Cluster GUI feature is enabled, a pull-down menu will be available to select which cluster members' Access Port/Point radios are displayed. To view Access Port/Point radios from all cluster members, select *All* from the pull-down menu. To view Access Port/Point radios from a specific cluster member, select that member's IP address from the pull-down menu.
 - 12 Click the *Global Settings* button to display a screen with settings applying to all radios on the system. For more information, see [“Configuring an AP's Global Settings” on page 209](#).

Configuring an AP Mesh Network

Use the *AP Mesh* screen to configure mesh network settings for the selected Access Point.

To configure AP Mesh:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Configuration* tab.

- Click the *AP Mesh* button to display a screen containing AP Mesh settings, which apply to the selected AP.

- To use the AP as a Base Bridge, check the *Base Bridge* checkbox and configure the following information:

Maximum Number of Client Bridges	When a radio has been configured as a Base Bridge, specify the maximum number of client bridges that can connect to the Base Bridge.
----------------------------------	--

- To use the AP as a Client Bridge, check the *Client Bridge* checkbox and configure the following information:

Mesh Network Name	When Client Bridge is enabled, enter the name of the Mesh Network that the selected radio will be a Client Bridge on.
-------------------	---

Max Client Bridge Mesh Associations	When Client Bridge is enabled, specify the maximum number of base bridges per client bridge in a an AP Mesh Network.
-------------------------------------	--

Client Bridge Signal Monitor	<p>The Client Bridge Signal Monitor feature continuously monitors the connection between the Client Bridge and the Base Bridge to which it is mesh connected to. When the signal strength of the Base Bridge falls below a configured threshold, the Client Bridge starts a periodic monitoring of the Base Bridge's signal strength for 60 seconds. This monitoring is abandoned if the signal strength becomes more than the configured threshold during the period of monitoring. When this happens, the monitoring period is reset back to 60 seconds. While this monitoring happens, the Client Bridge also passively listens to and monitors the signal strength of the other Base Bridges.</p> <p>If, at the end of 60 seconds, the Base Bridge's signal strength remains below the configured threshold, the Client Bridge compares the signal strength of the existing Base Bridge with the signal strength of each of the found Base Bridges. All Base Bridges with signal strength below the signal strength of the connected Base Bridge are ignored. Of the remaining Base Bridges, if the difference in signal strength is greater than the configured delta value, the connection to the existing Base Bridge is dropped and a new Base Bridge is selected based on the highest RSSI value. If the difference in signal strength is less than the configured delta value, the existing connection is maintained.</p> <p>Click to enable the device to monitor the signal strength of the base bridge to which it is connected.</p>
Client Bridge Signal Threshold	<p>This field configures the signal strength of the base bridge below which the device keeps monitoring the connection to the base bridge. The default value is 65 dbm.</p>
Client Bridge Signal Delta	<p>This value is the difference between the signal strength of the monitored base bridge and the found base bridges that causes the Client Bridge to drop its existing Base Bridge and establish a connection to a new Base Bridge.</p>
Mesh Time Out	<p>When Client Bridge is enabled, select either Enabled or Disabled to determine if the radio will time out mesh client associations.</p>

Configuring an AP's Global Settings

Use the *Global Settings* screen to define an adoption preference ID for the controller and enable an option to adopt non-configured radios. This can be helpful when you do not want to change an Access Port/Point's configuration but require the Access Port/Point be adopted.

To edit Global Radio configuration settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Click the *Global Settings* button to display a screen containing global settings, which apply to all radios on the controller.

- 4 Set an *Adoption Preference ID* value between 1 and 65535.

To define a radio as preferred, the Access Port/Point preference ID should be the same as the adoption preference ID. The adoption preference ID is used for AP load-balancing. A controller will preferentially adopt Access Ports/Points having the same adoption-preference-id as the controller itself.

The Adoption Preference ID defines the controller preference ID. The value can be between 1 and 65535. To define radios as preferred, the Access Port/Point preference ID should be the same as the adoption preference ID. If the value is set to 0, the controller automatically changes the value to 1.

In a Layer 3 environment, the Access Port/Point adoption process is somewhat unique. For more information, see [“Configuring Layer 3 Adoption”](#) on page 256.

- 5 To enable the automatic adoption of non-configured radios on the network, select the *Adopt unconfigured radios automatically* option. Default radio settings are applied to Access Ports/Points when automatically adopted. Enable this option to allow adoption even when the Access Port/Point is not configured. Default radio settings are applied to Access Ports/Points adopted automatically.
- 6 To limit the number of voice-enabled MUs which are associated, click the *Voice Call Admission Control* checkbox. Limiting voice MU traffic in a supported WLAN is a good idea to maintain data rates, voice quality, and throughput. WMM admission control is a mechanism for limiting traffic on a given access category. Per the recommendation of the 802.11e specification, Extreme Networks limits support of this feature to voice and video.



NOTE

Admission control is disabled by default. To enable it, configure from the controller. It is supported only on AP4600s.

- 7 To use WIPS, enter a *Primary WIPS Server Address* and *Secondary WIPS Server Address* into the corresponding fields.

**NOTE**

When using an AP35XX and AP4700 for use with WIPS and as a sensor, you must first configure the WIPS server IP Addresses before converting the AP35XX to a sensor.

- 8 Click the *Configure Port Authentication* button to open a new dialogue with port authentication configuration information.
- 9 Click *OK* to save the changes and return to the previous screen.

Port Authentication. To configure the port authentication settings on an Access Port/Point:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Click the *Global Settings* button.
- 4 Click the *Configure Port Authentication* button.
- 5 Enter the 802.1x *Username* assigned to the Access Port/Point.

Configure Port Authentication

Configure Port Authentication

Username

Password

Use Default Values

Warning: improper settings can stop radios from working!

Status:

- 6 Enter the 802.1x *Password* (for the corresponding username) providing authorization for Access Port/Point authorization adoption.

**NOTE**

The default user name and password for AP4600 Series port authentication is a user name of admin and a password of admin123.

- 7 Check the *Use Default Values* option checkbox to set the username and password to factory default values. The Access Port/Point can get disconnected if the 802.1x authenticator is not configured accordingly.

**NOTE**

802.1x username and password information is only passed to adopted Access Ports/Points when the Username and Password are set. Any AP adopted after this does not automatically receive a username and password.



NOTE

After setting the username and password to factory default settings, the system must be rebooted before the factory default settings are applied.

- 8 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 9 Click *OK* to use the changes to the running configuration and close the dialog.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Editing AP Settings

The *Edit* screen provides a means of modifying the properties of an existing radio. This is often necessary when the radio's intended function has changed and its name needs modification or if the radio now needs to be defined as a detector radio. The *Edit* screen also enables you to modify placement, channel, and power settings as well as a set of advanced properties in case its transmit and receive capabilities need to be adjusted.



NOTE

The screen display can vary slightly depending on whether the Access Port/Point radio is an 802.11b, 802.11bg and 802.11bgn or 802.11a and 802.11an model.

To edit a radio's configuration:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Select a radio to edit from the table.

- Click the *Edit* button to display a screen containing settings for the selected radio.

Configuration RADIO1

Properties

Radio Descr.

Dedicate this AP as Detector AP

Single-channel scan for Unapproved APs

Enable Enhanced Beacon Table

Enable Enhanced Probe Table*

MAC Address

Radio Type 802.11a

Config Method Static

Group Id (0 - 64)

Radio Settings

Placement Actual

Desired Channel unset

Antenna Gain* (0.0 - 15.0 dBi)

Desired Power (dBm) unset 100 mW

Advanced Properties

Antenna Diversity

RTS Threshold (0 - 2346) bytes

Maximum MUs* (1 - 256)

Beacon Interval (50 - 200) K-us

Adoption Preference ID (0 - 65535)

Self Healing Offset (0 - 20) dBm

Dynamic Chain Select

Admission Control Settings*

Max. Admitted MUs for Voice Traffic (0 - 256)

Max. Airtime for Voice %

Max. Roamed MUs for Voice Traffic (0 - 256)

Max. Airtime Reserved for Roaming %

802.11k RRM Settings

Enable 802.11k RRM Enable Quiet Element

Quiet Time (20 - 150) K-us

Quiet Interval (200 - 255) No. of Beacons

Status:

- The *Controller* field displays the IP address of the cluster member associated with each Access Point/Point radio. When clustering is enabled on the controller and Cluster GUI is enabled, the *Controller* field will be available on the Access Point/Point Radio edit screen. For information on configuring and enabling Cluster GUI, see [“Managing Clustering Using the Web UI”](#) on page 358.
- In the *Radio Descr.* field, enter a brief description to differentiate the radio. The description is used to describe radios of the same type and can be used to locate a radio if there are any problems.

- 7 Select the *Dedicate this AP as Detector AP* option to use this radio as a detector port to identify rogue APs on the network.

Setting this radio as a detector dedicates the radio to detect rogue APs on the network. Dedicated detectors do not connect to clients.

- 8 Select the *Single-channel scan for Unapproved APs* checkbox to enable the controller to scan for rogue devices using the radio's current channel of operation.
- 9 Select the *Enable Enhanced Beacon Table* checkbox to allow adopted Access Port or Access Point radios to scan for potentially unauthorized APs across all bands.

This option utilizes radio bandwidth, but is an exhaustive means of scanning across all available channels and listening for AP beacon traffic. Once probe responses are received, a network device management application like Extreme Networks WMS or the *Wireless Intrusion Detection System* (WIPS) can locate the device and remove it if defined as unauthorized.

- 10 Select the *Enable Enhanced Probe Table* checkbox to enable an adopted Access Port or Access Point radio to forward the probes required to obtain MU RSSI information.

RSSI data (as obtained by at least three detecting radios) can be used by the Extreme Networks WMS application to triangulate the location of an MU on a site map representative of the actual physical dimensions of the controller radio coverage area. Once located on a site map, intuitive decisions can be made regarding the MU's authorization within the controller-managed network.

- 11 The following read-only information is displayed:

MAC Address	The Base Radio MAC is the radio's first MAC address when it is adopted by the Controller.
Radio Type	Radio type identifies whether the radio is an 802.11bg and 802.11bgn or 802.11a and 802.11an radio.
Config Method	The Config Method displays whether the radio has been configured using static or dynamic settings.

- 12 To add the radio to a Radio Group, enter the *Group ID* for the radio group you wish to add it to. For more information on configuring Radio Groups, see [“Configuring Radio Groups for MU Load Balancing”](#) on page 231.

- 13 From within the *Radio Settings* field, define the *Placement* of the Access Port/Point as either *Indoors* or *Outdoors*.

An Access Port/Point can be set for Indoors or Outdoors use depending on the model and the placement location. Power settings and channel selection options differ based on each country's regulatory rules and whether or not the unit is placed indoors or outdoors.

Channel Width is the distance between two channels in the same frequency. This difference is measured in MHz. For type 'an' channels, the channel width is either 20 MHz or 40 MHz. For type 'bgn' channels, the width is 20 MHz. This field is read-only and is available only with type 'n' radios.

Desired Channel (sec) is the channel for communication between the Access Ports and MUs using the secondary radio of an AP having multiple radios. The selection of a channel determines the available power levels. The range of legally approved communication channels varies depending on the installation location and country. The selected channel can be a specific channel, Random, or ACS. Random assigns each radio a random channel. ACS (Automatic Channel Selection) allows the controller to systematically assign channels. Default is Random. Select a channel for communications between the Access Port and its associated MUs within the *Desired Channel* field.

The channel for communication between the Access Port and its associated MUs can be using the primary radio or the secondary radio of an AP. Accordingly the channel is called *Desired Channel (Pri)* or *Desired Channel (Sec)* respectively. The selection of a channel determines the available power levels. The range of legally-approved communication channels varies depending on the installation

location and country. The selected channel can be a specific channel, "Random," or "ACS." Random assigns each radio a random channel. ACS (*Automatic Channel Selection*) allows the controller to systematically assign channels. Default is Random.

- 14 After first selecting a channel, select a power level in dBm for RF signal strength in the *Desired Power (dBm)* field.

The optimal power level for the specified channel is best determined by a site survey prior to installation. Available settings are determined according to the selected channel. Set a higher power level to ensure RF coverage in WLAN environments that have more electromagnetic interference or greater distances between the Access Port/Point and MUs. Decrease the power level according to the proximity of other Access Ports/Points. Overlapping RF coverage may cause lost packets and problems for roaming devices trying to connect to an Access Port/Point. After setting a power level, channel, and placement the RF output power for the Access Port/Point is displayed in mW. The default is 20 dBm (802.11bg), 17 dBm (802.11a).



NOTE

After setting a power level, channel, and placement, the RF output power for the Access Port/Point displays in mW.

- 15 *Antenna Gain* relates the intensity of an antenna in a given direction to the intensity that would be produced by a hypothetical antenna that radiates equally in all directions and has no losses.
- 16 *Radio-Mode* displays the radio operating mode.



NOTE

This field is available only with AP 7131, AP 7181, and AP 650.

- 17 To configure optional rate settings, click the *Rate Settings* button to display a new dialogue containing rate setting information. Instructions on configuring rate settings is described in "[Configuring Rate Settings](#)" on page 218.
- 18 In most cases, the default settings for the *Advanced Properties* are sufficient. If needed, additional Advanced Properties can be modified for the following:

- | | |
|-------------------|---|
| Antenna Diversity | Use the drop-down menu to configure the Antenna Diversity settings for Access Ports using external antennas. Options include: <ul style="list-style-type: none">• <i>Full Diversity</i>—Utilizes both antennas to provide antenna diversity.• <i>Primary Only</i>—Enables only the primary antenna.• <i>Secondary Only</i>—Enables only the secondary antenna.• MIMO: Multiple-Input and Multiple-Output. This field is only available with type 'n' radios. |
|-------------------|---|

Antenna Diversity should only be enabled if the Access Port has two matching external antennas. Default value is *Full Diversity*.

- | | |
|------------------------|--|
| Maximum MUs | Sets the maximum number of MUs that can associate to a radio. The maximum number of MUs that can associate to a radio is 64. |
| Adoption Preference ID | Displays the preference ID of the controller. The value can be set between 1 and 65535. To define the radios as preferred, the Access Port preference ID should be the same as adoption preference ID. <p>The adoption preference ID is used for AP load-balancing. A controller will preferentially adopt APs, which have the same adoption-preference-ID as the controller itself.</p> |

Short Preambles only	<p>If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This checkbox does not display if using an 802.11a radio.</p>
RTS Threshold	<p>Specify a Request To Send (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.</p> <p>RTS is a transmitting station's signal that requests a Clear To Send (CTS) response from a receiving station. This RTS/CTS procedure clears the air where many MUs are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.</p> <p>Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.</p> <p>Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Ports. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.</p> <p>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold. Default is 2346.</p> <p>In 802.11b/g mixed RTS/CTS happens automatically. There is no way to disable RTS/CTS unless the network and all the devices used are 802.11g or 802.11a only. The proper co-existence of 802.11b and 802.11g is ensured through RTS/CTS mechanism. On 802.11g radios, CTS-to-self is enabled irrespective of whether or not 11b rates are enabled or disabled.</p> <p>When ERP Protection is ON, the 11bg radio will perform a CTS-to-self before it transmits the frame.</p>
Beacon Interval	<p>Specify a beacon interval in units of 1,024 microseconds (K-us). This is a multiple of the DTIM value, for example, 100: 10. (See "DTIM Period" below). A beacon is a packet broadcast by the adopted Access Ports to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the radio-port address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default is 100 K-us.</p>
Self Healing Offset	<p>When an Access Port increases its power to compensate for a failure, power is increased to the country's regulatory maximum. Set the Self Healing Offset to reduce the country's regulatory maximum power if Access Ports are situated close to each other or if an Access Port uses an external antenna.</p>

DTIM Periods	Select the <i>DTIM periods</i> button to specify a period for <i>Delivery Traffic Indication Messages</i> (DTIM) for BSS IDs 1-4. This is a divisor of the beacon interval (in milliseconds), for example, 10:100. (See “Beacon Interval” above). A DTIM is periodically included in the beacon frame transmitted from adopted Access Ports. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates broadcast and multicast frames (buffered at the Access Port) are soon to arrive. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default DTIM period is 10 beacons for BSS 1-4.
Dynamic Chain Select	When enabled, the Dynamic Chain Selection option forces the radio to transmit all packets utilizing legacy transmission rates (e.g. 11b, 11g and/ or 11a rates) with a single transmit chain. Transmissions utilizing 11n rates (e.g. MCS0 – MCS15) will continue to use the normal number of transmit chains.
Aggregation	This allows the type ‘n’ packets to be aggregated before transmission. This feature is available only for type ‘n’ radios.

19 When the *Voice Call Admission Control* is enabled in the *Global Settings*, the *Admission Control Settings* section allows you to modify the following properties.

Max Admitted MUs for Voice Traffic	Specify the maximum number of MUs allowed to connect to the specified radio for voice traffic. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality.
Max Roamed MUs for Voice Traffic	Specify the maximum number of voice MUs that are allowed to roam to this radio. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality.
Max Airtime for Voice	Specify a maximum percentage out of the radio's total airtime that may be used for voice.
Max Airtime for Reserved Roaming	Specify a maximum percentage out of the radio's total airtime that may be used for voice MUs which roam from other APs.

20 The dot11k Functionality for this radio can be enabled in the dot11k Settings section by checking the Enable dot11k checkbox. The quiet element associated with 802.11k can be configured if the quiet element is enabled for the radio by checking the “Enable Quiet Element” checkbox.

Quiet Time	The Quiet Time defines the Quiet Duration field in the Quiet Element IE and shall be set to the duration of the quiet interval, expressed in TUs. In user terms it can be defined as the duration in which no transmit/receive will happen.
Quiet Interval	The Quiet Interval indicates the Quiet Period in the Quiet Element IE and shall be set to the number of beacon intervals between the start of regularly scheduled quiet interval as defined in this Quiet element. In user terms it can be defined like how often the no transmit/receive will be repeated.

21 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

22 If clustering is configured and the Cluster GUI feature is enabled, the *Apply to Cluster* feature will be available. Click the *Apply to Cluster* button to apply the AP radio settings to all members in the cluster.

**NOTE**

When Cluster GUI is enabled and an Access Port/Point configuration is deleted from one controller, it is not automatically deleted from other controllers in the cluster.

23 Click *OK* to use the changes to the running configuration and close the dialog.

24 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Rate Settings. Use the *Rate Settings* screen to define a set of basic and supported rates for the target radio. This allows the radio to sync with networks using varying data rates and allows the radio to default to a predefined set of data rates when higher data rates cannot be maintained.

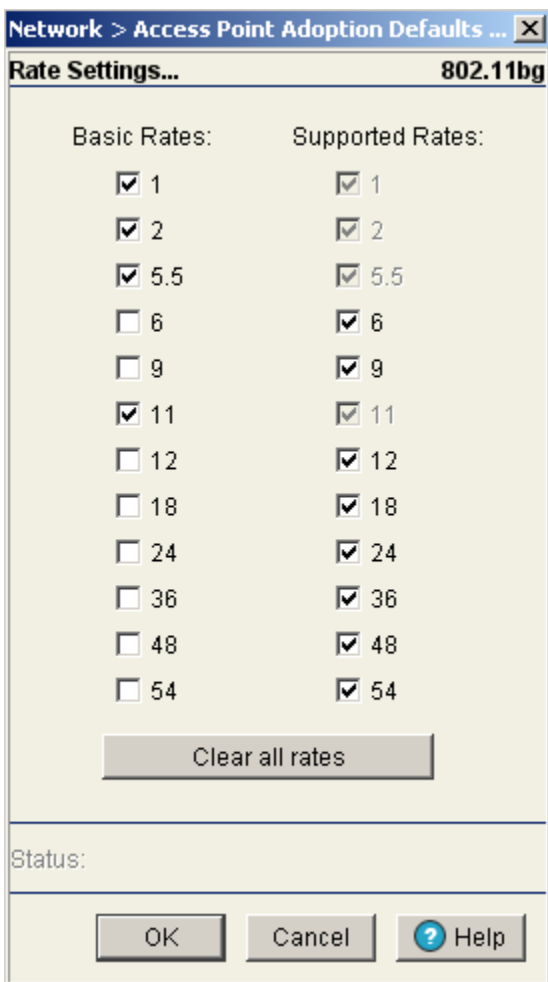
To configure Rate Settings for a radio:

1 Click the *Rate Settings* button within the radio edit screen to launch a new screen with rate setting information.

2 Check the boxes next to all the *Basic Rates* you want supported.

Basic Rates are used for management frames, broadcast traffic, and multicast frames. If a rate is selected as a basic rate, it is automatically selected as a supported rate.

3 Check the boxes next to all the *Supported Rates* you want supported.



Supported rates allow an 802.11 network to specify the data rate it supports. When an MU attempts to join the network, it checks the data rate used on the network. If a rate is selected as a basic rate, it is automatically selected as a supported rate. An 802.11a radio can support a maximum data rate of 54 Mbps.

- 4 Click the *Clear all rates* button to uncheck all of the Basic and Supported rates.



NOTE

For Altitude 4700 Series Access Points and Altitude 4600 Series Access Points the Rate Settings screen contains MCS data rates in addition to the basic rates. You can select the Enable Short Guard Interval option in the 11n Modulation Coding Schemes (MCS) section to increase the data rates. Checking the Enable Basic MCS0-7 option will allow only 11n capable clients to get connected to this radio.

- 5 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding APs

The *Add Radio* screen provides a facility for creating a new (unique) radio index for inclusion within the Configuration screen. Use the Add screen to add the new radio's MAC address and define its radio type.

To add a Radio to the controller:

- 1 Select *Network > Access Point Radios* from the main menu.
- 2 Click the *Configuration* tab.

- Click the *Add* button to display a screen containing settings for adding a radio

The screenshot shows the 'Add Radio' dialog box. The title bar reads 'Network > Access Point Radios > Add Radio'. The dialog is titled 'Add Radio'. It features the following fields and controls:

- AP MAC Address:** A text field containing five dashes (- - - - -).
- AP Type:** A dropdown menu with 'AP3550' selected. A list of options is visible: AP3510, AP3550 (highlighted), AP4700, and AP4600.
- Radio Settings:** A section containing four radio type checkboxes, each with a corresponding 'Radio Index' field and a range '(1 - 4096)':
 - 802.11a
 - 802.11bg
 - 802.11an
 - 802.11bgn
- Status:** A text field at the bottom left, currently empty.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

- Enter the device *MAC Address* (the physical MAC address of the radio). Ensure that this address is the actual hard-coded MAC address of the device.
- Use the *AP Type* drop-down menu to define the radio type you would like to add. If adding an Altitude 35xx or Altitude 4700 Series Access Point, the Access Port conversion will render the Access Point a “thin” Access Port.
- From the *Radio Settings* section, select the radio type checkboxes corresponding to the type of AP radio used. Available radio types are dependant on the *AP Type* selected above.
- Enter a numerical value in the *Radio Index* field for each selected radio.
The Radio Index is a numerical value assigned to the radio as a unique identifier. For example: 1, 2, or 3. The index is helpful for differentiating radios of similar type and configuration.
- Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- If clustering is configured and the Cluster GUI feature is enabled, the *Apply to Cluster* feature will be available. Click the *Apply to Cluster* button to apply the AP radio settings to all members in the cluster.
- Click *OK* to use the changes to the running configuration and close the dialog.
- Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing AP Statistics

Refer to the *Statistics* tab for information and high-level performance data for individual radios. Performance information can be reviewed for either a 30 second or one hour interval. Use the *Details* button to display additional information for an individual radio.

To view Radio Statistics:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Statistics* tab.

The screenshot shows the Summit WM3600 Controller interface. The main content area is titled "Network > Access Point Radios" and has tabs for Configuration, Statistics, WLAN Assignment, WMM, Bandwidth, Group, VCAC Statistics, Mesh Statistics, Smart RF, and Voice Statistics. The "Statistics" tab is active. Above the table, there are radio buttons for "Last 30s" (selected) and "Last Hr". A "Show Filtering Options" link is present above the table. The table has the following data:

Index	Description	Type	MUs	Throughput Mbps	ABS	RF Util	% Non-UNI	Retries
3	RADIO3	802.11bg	1	0.0	1.0	0.02%	28.57	0.0
4	RADIO4	802.11a	1	0.0	6.0	0.0%	50.0	0.0

Below the table, it says "Filtering is disabled". At the bottom of the interface, there are buttons for "Details", "Graph", "Save", "Logout", "Refresh", and "Help".

- 3 To select the time frame for the radio statistics, select either *Last 30s* or *Last Hr* above the statistics table.

- Select the *Last 30s* radio button to display statistics for the last 30 seconds for the radio.
- Select the *Last Hr* radio button to display statistics from the last hour for the radio.

- 4 Refer to the table for the following information:

Index Displays the numerical index (device identifier) used with the radio. Use this index (along with the radio name) to differentiate the radio from other device radios.

Description	Displays the name used with the radio. Use this name (along with the radio index) to differentiate the radio from other device radios.
Type	Identifies whether the radio is an 802.11bg and 802.11bgn or 802.11a and 802.11an radio.
MUs	Displays the number of MUs currently associated with the Access Point.
Throughput Mbps	Displays the average throughput in Mbps for the selected radio. The Rx column displays the average throughput in Mbps for packets received on the selected radio. The Tx column displays the average throughput for packets sent on the selected radio.
ABS	Displays the average bit speed in Mbps on the selected Access Port. This value includes packets both sent and received.
RF Util	Displays the percentage of the total packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
% Non-UNI	Displays the percentage of packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the average number of retries for all MUs associated with the selected radio.

- 5 Select a radio from those displayed and click the *Details* button for additional radio information. For more information, see [“Viewing AP Statistics in Detail” on page 222](#).
- 6 Select a radio from those displayed and click the *Graph* button for additional radio performance information in graphical format. For more information, see [“Viewing AP Statistics in Detail” on page 222](#).

Viewing AP Statistics in Detail

The *Details* screen provides additional (and more specific) traffic, performance, and error information for the selected radio.

To view Radio Statistics Details:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Statistics* tab.
- 3 Select a radio from the table and click the *Details* button to display a screen with detailed statistics for that radio.

Radio statistics details are split into four fields: *Information*, *Traffic*, *RF Status*, and *Errors*. Information in black represents the statistics from the last 30 seconds and information in blue represents statistics from the last hour.

- 4 Refer to the *Information* field for the following information:

Description	Displays a brief description of the radio to help differentiate the radio from similar models.
MAC Address	Displays the Hardware or <i>Media Access Control (MAC)</i> address for the Access Port/Point. Access Ports/Points with dual radios will have a unique hardware address for each radio.
Num Associated Stations	Displays the number of MUs currently associated with the radio.
Radio Type	Displays the Access Port/Point model.

Current Channel	Displays the channel the Access Port/Point is currently passing traffic on. If the channel is displayed in red, it means the configured channel does not match the current channel. The configured channel, in this case, is the value in parentheses. The AP may not be operating on the configured channel for 2 reasons: Uniform spreading is enabled or radar was encountered on the configured channel.
-----------------	--

5 Refer to the *Traffic* field for the following information:

Pkts per second	Displays the average total packets per second that cross the selected radio. The Rx column displays the average total packets per second received on the selected radio. The Tx column displays the average total packets per second sent on the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Throughput	Displays the average throughput in Mbps on the selected radio. The Rx column displays the average throughput in Mbps for packets received on the selected radio. The Tx column displays the average throughput for packets sent on the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Avg Bit Speed	Displays the average bit speed in Mbps on the selected radio. This includes all packets that are sent and received. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
Non-unicast Pkts	Displays the percentage of the total packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.

6 Refer to the *RF Status* field for the following information:

Avg MU Signal	Displays the average RF signal strength in dBm for all MUs associated with the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Avg MU Noise	Displays the average RF noise for all MUs associated with the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
Avg MU SNR	Displays the average <i>Signal to Noise Ratio</i> (SNR) for all MUs associated with the selected radio. The Signal to Noise Ratio is an indication of overall RF performance on your wireless network.

7 Refer to the *Errors* field for the following information:

Avg Num of retries	Displays the average number of retries for all MUs associated with the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
% Gave Up Pkts	Displays the percentage of packets the controller gave up on for all MUs associated with the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.
% of Undecryptable Pkts	Displays the percentage of undecryptable packets for all MUs associated with the selected radio. The number in black represents this statistics for the last 30 seconds and the number in blue represents this statistics for the last hour.

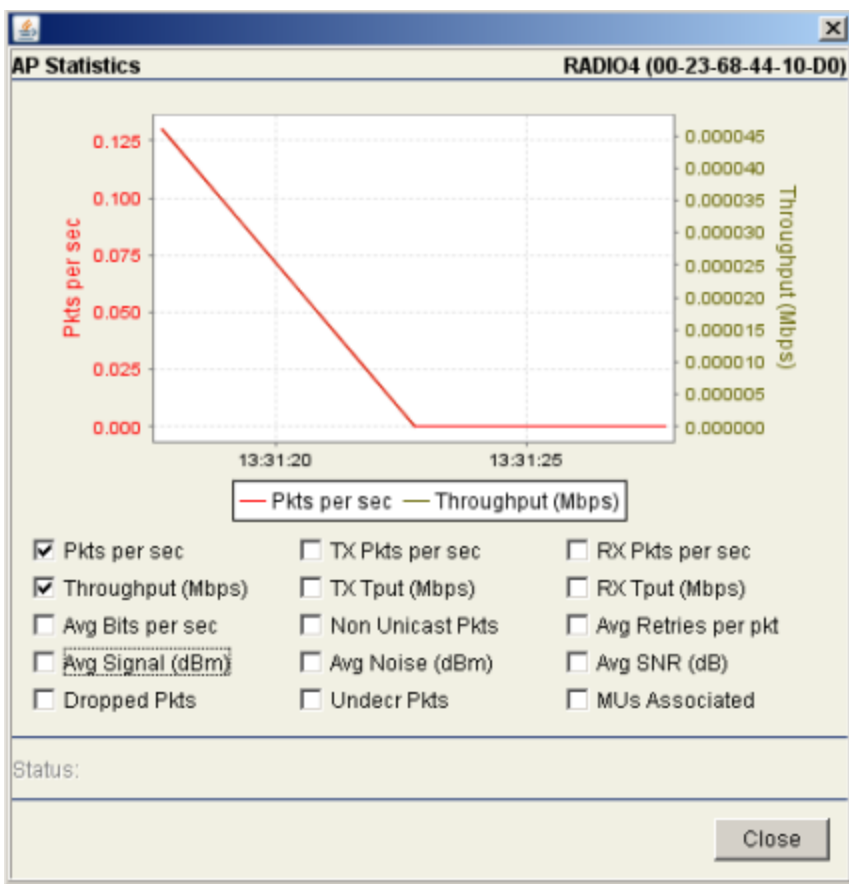
- 8 Click *Refresh* to update the content of the screen with the latest values.
- 9 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing AP Statistics in Graphical Format

The *Statistics* tab has an option for displaying detailed Access Port/Point radio statistics in a graph. This information can be used to chart associated controller radio performance and help diagnose radio performance issues.

To view the MU Statistics in a graphical format:

- 1 Select a *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Statistics* tab.
- 3 Select a radio index from the table displayed in the *Statistics* screen and click the *Graph* button.



- 4 Select a checkbox to display that metric charted within the graph. Do not select more than four checkboxes at any one time.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *Close* to exit the Graph and return to the parent Access Port/Point Radios Statistics screen.

Configuring WLAN Assignment

The *WLAN Assignment* tab displays a high-level description of the radio. It also displays the radios WLAN and BSSID assignments on a panel on the right-hand side of the screen.

To view existing WLAN Assignments:

- 1 Select *Network > Access Port/Point Radios* from the main menu tree.
- 2 Click the *WLAN Assignment* tab.
- 3 Select a radio from the table to view WLAN assignment information.

The screenshot shows the Summit WM3600 Controller interface. The main content area is titled "Network > Access Point Radios" and has tabs for Configuration, Statistics, WLAN Assignment (selected), WMM, Bandwidth, Group, VCAC Statistics, Mesh Statistics, Smart RF, and Voice Statistics. Below the tabs is a "Select Radios" table with the following data:

Index	Description	Type	AP Mac
1	RADIO1	802.11bgn	00-04-96-44-51-8C
2	RADIO2	802.11an	00-04-96-44-51-8C
3	RADIO3	802.11bg	00-04-96-43-50-70
4	RADIO4	802.11a	00-04-96-43-50-70

Below the table is a "Page 1 of 1 loaded." message and an "Edit" button. To the right of the table is a panel titled "Assigned WLANs" showing a tree view with "noSuchInstance" and "1 - RADIO1 - 802.11bgn". Under "1 - RADIO1 - 802.11bgn", there is a "BSS-ID" column and an "Assigned WLANs" column. The BSS-ID "1" is selected, and its assigned WLAN is "ESS ID : test-4600bgn-". The other BSS-IDs (2, 3, 4) are listed as "No WLANs Assigne".

The *WLAN Assignment* tab is divided into two fields: *Select Radios* and *Assigned WLANs*.

- 4 Refer to the *Select Radios* field for the following information:

Index	Displays the numerical index (device identifier) used with the radio. Use this index (along with the radio description) to differentiate the radio from other radios with similar configurations.
Description	Displays a description of the Radio. Modify the description as required to name the radio by its intended coverage area or function.
Type	Displays whether the radio is an 802.11bg and 802.11bgn or 802.11a and 802.11an radio.

AP Mac Displays the MAC address of the port in AA-BB-CC-DD-EE-FF format.

The *Assigned WLANs* field displays the WLANs associated to each BSSID used by the radios within the radio table. There can be up to 16 WLANs associated with each BSS. Out of these, one WLAN must be the primary WLAN.

- 5 Select a WLAN Assignment (by index) and click the *Edit* button to modify its properties. For more information, see [“Editing a WLAN Assignment” on page 226](#).
- 6 To remove an existing WLAN from the list available for WLAN assignment, select the WLAN and click the *Delete* button.

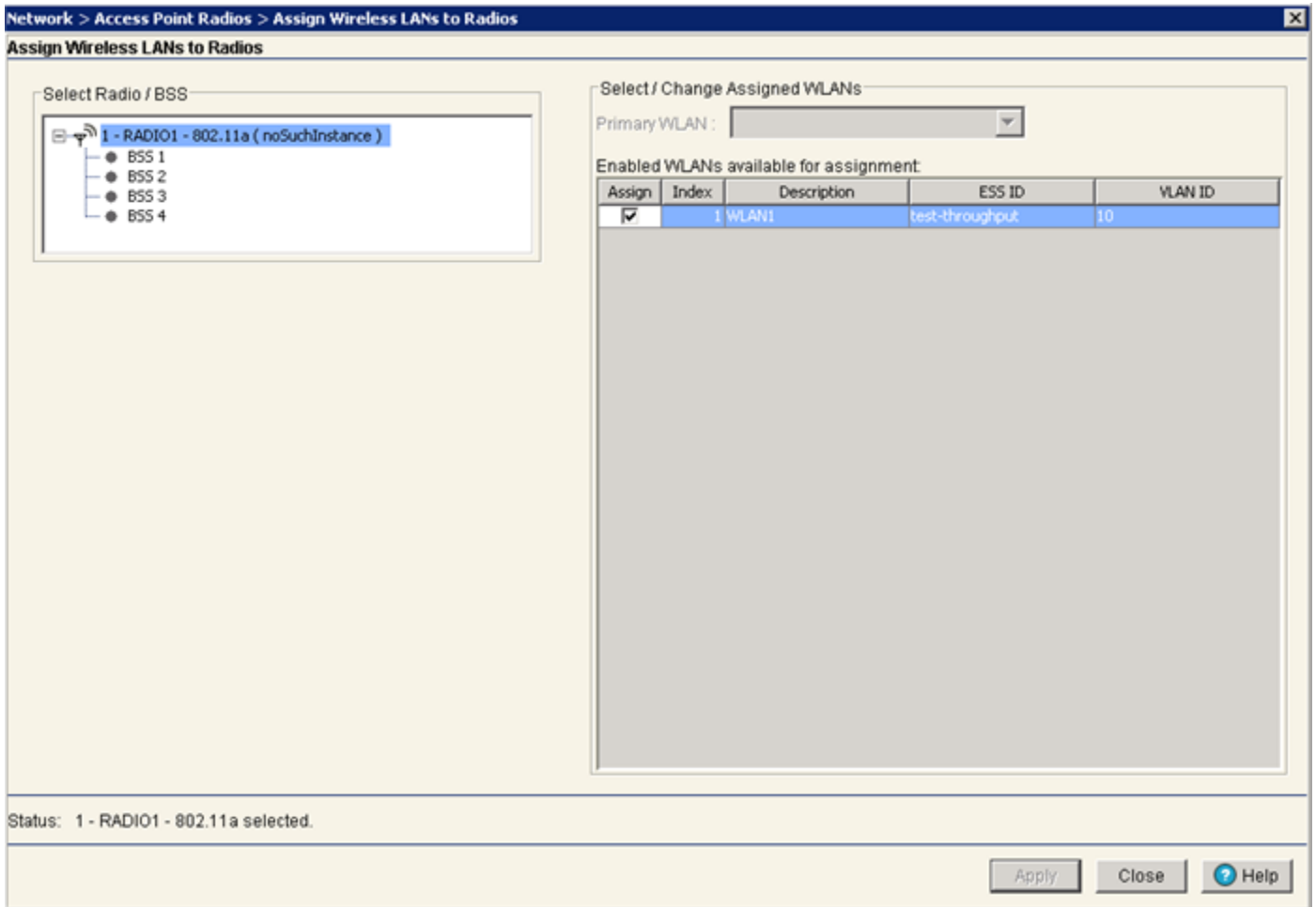
Editing a WLAN Assignment

The properties of an existing WLAN assignment can be modified to meet the changing needs of your network.

To edit an existing WLAN assignment:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *WLAN Assignment* tab.
- 3 Select a radio from the table and click the *Edit* button.

The *Select Radio/BSS* field displays the WLANs associated to each of the BSSIDs used by the radios within the radio table. Use *Select/Change Assigned WLANs* field to edit the WLAN assignment.



- 4 Select any of the WLANs from the table to unassign/disable it from the list of available WLANs.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click the *Apply* button to save the modified WLAN assignment.
- 7 Click *Close* to exit the screen without committing updates to the running configuration.

Configuring WMM

Use the *WMM* tab to review each radio's current index (numerical identifier), the Access Category that defines the data type (Video, Voice, Best Effort, and Background) as well as the transmit intervals defined for the target access category.

To view existing WMM Settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *WMM* tab.

SUMMIT® WM3600 CONTROLLER

Network > Access Point Radios

Configuration | Statistics | WLAN Assignment | **WMM** | Bandwidth | Group | VCAC Statistics | Mesh Statistics | Smart RF | Voice Statistics

Show Filtering Options

Index	AP	Access Category	AIFSN	Transmit Ops	ECW Min	ECW Max
1/1	RAD1O1	Best Effort	3	0	4	6
1/2	RAD1O1	Background	7	0	4	10
1/3	RAD1O1	Video	1	94	3	4
1/4	RAD1O1	Voice	1	47	2	3
2/1	RAD1O2	Best Effort	3	0	4	6
2/2	RAD1O2	Background	7	0	4	10
2/3	RAD1O2	Video	1	94	3	4
2/4	RAD1O2	Voice	1	47	2	3
3/1	RAD1O3	Best Effort	3	0	4	6
3/2	RAD1O3	Background	7	0	4	10
3/3	RAD1O3	Video	1	94	3	4
3/4	RAD1O3	Voice	1	47	2	3
4/1	RAD1O4	Best Effort	3	0	4	6
4/2	RAD1O4	Background	7	0	4	10
4/3	RAD1O4	Video	1	94	3	4
4/4	RAD1O4	Voice	1	47	2	3

Filtering is disabled

Save Logout Refresh Edit Help

Wireless Management Applet

WMM information displays per radio with the following information:

- Index** Displays the identifier assigned to each Radio index. Each index is assigned a unique identifier such as (1/4, 1/3, etc.).
- AP** Displays the name of the Access Port/Point associated with the index. The Access Port/Point name comes from the description field in the *Radio Configuration* screen.
- Access Category** Displays the Access Category currently in use. There are four categories: Video, Voice, Best Effort, and Background. Click the *Edit* button to change the current Access Category. Ensure the Access Category reflects the radio's intended network traffic.
- AIFSN** Displays the current Arbitrary Inter-frame Space Number (Check). Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before trying to access the medium.
- Transmit Ops** Displays the maximum duration a device can transmit after obtaining a transmit opportunity.

ECW Min	Displays the ECW Max to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
ECW Max	Displays the ECW Min to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.

- 3 Use the Filter Options facility (by clicking the *Show Filter Options* link) to specify if information is filtered by Index (default setting), AP, Access Category, AIFSN, Transmit Ops, CW Min, or CW Max. Select *Turn Filtering Off* to disable filtering.
- 4 Select a radio and click the *Edit* button to modify its properties. For more information, see [“Editing WMM Settings” on page 229](#).

Editing WMM Settings

Use the *Edit* screen to modify a WMM profile's properties (AIFSN, Tx Op, Cw Min, and CW Max). Modifying these properties may be necessary as Access Categories are changed and transmit intervals need to be adjusted to compensate for larger data packets and contention windows. Use [“Configuring WMM” on page 227](#) to configure downstream traffic parameters. WLAN WMM configuration affects your upstream traffic parameters.

To edit existing WMM Settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *WMM* tab.
- 3 Select a radio from the table and click the *Edit* button to launch a screen displaying the WMM configuration for that radio.

- 4 Enter a number between 0 and 15 for the *AIFSN* value for the selected radio.
The AIFSN value is the current Arbitrary Inter-frame Space Number. Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before trying to access the medium.
- 5 Enter a number between 0 and 65535 for the *Transmit Ops* value.

The Transmit Ops value is the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set higher.

- 6 Enter a value between 0 and 15 for the Extended Contention Window minimum (*ECW Min*) value. The *ECW Min* is combined with the *ECW Max* to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority (video or voice) traffic.
- 7 Enter a value between 0 and 15 for the Extended Contention Window maximum (*ECW Max*) value. The *ECW Max* is combined with the *ECW Min* to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority (video or voice) traffic.
- 8 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 9 Click *OK* to use the changes to the running configuration and close the dialog.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Access Point Radio Bandwidth

Refer to the *Bandwidth* tab to view the QoS weight associated with each radio when added to a WLAN. The weight represents the controller priority assigned to the traffic transmitted from the radio for the WLAN.

For information on revising the weight assigned to each radio in respect to its intended operation within its assigned WLAN, see [“Editing the WLAN Configuration” on page 134](#).

To view existing radio bandwidth weight settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Bandwidth* tab.

SUMMIT® WM3600 CONTROLLER

Network > Access Point Radios

Configuration | Statistics | WLAN Assignment | WMM | **Bandwidth** | Group | VCAC Statistics | Mesh Statistics | Smart RF | Voice Statistics

Show Filtering Options <<< Page 1 of 1 Go >>>

Index	Description	QoS Weight
1	RADIO1	WLAN 4 bw = 100%
2	RADIO2	WLAN 3 bw = 100%
3	RADIO3	WLAN 6 bw = 100%
4	RADIO4	WLAN 4 bw = 100%

Filtering is disabled Page 1 of 1 loaded.

Save Logout Refresh Help

Bandwidth information displays per radio with the following data:

Index	The Index is the numerical index (device identifier) used with the device radio. Use this index (along with the radio name) to differentiate the radio from other device radios.
Description	The displayed name is the name used with the device radio. Use this name (along with the radio index) to differentiate the radio from other device radios.
QoS Weight	Displays the Quality of Service weight for the AP. The default value for the weight is 1. AP QoS will be applied based on the QoS weight value with the higher values given priority.

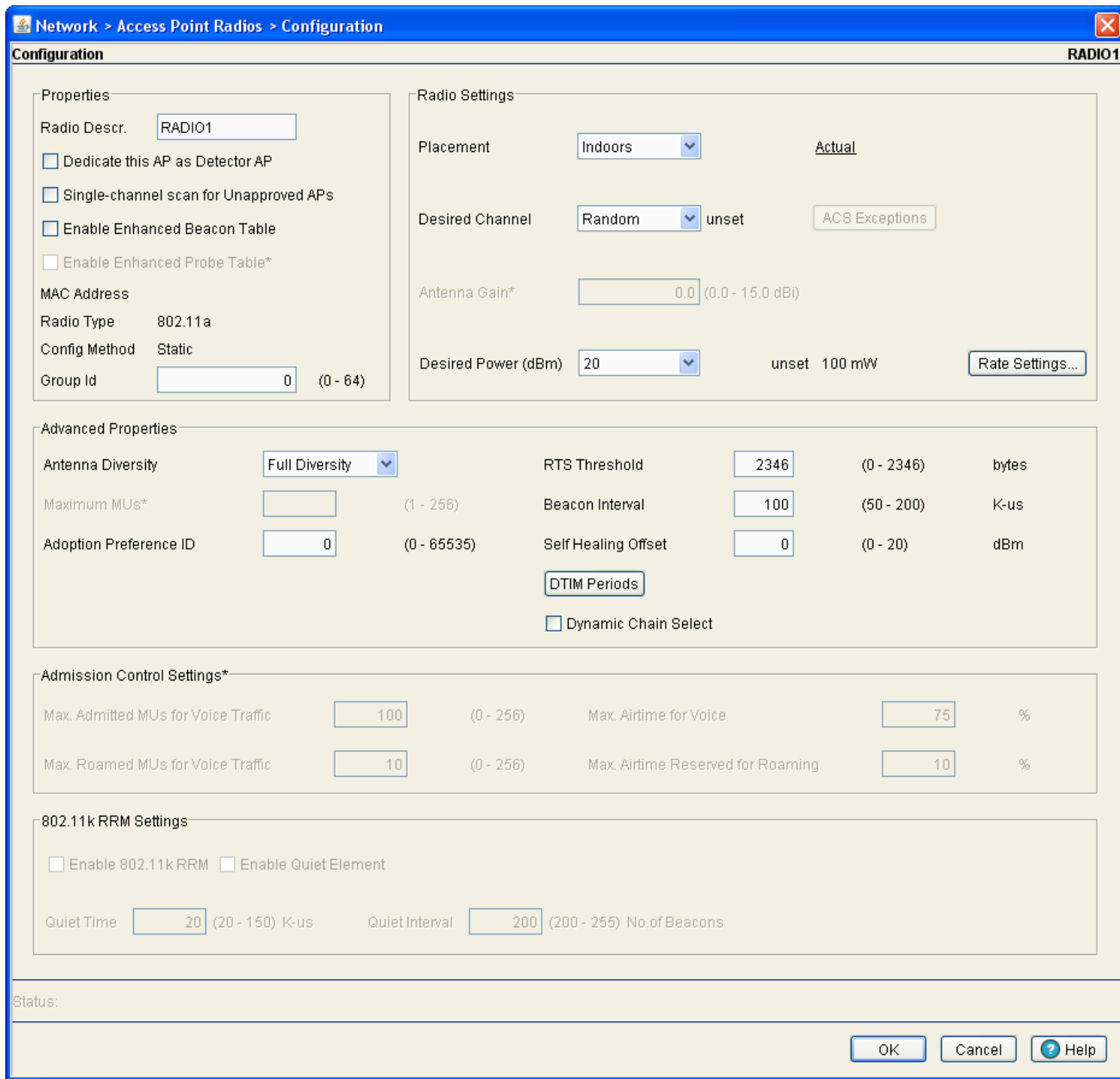
Configuring Radio Groups for MU Load Balancing

In order to do MU load balancing, radios must be grouped. Usually, two radios with similar characteristics and geographically close to each other can be grouped together.

By default, a radio is not in any group and the load balancing algorithm would not apply to it.

To configure a group of radios together:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Go to the *Configuration* tab.
- 3 Select a radio you wish to add to a group and click the *Edit* button.



- 4 Enter the *Group ID* for the group you wish to add the selected radio to.

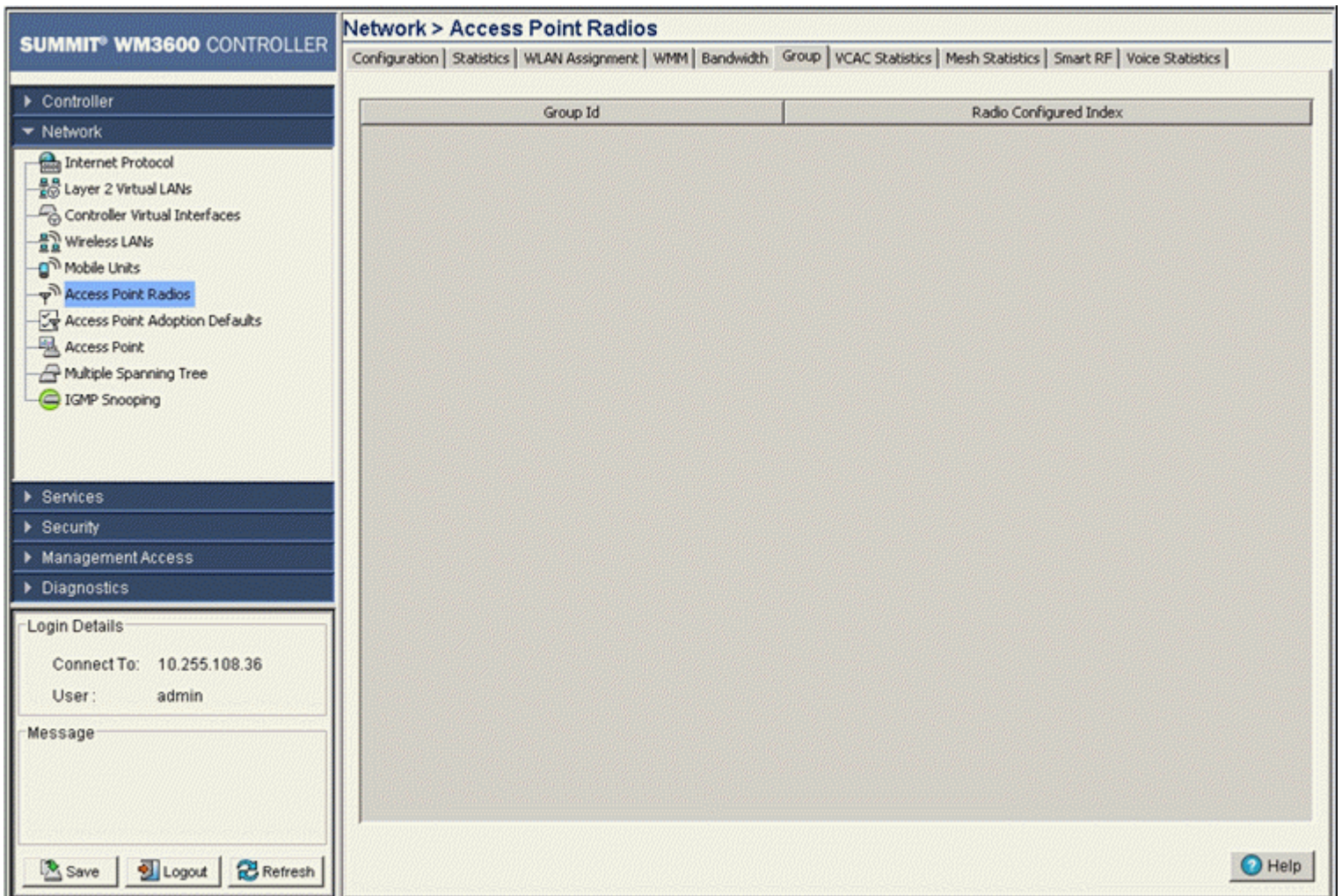
- 5 Click *OK* to save the changes.
- 6 Repeat steps 3 through 5 for each radio you wish to add to groups.
- 7 When you have finished adding radios to groups, click the *Apply* button on the *Configuration* tab to save your changes.
- 8 To verify the radio groups, click the *Groups* tab to view configured radio groups. For more information on viewing radio groups, refer to [“Viewing Access Point Radio Groups” on page 233](#).

Viewing Access Point Radio Groups

Refer to the *Groups* tab to view the *Group ID* and *Index* associated with each radio when added to a WLAN.

To view existing radio group settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Group* tab.



Group information displays per radio with the following data:

Group Id Displays the Group Id associated with each adopted radio.

Radio Configured Index The Index is the numerical index (device identifier) used with the device radio. Use this index (along with the radio name) to differentiate the radio from other device radios.

Viewing Active Calls (AC) Statistics

To view Active Calls statistics:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *VCAC Statistics* tab.

SUMMIT® WM3600 CONTROLLER

Network > Access Point Radios

Configuration | Statistics | WLAN Assignment | WMM | Bandwidth | Group | **VCAC Statistics** | Mesh Statistics | Smart RF | Voice Statistics

Show Filtering Options <<< Page 1 of 1 Go >>>

Index	Description	Total Voice Calls	Roamed Calls	Rejected Calls	Used Air Time (%)	Total Air Time (%)
3	RADIO3	0	0	0	0	82
4	RADIO4	0	0	0	0	82

Filtering is disabled Page 1 of 1 loaded.

Save Logout Refresh Help

3 The following statistics are displayed:

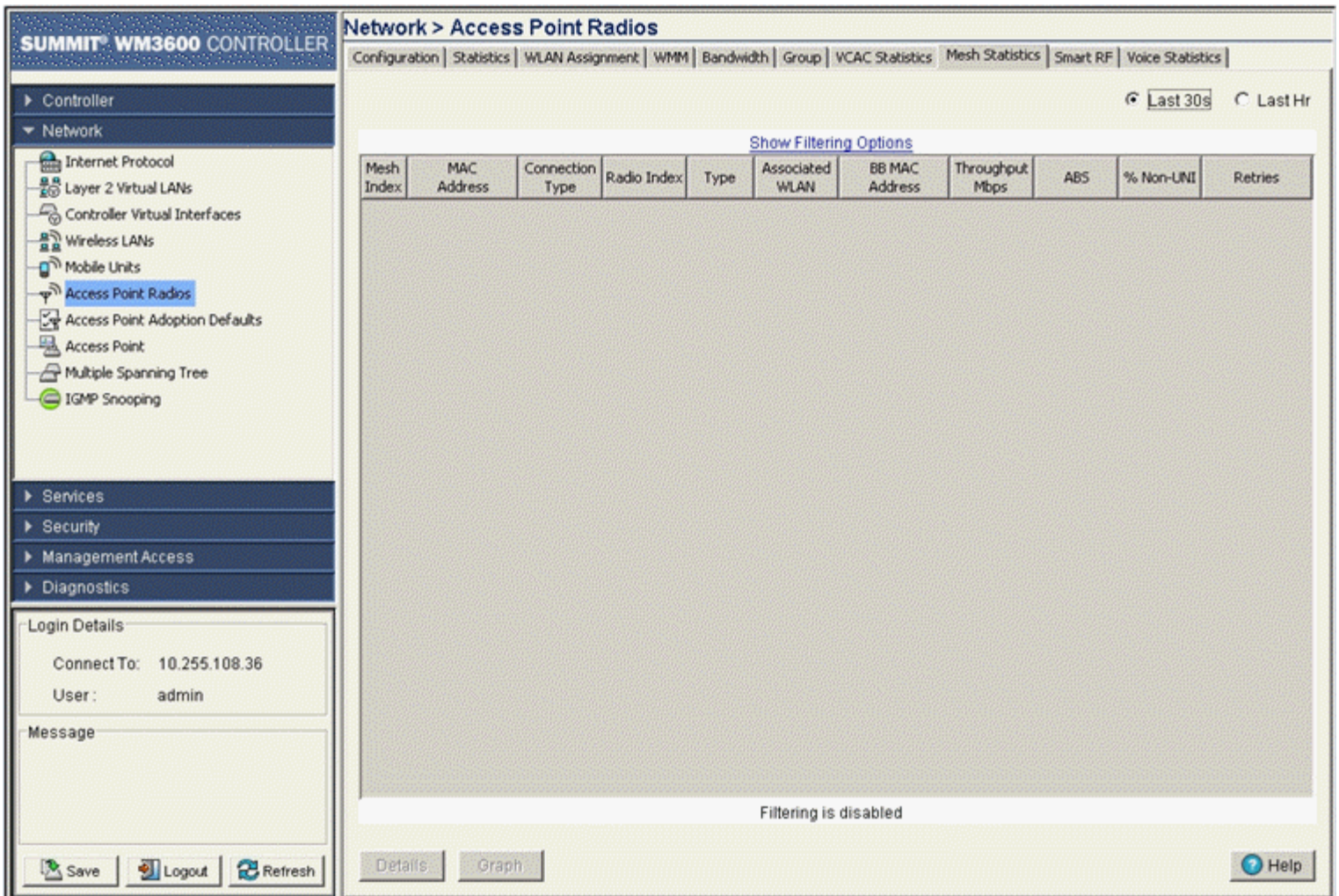
Index	Displays the numerical identifier assigned to each Access Port/Point.
Description	Displays the names assigned to each of the APs. The AP name can be configured on the Access Port/Point Radios Configuration page.
Total Voice Calls	Displays the total number of voice calls attempted for each Access Port/Point.
Roamed Calls	Displays the total number of voice calls that were roamed from each Access Port/Point.

- Rejected Calls Displays the total number of voice calls rejected by each Access Port/Point. Calls may be rejected if the call does not meet the TPSEC Admission Control requirements for the AP or when an AP would not be able to provide the necessary QoS for the call.
- Used Air Time(%) Displays the total percentage of air time that each Access Port/Point has dedicated to voice calls.
- Total Air Time(%) Displays the total percentage of air time allocated for TPSEC clients.

Viewing Mesh Statistics

To view Mesh Statistics:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Mesh Statistics* tab.



- 3 The following statistics are displayed:

- Mesh Index Displays the numerical identifier assigned to each mesh member AP.
- MAC Address Displays the Media Access Control (MAC) address for each Access Port/Point.

Connection Type	Displays the connection type for each Access Port.
Radio Index	The Radio Index is a numerical value assigned to the radio as a unique identifier. For example: 1, 2, or 3. The index is helpful for differentiating radios of similar type and configuration.
Type	Displays the radio type of the corresponding APs. Available types are: <ul style="list-style-type: none">• 802.11a• 802.11an• 802.11bg• 802.11bgn
Associated WLAN	Displays the WLAN that each Access Port/Point is associated to.
Throughput Mbps	Throughput Mbps is the average throughput in Mbps on the selected Access Port/Point.
Average Mbps	Average Mbps is the average throughput in Mbps on the selected Access Port/Point.
% Non-UNI	% Non-Uni is the percentage of the total packets for the selected radio that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries	Displays the total number of retries for each Access Port/Point.

Smart RF

When invoked by an administrator, Smart RF (or self-monitoring at run time) instructs radios to change to a specific channel and begin beaconing using their maximum available transmit power. Within a well planned deployment, any associated radio should be reachable by at least one other radio. The Smart RF feature records signals received from its neighbors as well as signals from external, un-managed radios. AP to AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

- Smart RF management is comprised of the following two phases:
- [Smart RF Calibration Phase on page 236](#)
- [Smart RF Monitoring Phase on page 237](#)

Smart RF is well suited for clustered environments. Smart RF interacts with a number of existing features, (such as radio detection, MU load balancing, and self-healing).



CAUTION

SmartRF should only be enabled on AP35xx Access Points when using antennas with gains of 7dBi or less. For AP4700 Series Access Points it should only be used with the façade antenna, and for AP4600 Access Ports it should only be used with internal antenna models.

Smart RF Calibration Phase

Smart RF calibration is initiated by an administrator during initial deployment or can be scheduled at a specified frequency or time of the day. Smart RF instructs adopted radios to scan legal channels and measure signal strength from associated radio and other device signals detected within the environment.

Smart RF conducts the following network management activities:

- Automatically calibrates associated radio's maximum power capability
- Automatically assigns certain radios to be detectors
- Automatically assign channels to radios to avoid channel overlap and interference from external RF sources
- Automatically calculates the transmit power of working radios
- Automatically configures self-healing parameters. Radio assume the roles of caretaker and caregiver. When a radio is down, it is referred to as the caretaker. Neighbor radios raising their transmit power to cover for the failed radio are referred to as caregivers. Smart RF calibration automatically chooses caregiver radios along with the power needed to cover.

Smart RF Monitoring Phase

Smart RF monitoring occurs continuously. It includes the following monitoring activities:

- Self-healing to monitor whether a radio is down
- Interference monitoring using retry stats
- Defines coverage holes and discerns transmit rates and MU signal strength. When necessary, Smart RF increases MU power to maintain coverage
- Extensible to future smart-tuning. For example, distinguish between AP to AP interference and static interference

Viewing Smart RF Information

To view Smart RF information:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Smart RF* tab.

SUMMIT® WM3600 CONTROLLER

Network > Access Point Radios

Configuration | Statistics | WLAN Assignment | WMM | Bandwidth | Group | VCAC Statistics | Mesh Statistics | **Smart RF** | Voice Statistics

For SMART-RF calibration and configuration, use "Smart RF Settings" button below.

Show Filtering Options << Page 1 of 1 Go >>

MAC Address	Index	AP Name	Type	Antenna Gain(dBi)	Coverage Rate(Mbps)	Is Detecto	Lock Detecto	Lock Channe	Lock Power	Lock Resouer	Controller IP
00-04-96-43-50-C0	4	AP-00-04-96-43-50-70	802.11a	0	18	×	×	×	×	×	0 . 0 . 0 . 0
00-04-96-43-50-D0	3	AP-00-04-96-43-50-70	802.11bg	0	18	×	×	×	×	×	0 . 0 . 0 . 0
00-23-68-2E-D6-A0	1	AP-00-04-96-44-51-8C	802.11...	0	18	×	×	×	×	×	0 . 0 . 0 . 0
00-23-68-2E-D6-F0	2	AP-00-04-96-44-51-8C	802.11an	0	18	×	×	×	×	×	0 . 0 . 0 . 0

Filtering is disabled Page 1 of 1 loaded.

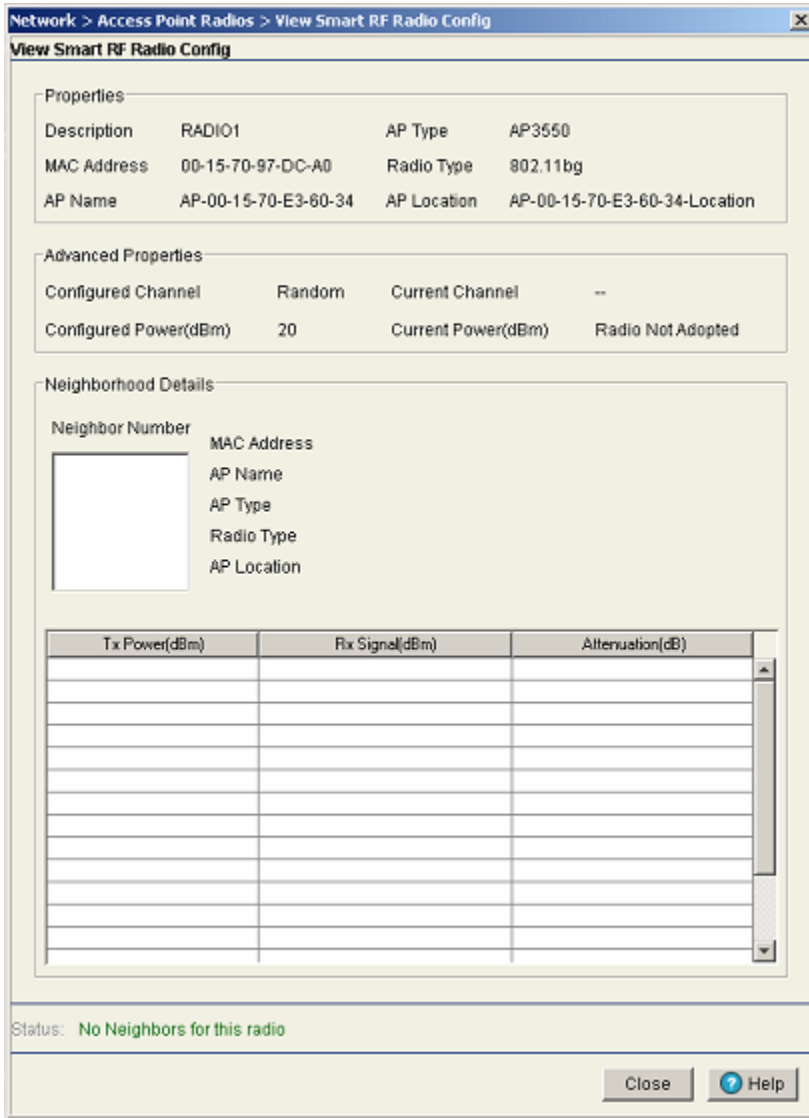
Save Logout Refresh Details Edit Smart RF History Smart RF Settings Help

3 The following *Smart RF* details are displayed:

- MAC Address** Displays the Media Access Control (MAC) Address of each of the APs in the table.
- Index** Displays the numerical identifier assigned to each detector AP used in Smart RF calibration.
- AP Name** Displays the names assigned to each of the APs. The AP name can be configured on the Access Point Radios Configuration page.

Type	<p>Displays the radio type of the corresponding APs.</p> <p>Available types are:</p> <ul style="list-style-type: none"> • 802.11a • 802.11an • 802.11bg • 802.11bgn
Antenna Gain (dBi)	Displays the current antenna gain value in dBi for each Access Port/Point.
Coverage Rate (Mbps)	Displays the current coverage rate for each Access Port based on the Smart RF settings.
Is Detector	Displays whether or not an Access Port/Point is a detector or not. Detector status is determined through Smart RF based on coverage and location of other APs in the network.
Lock Detector	Displays whether or not each Access Port is locked in detector status.
Lock Channel	Displays whether or not each Access Port is locked to a specific channel.
Lock Power	Displays whether or not each Access Port is locked to a specific power level.
Lock Rescuers	Displays whether or not each Access Port is locked to group of rescuer APs.
Controller IP	Displays the IP address of the controller.

- To view the details of individual radio Smart RF information, select a radio from the list and click the *Details* button.



- The *Properties* section displays the following information:

Description	Displays a description of the Radio. Modify the description as required to name the radio by its intended coverage area or function.
MAC Address	Displays the Media Access Control (MAC) Address of the selected AP.
AP Name	Displays the name assigned to the AP. The AP name can be configured on the Access Point Radios Configuration page.
AP Type	Displays the type of Access Port/Point detected. The controllers support AP35xx Access Points, AP4600 Series Access Ports and AP4700 Series Access Points.

Radio Type	Displays the radio type of the corresponding APs. Available types are: <ul style="list-style-type: none"> • 802.11a • 802.11an • 802.11bg • 802.11bgn
AP Location	Displays the current location for the selected AP. The location can be configured on the Access Point Radios Configuration page.

6 The *Advanced Properties* section displays the following information:

Configured Channel	Displays the configured channel for the access point.
Current Channel	Displays the channel on which the access point is currently passing traffic. If the channel is displayed in red, it means the configured channel does not match the current channel. The access point may not be operating on the configured channels for two reasons: Uniform spreading is enabled or radar was encountered on the configured channel.
Configured Power(dBm)	Displays the currently configured power level in dBm for the selected access point.
Current Power (dBm)	Displays the current power level in dBm for the selected access point.

7 The *Neighbor Details* section allows you to select detected neighbor radios and view the following information:

MAC Address	Displays the Media Access Control (MAC) Address of the selected AP.
AP Name	Displays the name assigned to the AP. The AP name can be configured on the Access Point Radios Configuration page.
AP Type	Displays the type of Access Port/Point detected. The controllers support AP35xx Access Points, AP4600 Series Access Ports and AP4700 Series Access Points.
Radio Type	Displays the radio type of the corresponding APs. Available types are: <ul style="list-style-type: none"> • 802.11a • 802.11an • 802.11bg • 802.11bgn
AP Location	Displays the current location for the selected AP. The location can be configured on the Access Point Radios Configuration page.
tx/rx dbm	Displays the transmit, receive, and attenuation information of the selected neighbor radio.

Editing Smart RF Radio Settings

To edit Smart RF radio settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Smart RF* tab

- 3 Select a radio from the table and click the *Edit* button.

- 4 The radio settings are divided into the following three sections:

- Properties
- Radio Rescuer Settings
- Advanced Properties

- 5 The *Properties* section displays the following information:

Description	Displays a description of the Radio. Modify the description as required to name the radio by its intended coverage area or function.
MAC Address	Displays the Media Access Control (MAC) Address of the selected AP.
AP Name	Displays the name assigned to the AP. The AP name can be configured on the Access Point Radios Configuration page.
AP Type	Displays the type of Access Port/Point detected. The controllers support AP35xx Access Points, AP4600 Series Access Ports and AP4700 Series Access Points.

Radio Type	Displays the radio type of the corresponding APs. Available types are: <ul style="list-style-type: none"> • 802.11a • 802.11an • 802.11bg • 802.11bgn
AP Location	Displays the current location for the selected AP. The location can be configured on the Access Point Radios Configuration page.

6 The *Radio Rescuer Settings* section allows you to configure the following radio rescuer settings and information:

Available Radios	Displays a list of radios available to be used as rescuer radios.
Rescuer Radios	Displays a list of radios that have been configured as Rescuer Radios.
Add	Click the <i>Add</i> button to add a selected radio or radios from the Available Radios list into the Rescuer Radios list.
Remove	Click the <i>Remove</i> button to remove a selected radio or radios from the Rescuer Radios list.
Rescuer MAC	Displays the Media Access Control (MAC) Address of the selected Rescuer Radio.
AP Name	Displays the configured AP Name for the selected Rescuer Radio.
AP Location	Displays the configured AP Location for the selected Rescuer Radio. The location can be configured on the Access Point Radios Configuration page.
Rescuer Power	Displays the current power level of the selected Rescuer Radio.
Rescuer Attenuation	Displays the current Attenuation power for the selected Rescuer Radio.

7 The *Advanced Properties* section contains the following configurable items:

Antenna Gain	Specify the desired antenna gain in dBi for the selected radio.
Coverage Rate	Specify the desired coverage rate for the selected radio from the pull-down menu options.
Lock Detector	Enable or disable radio detector mode lock for the selected radio.
Lock TX Power	Check this box to lock the TX power for the selected radio.
Lock Channel	Check this box to lock the channel for the selected radio.
Lock Rescuer	Check this box to lock the rescuer radio for the selected radio.

8 Click *OK* to use the changes to the running configuration and close the dialog.

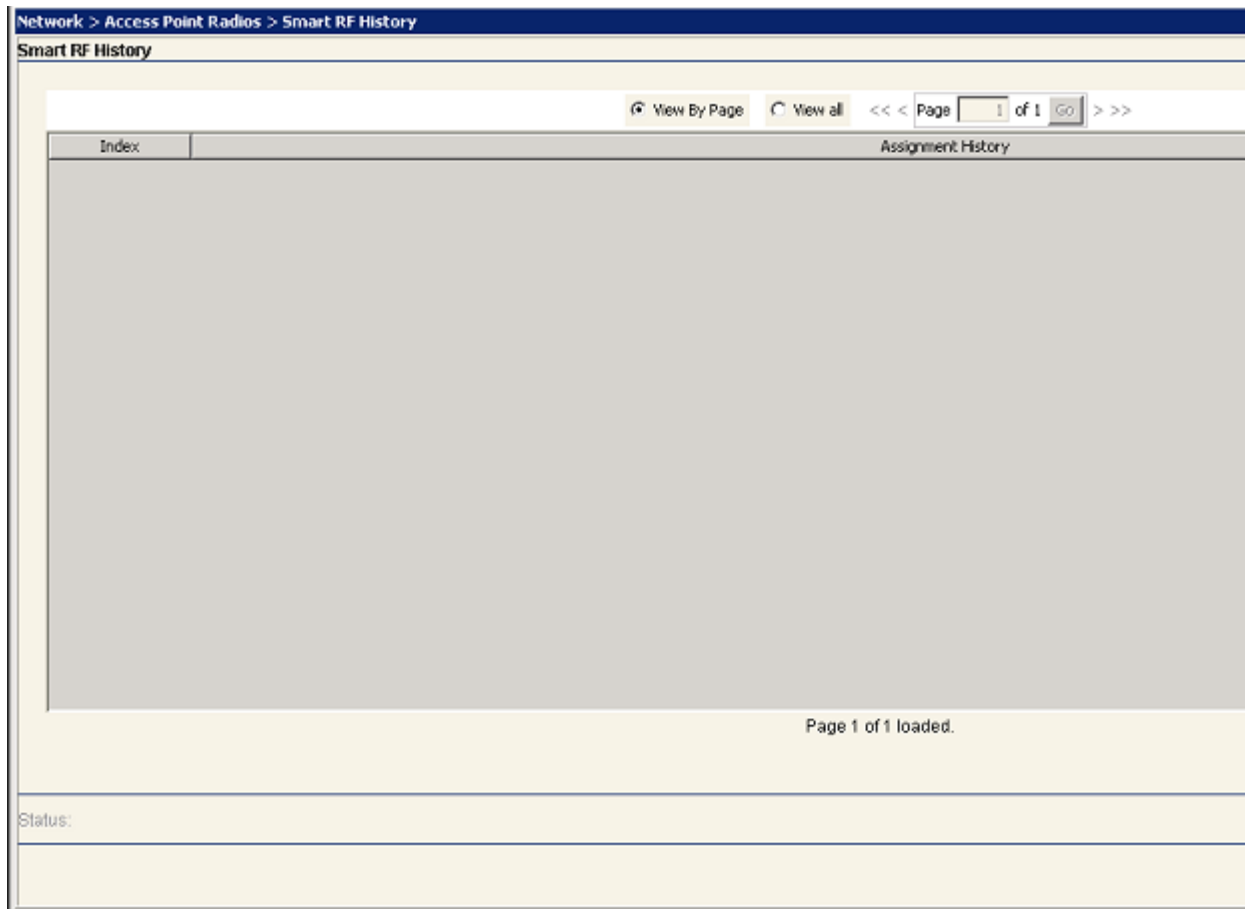
9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing Smart RF History

To view Smart RF history:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Smart RF* tab

- 3 Click the *Smart RF History* button



- 4 The *Smart RF History* window displays the *Index* number and *Assignment History* of Smart RF activity.

Configuring Smart RF Settings

To configure Smart RF settings:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Smart RF* tab.
- 3 Click the *Smart RF Settings* button.

Network > Access Point Radios > Smart RF Global Settings

Smart RF Global Settings

Check All Boxes Enable Smart RF Module

Calibration Configuration

Assign - Detector
 Assign - Channel
 Assign - Tx - Power
 Assign - Rescuers

Available
 2
3
4
5
7

Configured
 1
6
11
36
40

Number of Rescuers: (1-5) Assignable Power Range (dBm): - (4-20)

Retry Threshold (avg attempts/pkt): (0.0-15.0) Scan Dwell Time (seconds): (1-10)

Hold Time (seconds): (30-65535)

Monitoring/Recovery Configuration

 Interference Recovery
 Faulty Radio Recovery
 Coverage Hole Recovery

Calibration Schedule

 Schedule Calibration
 Start Date: MM/DD/YY
 Start Time: HH:MM:SS
 Interval: Days

Diagnostic Configuration

 Verbose Mode
 Extensive Scan Mode

Status:

- 4 Click the *Check All Boxes* option in the *Smart RF Global Settings* dialog to check every box in the configuration window. To uncheck all boxes, click this box a second time.
- 5 Check the *Enable Smart RF Module* box to enable Smart RF functions on the controller.
The remainder of the Smart RF Settings screen is divided into the following four sections:

- Calibration Configuration
- Monitoring/Recovery Configuration
- Diagnostic Configuration
- Calibration Schedule

6 The *Calibration Configuration* section contains the following RF calibration settings:

Assign - Detector	Check this box to enable automatic assignment of radio detectors.
Assign - Channel	Check this box to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources.
Assign - Tx Power	Check this box to enable automatic assignment of transmit power.
Assign - Rescuers	Check this box to enable automatic assignment of rescuers along with rescuing power.
Available	The Available box lists all available channels for Smart RF.
Configured	The Configured box lists all channels enabled for Smart RF.
Add	To add a channel to the configured list, select one or more channels from the Available box and click the <i>Add</i> button.
Remove	To remove a channel from the configured list, select one or more channels from the Available box and click the Remove button.
Number of Rescuers	Assign a number of radios to dedicate as rescuers. The valid range is between 1 and 5. Default value is 3.
Retry Threshold (avg attempts/pkt)	Specify the retry threshold, which is the average number of retries per packet to cause a radio to re-run channel selection. The valid range is between 0.0 and 15.0. The default threshold is 14.0.
Hold Time (seconds)	Specify the global hold time in seconds. The valid range is between 30 and 65535 seconds. Default hold time is 3600 seconds.
Assignable Power Range (dBm)	Specify a valid range for the power in dBm. The valid minimum is 4 and maximum is 20. Default range is 4 to 16 dBm.
Scan Dwell Time (seconds)	Specify the RF Scan Dwell Time in seconds. The valid range is between 1 and 10 seconds. Default dwell time is 1 second.

7 The *Monitoring/Recovery Configuration* section contains the following configuration items:

Interference Recovery	Check this box to enable monitoring for interference and self-healing it by rescuer.
Faulty Radio Recovery	Check this box to enable monitoring for defective radio and self-healing by its rescuer.
Coverage Hole Recovery	Check this box to enable monitoring and recovering for coverage holes.

8 The *Diagnostic Configuration* section contains the following two configuration items:

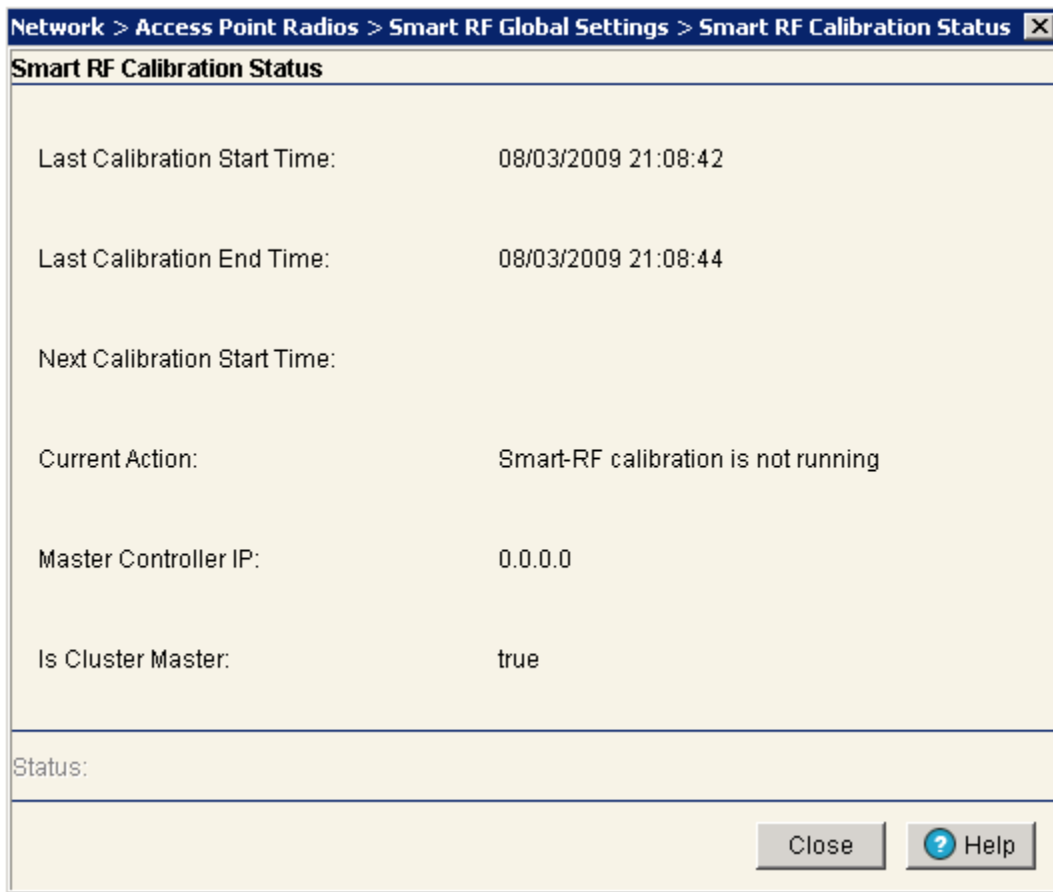
Verbose Mode	Check this box to enable verbose diagnostic information for Smart RF.
Extensive Scan Mode	Check this box to enable extensive scan mode when using Smart RF.

9 The *Calibration Schedule* contains the following calibration settings:

Schedule Calibration	Check this box to enable scheduled RF Calibration.
Start Date	If scheduled RF Calibration is enabled, enter a start date in MM/DD/YY format for the start date of scheduled calibration.

Start Time	If scheduled RF Calibration is enabled, enter a start time in HH:MM:SS format for the start time of scheduled calibration.
Interval	If scheduled RF Calibration is enabled, enter an interval in days for how long the scheduled calibration should continue after its start date.

- Once the settings have been configured, click the *Run Calibration* button to start a Smart RF calibration.
- Click the *Calibration Status* button to open a dialogue with the following calibration status information



Last Calibration Start Time	Displays the date and time that the last Smart RF calibration began.
Last Calibration End Time	Displays the date and time that the last Smart RF calibration ended.
Next Calibration Start Time	Displays the date and time scheduled for the next Smart RF calibration.
Current Action	Displays what the Smart RF engine is currently doing. If there is a scan in process, it will be displayed here.
Master Controller IP	Displays the IP address of the master controller in the cluster.
Is Cluster Master	Displays the cluster master status of the controller. If the controller is the master, it will display <i>true</i> , if not, it will display <i>false</i> .

- Click *OK* to use the changes to the running configuration and close the dialog.

13 Click *Cancel* to close the dialog without committing updates to the running configuration.

Voice Statistics

To view Voice Statistics:

- 1 Select *Network > Access Point Radios* from the main menu tree.
- 2 Click the *Voice Statistics* tab.

The screenshot shows the Summit WM3600 Controller interface. The left sidebar contains a navigation tree with categories like Controller, Network, Services, Security, Management Access, and Diagnostics. The 'Access Point Radios' option is selected under the Network category. The main content area is titled 'Network > Access Point Radios' and has several tabs: Configuration, Statistics, WLAN Assignment, WMM, Bandwidth, Group, VCAC Statistics, Mesh Statistics, Smart RF, and Voice Statistics. The 'Voice Statistics' tab is active, showing a table with columns: Index, Description, Type, Calls per Radio(Current), Calls per Radio(Max), Calls per Radio(Avg), Packets Dropped(%), Packets Dropped, Delay to AP, and MUs Associated. Below the table, it says 'Filtering is disabled'. At the bottom, there is a 'Call Details' section with a table with columns: Index, Protocol, Successful Calls, Avg Call Quality R Factor, Avg Call Quality MOS-CQ, Average Jitter (msec), and Average Latency (msec). The interface also includes a 'Login Details' section with 'Connect To: 10.255.108.36' and 'User: admin', and buttons for Save, Logout, Refresh, and Help.

Index	Description	Type	Calls per Radio(Current)	Calls per Radio(Max)	Calls per Radio(Avg)	Packets Dropped(%)	Packets Dropped	Delay to AP	MUs Associated
3	RADIO3	802.11bg	0	0	0.0	0.0	0	1	0
4	RADIO4	802.11a	0	0	0.0	0.0	0	1	0

3 The following statistics are displayed:

- | | |
|-------------|---|
| Index | Displays the numerical identifier assigned to each AP. |
| Description | Displays the names assigned to each of the APs. The AP name can be configured on the Access Points Radios Configuration page. |
| Type | Displays the radio type of the corresponding APs. Available types are: <ul style="list-style-type: none"> • 802.11a • 802.11an • 802.11bg • 802.11bgn |

Calls per radio (Current)	Displays the current number of active voice calls for each Access Port/Point.
Calls per radio (Max)	Displays the maximum number of concurrent voice calls that each Access Port/Point has seen.
Calls per radio (Avg)	Displays an average number of calls active on each Access Port/Point.
Packets Dropped(%)	Displays a percentage of the packets that each Access Port/Point has dropped in comparison to the total number of packets.
Packets Dropped	Displays the total number of packets dropped by each Access Port/Point.
Delay to AP	Displays the current delay time for each Access Port/Point.
MUs Associated	Displays the total number of mobile units associated with each Access Port/Point.

4 Selecting a radio from the table will display the following details of individual calls:

Index	Displays the numerical identifier assigned to each MU.
Protocol	Displays which voice protocol is being used for the selected call. Voice protocols include: <ul style="list-style-type: none"> • SIP • TPSEC • Spectralink • H.323
Successful Calls	Displays the number of successful calls for the displayed MUs.
Avg Call Quality R Factor	Displays the average call quality using the R Factor scale. The R Factor method rates voice quality on a scale of 0 to 120 with a higher score being better. If the R Factor score is lower than 70 it is likely that users will not be satisfied with the voice quality of calls.
Avg Call Quality MOS-CQ	Displays the average call quality using the Mean Opinion Score (MOS) call quality scale. The MOS scale rates call quality on a scale of 1-5 with higher scores being better. If the MOS score is lower than 3.5 it is likely that users will not be satisfied with the voice quality of calls.
Average Jitter (msec)	Displays the average jitter time for calls on the displayed MUs. Jitter is delays on the network that can result in a lag in conversations. A jitter score higher than 150 ms is likely to be noticed by end users during a call.
Average Latency (msec)	Displays the average latency in milliseconds for calls on the selected MUs.

Viewing Access Point Adoption Defaults

Use the *Access Point Adoption Defaults* screen to configure the current radio adoption configurations, assigning WLANs and security schemes and to review each radio type, as well as the Access Category that defines which data type (Video, Voice, Best Effort, and Background) the radio has been configured to process. It has the following tabs: In a Layer 3 environment, the Access Point adoption process is somewhat unique., For more information, see [“Configuring Layer 3 Adoption” on page 256](#).

- [Configuring AP Adoption Defaults on page 250](#)
- [Configuring Layer 3 Adoption on page 256](#)
- [Configuring WLAN Assignment on page 258](#)
- [Configuring WMM on page 259](#)

Configuring AP Adoption Defaults

The *Configuration* tab displays the current radio adoption configuration including radio type, placement, channel setting, and power settings. Many of these settings can be modified (as well as radio's current rate settings) by selecting a radio and clicking the *Edit* button. These settings are the default configurations when the radios are set to auto-adopt.

To view existing Radio Configuration information:

- 1 Select *Network > Access Point Adoption Defaults* from the main menu tree.
- 2 Click the *Configuration* tab.

SUMMIT WM3600 CONTROLLER

Network > Access Point Adoption Defaults

Configuration | WLAN Assignment | WMM

Show Filtering Options

Type	Placement	Channel	Power dBm	Power mW
802.11a	Indoors	Random	20	100
802.11bg	Indoors	Random	20	100
802.11an	Indoors	Random	20	100
802.11bgn	Indoors	Random	20	100

Filtering is disabled

Save Logout Refresh Edit Help

- 3 Refer to the following information as displayed within the *Configuration* tab:

Type	Displays whether the radio is an 802.11bg and 802.11bgn or 802.11a and 802.11an radio.
Placement	Displays the default placement when an radio auto-adopts and takes on the default settings. Options include Indoor or Outdoor. Default is Indoor.

Channel	Displays the default channel when a radio auto-adopts and takes on the default settings. This value can be a specific channel, Random, or ACS. Random assigns each radio a random channel. ACS (Automatic Channel Selection) allows the controller to systematically assign the channel. Default is random.
Power dBm	Displays the default power when a radio auto-adopts and takes on the default settings. Defaults are 20 dBm for 802.11bg) and 17 dBm for 802.11a.
Power mW	Displays the default transmit power in mW (derived from the Power dBm setting). Defaults are 100 mW for 802.11bg and 50 mW for 802.11a.

- 4 To modify a radio's adoption defaults, select a radio and click the *Edit* button. For more information, see [“Editing Default Access Port/Point Adoption Settings” on page 251.](#)



NOTE

Up to 256 Access Points/Ports are supported by the Summit WM3600. Up to 1024 Access Points/Ports are supported by the Summit WM3700 controller. Up to 6 Access Points/Ports are supported by the Summit WM3400 controller. The actual number of Access Ports adoptable by a controller is defined based on Access Port or Adaptive AP licenses and on a per platform basis.



CAUTION

An Access Port is required to have a DHCP provided IP address before attempting Layer 3 adoption, otherwise it will not work. Additionally, the Access Port must be able to find the IP addresses of the controllers on the network.

To locate controller IP addresses on the network:

- Configure DHCP option 189 to specify each controller IP address.
 - Configure a DNS Server to resolve an existing name into the IP of the controller. The Access Port has to get DNS server information as part of its DHCP information.
-

Editing Default Access Port/Point Adoption Settings

Use the *Edit* screen to dedicate a target radio as a detector radio, as well as change the radios settings (placement, power, and channel) and advanced properties (antenna setting, maximum associations, adoption preference, etc.).

To edit radio adoption configuration settings:

- 1 Select *Network Setup > Access Point Adoption Defaults* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Select a radio from the table.

- Click the *Edit* button to display a screen to change the radio adoption default values for the currently selected radio type (802.11bg and 802.11bgn or 802.11a and 802.11an).

Network > Access Point Adoption Defaults > Configuration 802.11a

Configuration

Properties Model: AP3510/AP3550 Radio Type: 802.11a <input type="checkbox"/> Dedicate this AP as Detector AP <input type="checkbox"/> Single-channel scan for Unapproved APs <input type="checkbox"/> Enable Enhanced Beacon Table <input type="checkbox"/> Enable Enhanced Probe Table		Radio Settings Placement: Indoors Desired Channel: Random Desired Power: 20 dBm 100 mW <input type="button" value="Rate Settings..."/>	
Advanced Properties			
Antenna Diversity	Full Diversity	RTS Threshold	2346 bytes
Maximum MUs	256	Beacon Interval	100 K-us
Adoption Preference ID	0	Self Healing Offset	0 dBm
<input type="button" value="DTIM Periods"/>			
Admission Control Settings			
Max. Admitted MUs for Voice Traffic	100	Max. Airtime for Voice	75 %
Max. Roamed MUs for Voice Traffic	10	Max. Airtime Reserved for Roaming	10 %
Status:			
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>			

The *Properties* field displays the *Model* family for the selected Access Port/Point. The *Model* is read only and cannot be modified. The *Radio Type* displays the radio type (802.11b, 802.11bg and 802.11bgn or 802.11a and 802.11an). This value is read only and cannot be modified.

- To use this radio as a detector to identify rogue APs on your network, check the box titled *Dedicate this AP as Detector AP*. Setting this radio as a detector will dedicate this radio to detecting rogue APs on the network. Dedicated detectors do not connect to by clients.
- Select the *Single-channel scan for Unapproved APs* checkbox to enable the controller to detect rogue devices using its only current channel of operation.

-
- 7 Select the *Enable Enhanced Beacon Table* checkbox to allow the AP to receive beacons and association information.
 - 8 Select the *Enable Enhanced Probe Table* checkbox to allow an AP to forward MU probe requests to the controller.
 - 9 Within the *Radio Settings* field, configure the *Placement* of the radio as either *Indoors* or *Outdoors*. The setting will affect the selection channel and power levels. Default is *Indoors*.
 - 10 Select a channel for communications between the Access Port/Point and MUs in the *Desired Channel* field.

The selection of a channel determines the available power levels. The range of legally approved communication channels varies depending on the installation location and country. The selected channel can be a specific channel, "Random," or "ACS." Random assigns each radio a random channel. ACS (Automatic Channel Selection) allows the controller to systematically assign channels. Default is Random.

- 11 After first selecting a channel, select a power level in dBm for RF signal strength in the *Desired Power (dBm)* field.

The optimal power level for the specified channel is best determined by a site survey prior to installation. Available settings are determined according to the selected channel. Set a higher power level to ensure RF coverage in WLAN environments that have more electromagnetic interference or greater distances between the Access Port/Point and MUs. Decrease the power level according to the proximity of other Access Ports/Points. Overlapping RF coverage may cause lost packets and difficulty for roaming devices trying to engage an Access Port/Point. After setting a power level, channel, and placement the RF output power for the Access Port/Point is displayed in mW. Default is 20 dBm (802.11bg), or 17 dBm (802.11a).



NOTE

After setting a power level, channel, and placement the RF output power for the Access Port/Point is displayed below in mW.

- 12 To configure optional rate settings, click the *Rate Settings* button to display a new dialogue containing rate setting information. Instructions on configuring rate settings are described in "[Configuring Rate Settings](#)" on page 218.
- 13 In most cases, the default settings for the *Advanced Properties* section are sufficient for most users. If needed, additional radio settings can be modified for the following properties:

Antenna Diversity	Use the drop-down menu to configure the Antenna Diversity settings for Access Points using external antennas. Options include: <ul style="list-style-type: none">• Full Diversity: Utilizes both antennas to provide antenna diversity.• Primary Only: Enables only the primary antenna.• Secondary Only: Enables only the secondary antenna. Antenna Diversity should only be enabled if the Access Port has two matching external antennas. Default value is <i>Full Diversity</i> . Antenna Diversity for AP4600 Series Access Ports is fixed to <i>MIMO</i> .
Maximum MUs	Sets the maximum number of MUs that can associate to a radio. The maximum number of stations that can associate to a radio are 256.

Adoption Preference ID	<p>The Adoption Preference ID defines the preference ID of the controller. The value can be set between 1 and 65535. To make the radios preferred, the Access Port/Point preference ID should be the same as adoption preference ID.</p> <p>The adoption preference id is used for RP load-balancing. A controller will preferentially adopt Access Ports/Points, which have the same adoption-preference-id as the controller itself.</p>
Short Preambles only (this is not seen in Summit WM3400)	<p>If using an 802.11 bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectralLink phones) require long preambles. This checkbox does not display if using an 802.11a radio.</p>
RTS Threshold	<p>Specify a <i>Request To Send</i> (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports/Points.</p> <p>RTS is a transmitting station's signal that requests a <i>Clear To Send</i> (CTS) response from a receiving station. This RTS/CTS procedure clears the air where many MUs (or nodes) are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.</p> <p>Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and simply sends (without RTS/CTS) any data frames that are smaller than the threshold.</p> <p>Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Ports/Points. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of the additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.</p> <p>A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold. Default is 2346.</p> <p>In 802.11b/g mixed RTS/CTS happens automatically. There is no way to disable RTS/CTS unless the network and all the devices used are 802.11g or 802.11a only.</p> <p>When ERP Protection is ON, the 11bg radio will perform a CTS-to-self before it transmits the frame.</p>
Beacon Interval	<p>Specify a beacon interval in units of 1,000 microseconds (K-us). This is a multiple of the DTIM value, for example, 100: 10. (See "DTIM Period" below). A beacon is a packet broadcast by the adopted Access Ports/Points to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the radio-port address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM.</p> <p>Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. Default is 100 K-us.</p>

DTIM Periods	Specify a period for the <i>Delivery Traffic Indication Message</i> (DTIM). This is a divisor of the beacon interval (in milliseconds), for example, 10 : 100. (See “Beacon Interval” above). A DTIM is periodically included in the beacon frame transmitted from adopted Access Ports/Points. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates that broadcast and multicast frames (buffered at the Access Port/Point) are soon to arrive. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default DTIM period is 2 beacons.
Self Healing Offset	When an Access Port increases its power to compensate for a failed Access Port, power is increased to the country's regulatory maximum. Set the Self Healing Offset to reduce the country's regulatory maximum power if Access Ports are situated close to each other or if Access Ports use external antennas. For additional information on determining the offset value, see the documentation shipped with the Access Port.

- 14 In the *Max Admitted MUs for Voice Traffic* field, specify the maximum number of MUs allowed to connect to the specified radio for voice traffic. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality. Admission control is only available for TSPEC enabled voice clients.
- 15 In the *Max Roamed MUs for Voice Traffic* field, specify the maximum number of voice MUs that are allowed to roam to this radio. Limiting the number of MUs can ensure that all voice MUs receive enough bandwidth to ensure voice quality. Admission control is only available for TSPEC enabled voice clients.
- 16 In the *Max Airtime for Voice* field, specify a maximum percentage out of the radio's total airtime that may be used for voice.
- 17 In the *Max Airtime for Reserved for Roaming* field, specify a maximum percentage out of the radio's total airtime that may be used for voice MUs which roam from other APs.
- 18 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 19 Click *OK* to use the changes to the running configuration and close the dialog.
- 20 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Rate Settings. Use the *Rate Settings* screen to define a set of basic and supported rates for the target radio. This allows the radio to sync with networks using varying data rates and allows the radio to default to a predefined set of data rates when higher data rates cannot be maintained.

To configure a radio's rate settings:

- 1 Click the *Rate Settings* button in the radio edit screen to launch a screen wherein rate settings can be defined for the radio.
- 2 Check the boxes next to all *Basic Rates* you want supported by this radio.
Basic Rates are used for management frames, broadcast traffic, and multicast frames. If a rate is selected as a basic rate, it is automatically selected as a supported rate.
- 3 Check the boxes next to all *Supported Rates* you want supported by this radio.



Supported Rates allow an 802.11 network to specify the data rate it supports. When a station attempts to join the network, it checks the data rate used on the network. If a rate is selected as a basic rate, it is automatically selected as a supported rate.

- 4 Click the *Clear all rates* button to uncheck all of the Basic and Supported rates.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Layer 3 Adoption

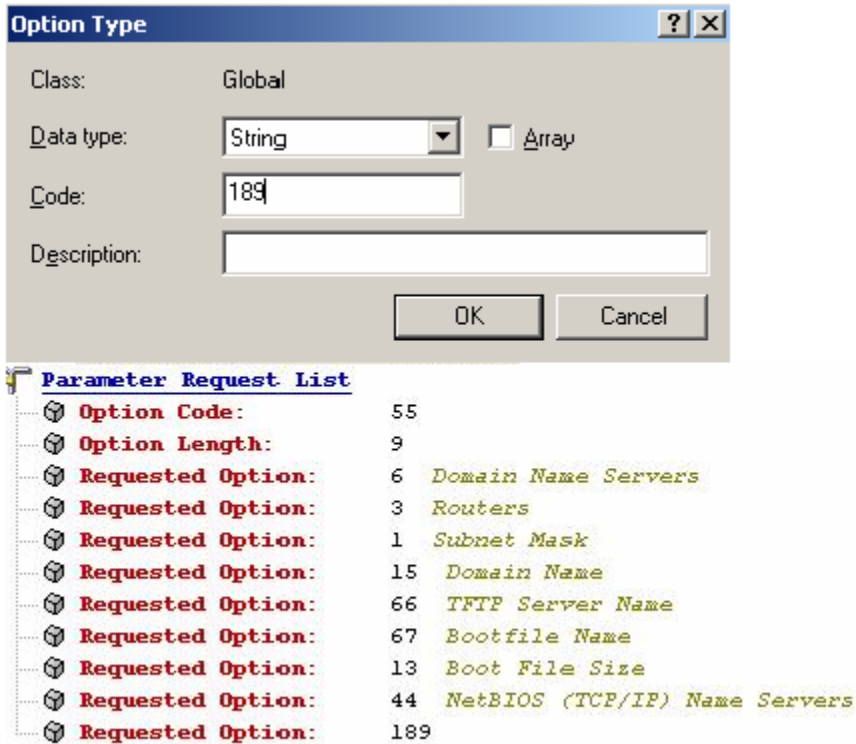
The configuration activity required for adopting AP4600 Series Access Ports in a layer 3 environment is unique. In a layer 3 environment, controller discovery is attempted in the following ways:

- On the local VLAN
- Through the DHCP Server

Initially, the Access Port attempts to find its wireless controller by broadcasting a Hello packet on its local VLAN. During this activity:

- 1 All controllers on the VLAN that receive this Hello packet respond with a parent packet.
- 2 If no response is received, the Access Port attempts to discover its controller by first obtaining an IP address from a DHCP (or DNS) server and checking the options field within the DHCP response.

The options field (Option 189) contains a list of controller IP addresses available for the Access Port.



- 3 The system administrator now programs these options into the DHCP server.
- 4 If the Access Port finds the list, it sends a unidirectional Hello packet (encapsulated in a UDP/IP frame) to each controller on the list.
- 5 Each controller that receives such a packet responds with a Parent response.

Configuring WLAN Assignment

Use the *WLAN Assignment* tab to assign WLANs and security schemes.

To view existing WLAN Assignments:

- 1 Select *Network > Access Point Adoption Defaults* from the main menu tree.
- 2 Click the *WLAN Assignment* tab.

The screenshot shows the configuration page for 'Network > Access Point Adoption Defaults' with the 'WLAN Assignment' tab selected. The left sidebar contains a navigation tree with 'Access Point Adoption Defaults' highlighted. The main area features a 'Select Radio / BSS' section with a dropdown menu set to '802.11a' and a list of BSS options (BSS 1, BSS 2, BSS 3, BSS 4). To the right is the 'Select / Change Assigned WLANs' section, which includes a 'Primary WLAN' dropdown and a table of available WLANs.

Assign	Index	Description	ESS ID	VLAN ID
<input type="checkbox"/>	1	WLAN1	test-open-1x	1
<input type="checkbox"/>	2	WLAN2	test-open-hotspot	1
<input type="checkbox"/>	3	WLAN3	test-4600an-local	1
<input type="checkbox"/>	4	WLAN4	test-4600bgn-local	1
<input type="checkbox"/>	5	WLAN5	test-3510a-local	1
<input type="checkbox"/>	6	WLAN6	test-3510bg-local	1

At the bottom left, a message box displays '802.11a selected.' and buttons for 'Save', 'Logout', and 'Refresh'. At the bottom right, buttons for 'Apply', 'Revert', and 'Help' are visible.

The Assigned WLANs tab displays two fields: *Select Radios/BSS* and *Select/Change Assigned WLANs*.

- 3 With the *Select Radios/BSS* field, select the radio type to configure (802.11bg and 802.11bgn or 802.11a and 802.11an) from the *Select Radio* drop-down menu.
- 4 Select the desired BSS from the *BSS list* or select a *Radio* (802.11bg and 802.11bgn or 802.11a and 802.11an) to modify.

5 Refer to the *Select/Change Assigned WLAN* field for the following information:

Primary WLAN	<p>If a specific BSS was selected from the <i>Select Radio/BSS</i> area, choose one of the selected WLANs from the drop-down menu as the primary WLAN for the BSS.</p> <p>If the radio was selected, the applet will automatically assign one WLAN to each BSS in order, and that WLAN will be set as the <i>Primary WLAN</i> for the BSS.</p> <p>If the number of WLANs selected is greater than the number of BSSIDs, the remaining WLANs are included with the last BSS.</p>
Assign	Assign the WLAN(s) to the selected BSS or Radio.
Index	Displays (in ascending order) the numerical index assigned to each SSID. Use the index (along with the WLANs name) as a means of identifying WLANs once assigned to different radio BSSIDs. A BSSID cannot support two WLANs with the same numerical index.
Description	Use the WLAN description (along with the WLANs index) as a means of identifying WLANs assigned to different radio BSSIDs. A BSSID cannot support two WLANs with the same description.
ESS ID	Displays the assigned SSID uniquely distributed between the WLANs assigned to the BSSIDs.
VLAN ID	Displays the VLAN ID of VLANs assigned to WLANs. By default, all WLANs are assigned to VLAN 1.

6 Click *Apply* to save the changes made within the screen.

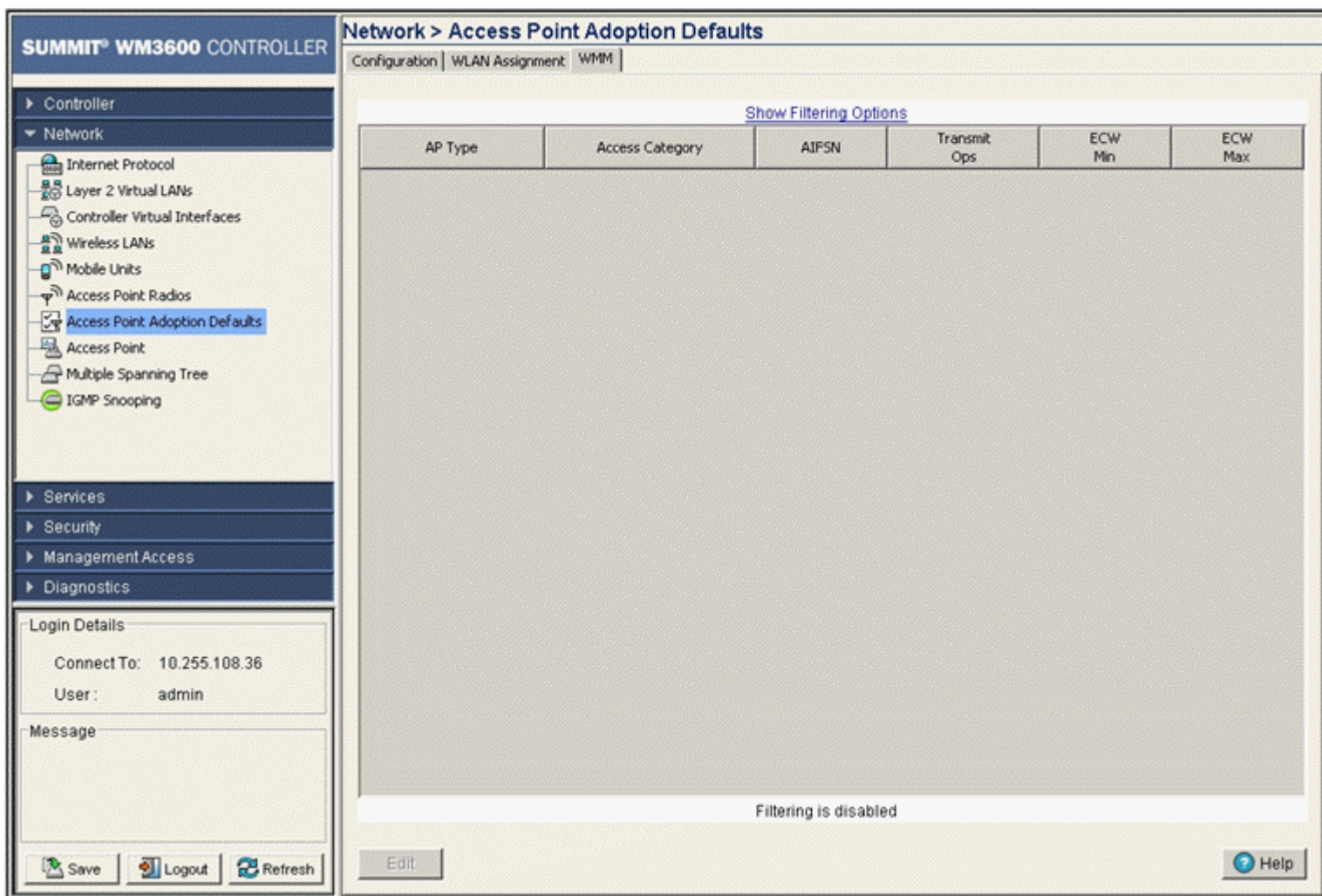
7 Click *Revert* to cancel the changes made and revert back to the last saved configuration.

Configuring WMM

Use the *WMM* tab to review each radio type, as well as the Access Category that defines the data (Video, Voice, Best Effort, and Background) the radio has been configured to process. Additionally, the *WMM* tab displays the transmit intervals defined for the target access category.

To view existing WMM Settings:

- 1 Select *Network > Access Point Adoption Defaults* from the main menu tree.
- 2 Click the *WMM* tab.



- 3 Refer to the WMM table for the following information:

AP Type	Displays whether the radio is an 802.11bg and 802.11bgn or 802.11a and 802.11an radio. This value is read-only and cannot be modified.
Access Category	Displays the Access Category currently in use. There are four categories: Video, Voice, Best Effort, and Background. Click the <i>Edit</i> button to change the current Access Category. Ensure that the Access Category reflects the radios intended network traffic.
AIFSN	Displays the current <i>Arbitrary Inter-frame Space Number</i> (AIFSN). Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before trying to access the medium.
Transmit Ops	Displays the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set higher.

ECW Min	The ECW Min is combined with the ECW Max to define the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.
ECW Max	The ECW Max is combined with the ECW Min to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.

- 4 To modify the properties of WMM Adoption Settings, select a radio and click the *Edit* button. For more information, see [“Editing Access Port/Point Adoption WMM Settings”](#) on page 261.

Editing Access Port/Point Adoption WMM Settings

Use the *Edit* screen to modify a WMM profile's properties (AIFSN, Transmit Ops, Cw Min, and CW Max). Modifying these properties may be necessary as Access Categories are changed and transmit intervals need adjustment to compensate for larger data packets and contention windows. Use [“Configuring WMM”](#) on page 227 to configure downstream traffic parameters. WLAN WMM configuration affects your upstream traffic parameters.

To edit the existing WMM settings:

- 1 Select *Network Setup > Radio Adoption Defaults* from the main menu tree.
- 2 Click the *WMM* tab.
- 3 Select a radio from the table and click the *Edit* button.

The *AP Type* identifies whether the radio is an 802.11bg and 802.11bgn or 802.11a and 802.11an radio. This value is read-only and cannot be modified. There are four editable access categories: Video, Voice, Best Effort and Background.

- 4 Enter a number between 0 and 15 for the *AIFSN* value for the selected radio.

The AIFSN value is the current *Arbitrary Inter-frame Space Number*. Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before trying to access the medium.

- 5 Enter a number between 0 and 65535 for the *Transmit Ops* value.

The Transmit Ops value is the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set higher.

- 6 Enter a value between 0 and 15 for the *Contention Window minimum* value.

The CW Minimum is combined with the CW Maximum to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.

- 7 Enter a value between 0 and 15 for the *Contention Window maximum* value.

The CW Maximum is combined with the CW Minimum to make the Contention Window. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic.

- 8 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

- 9 Click *OK* to use the changes to the running configuration and close the dialog.

- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Access Ports/Points

Use the *Access Point* screen to view device hardware address and software version information for adopted and unadopted Access Ports/Points.

Viewing Adopted Access Ports/Points

Use the *Adopted AP* tab for gathering device hardware address and software version information for the Access Port/Point. Use this information to determine whether the Access Port/Point's version supports the optimal feature set available for the network.

To view existing adopted radio information:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *Adopted AP* tab.

SUMMIT WM3600 CONTROLLER

Network > Access Point

Adopted AP | Unadopted AP | Configuration | Secure WSPe | AP Firmware | IP Filter

Show Filtering Options <<< Page 1 of 1 Go >>>

MAC Address	Model	AP Type	Serial	HW Version	IP Address	Bootloader	Protocol Version	Fw Version	Radio Indices
00-04-96-43-50-70	AP3510-US	AP3510	08499-80154	F	10.255...	2.4.1.0...	WISP-EX...	2.4.1.0...	3,4

Filtering is disabled Page 1 of 1 loaded.

Number of adopted APs: 1

Export Location LED Help

Save Logout Refresh

3 Refer to the *Adopted AP* screen for the following information:

- | | |
|-------------|--|
| Controller | The <i>Controller</i> field displays the IP address of the cluster member associated with each AP. When clustering is enabled on the controller and Cluster GUI is enabled, the <i>Controller</i> field will be available on the AP configuration screen. For information on configuring enabling Cluster GUI, see “ Managing Clustering Using the Web UI ” on page 358. |
| MAC Address | Displays the radio's first MAC address when it is adopted by the controller. |
| Model | Displays the model number of the Access Port/Point. |
| AP Type | Displays the Access Port/Point type. |
| Serial | Displays the serial number of the Access Port/Point. This information is used for controller management purposes. It is read-only and cannot be modified. |
| HW Version | Displays the hardware version of the Access Port/Point. This information can be helpful when troubleshooting problems with the Access Port/Point. |

IP Address	Displays the IP address of the adopted Access Port/Point.
Bootloader	Displays the software version the Access Port/Point boots from. This information can be helpful when troubleshooting problems.
Protocol Version	Displays the version of the interface protocol between the Access Port/Point and the controller. This information can be helpful when troubleshooting problems with the Access Port/Point.
Fw Version	Displays the Access Port/Point firmware version at run time. Use this information to assess whether the software requires an upgrade for better compatibility with the controller.
Radio Indices	Displays the indices of the radios belonging to the selected Access Port/Point. These indices are equivalent to a numerical device recognition identifier (index) for the radio.
Number of Adopted APs	The Number of Adopted APs is the total number of Access Ports/Points currently adopted by Controller.

- When using clustering and the Cluster GUI feature is enabled, a pull-down menu will be available to select which cluster members' APs are displayed. To view APs from all cluster members, select *All* from the pull-down menu. To view APs radios from a specific cluster member, select that member's IP address from the pull-down menu.
- Click the *Export* button to export the contents of the table to a Comma Separated Values file (CSV).



NOTE

When using a standalone Access Point, such as the Altitude 35x0 Series Access Point, one radio can be converted into a sensor and the other radio can function as standard radio.



NOTE

When converting APs to sensors, the default sensor configuration will be sent to each AP. If a static IP is configured in the default sensor configuration, all sensors will receive the same IP address and cause an IP address conflict. It is recommended not to set a static IP for the default sensor configuration and to update individual sensors if they require static IPs.

WIPS uses sensors to collect data transmitted by 802.11a and 802.11b/g compliant devices and sends the data to a centralized server for analysis and correlation. Sensors are passive devices that function primarily in listen-only mode. A single sensor can monitor multiple APs.

Once the sensor collects wireless LAN data, the centralized server analyzes the 802.11 frames and extracts meaningful data points to determine key attributes, such as:

- Wireless device associations
- Use of encryption and authentication
- Vendor identification of all devices
- Total data transferred

Preprocessing data centrally ensures a reduced reliance on network bandwidth to perform wireless network management.

- Click the *Location LED* button to flash the LEDs on the AP to assist in locating and identifying a selected AP within an installation.

Viewing Unadopted Access Ports/Points

Use the *Unadopted AP* tab for gathering device hardware address and software version information for the Access Port/Point.

To view existing Radio Configuration information:

- 1 Select *Network > Access Point* from the main menu tree.

Click the *Unadopted AP* tab.

The screenshot shows the Summit WM3600 Controller web interface. The main content area is titled "Network > Access Point" and has several tabs: "Adopted AP", "Unadopted AP", "Configuration", "Secure WiSPe", "AP Firmware", and "IP Filter". The "Unadopted AP" tab is selected. Below the tabs is a table with three columns: "Index", "MAC Address", and "Last Seen(In Seconds)". The table is currently empty. At the bottom of the page, it says "Number of unadopted APs: 0" and has "Adopt" and "Export" buttons. The left sidebar shows a navigation tree with "Access Point" selected. The top left corner says "SUMMIT WM3600 CONTROLLER". The bottom left has "Save", "Logout", and "Refresh" buttons. The bottom right has a "Help" button.

- 2 The *Unadopted AP* tab displays the following information:

Index	Displays a numerical identifier used to associate a particular Access Port/Point with a set of statistics and can help differentiate the Access Port/Point from other Access Ports/Points with similar attributes.
MAC Address	Displays the unique Hardware or <i>Media Access Control</i> (MAC) address for the Access Port/Point. Access Ports/Points with dual radios will have a unique MAC address for each radio. The MAC address is hard-coded at the factory and cannot be modified.

Last Seen (In Seconds)	Displays the time the Access Port/Point was last seen (observed within the controller-managed network). This value is expressed in seconds. Use this value to assess if the Access Port/Point is no longer in communications with the controller.
Number of Unadopted APs	Displays the total number of Access Ports/Point (at the bottom of the screen) that have been recognized, but not adopted by the controller.

- 3 Select an available index and click the *Adopt* button to display a screen wherein the properties of a new radio can be added for adoption to the controller. When displayed, the screen prompts for the MAC address and type of radio. Complete the fields and click the *OK* button to add the radio.
- 4 Click the *Export* button to export the contents of the table to a *Comma Separated Values* file (CSV).



CAUTION

An AP4600 Series Access Port is required to have a DHCP provided IP address before attempting layer 3 adoption, otherwise it will not work. Additionally, the Access Port must be able to find the IP addresses of the controllers on the network. To locate controller IP addresses on the network:

- Configure DHCP option 189 to specify each controller IP address.
 - Configure a DNS Server to resolve an existing name into the IP of the controller. The Access Port has to get DNS server information as part of its DHCP information.
-

Access Port/Point Configuration

Use the *Configuration* tab to view information on all known Access Ports/Points and edit their profiles.

To view existing adopted Access Port/Point information:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *Configuration* tab.

SUMMIT® WM3700 CONTROLLER

Network > Access Point

Adopted AP | Unadopted AP | **Configuration** | Sensor | Secure WISPe | AP Firmware | IP Filter

MAC Address	AP Type	Country	Ip Filter List	Syslog Mode
00-04-96-42-37-64	AP3510	Egypt-eg		✗
00-04-96-42-37-66	AP3510	Egypt-eg		✗
00-04-96-42-37-9E	AP3510	Egypt-eg		✗
00-04-96-42-37-AE	AP3510	Egypt-eg		✗
00-04-96-42-37-DE	AP3510	Egypt-eg		✗
00-04-96-42-37-E4	AP3510	Egypt-eg		✗
00-04-96-42-37-F8	AP3550	Egypt-eg		✗
00-04-96-42-38-04	AP3550	United States-us		✗
00-04-96-44-51-94	AP4600	Egypt-eg		N/A
00-04-96-44-54-A4	AP4600	Egypt-eg		N/A
00-04-96-44-57-CC	AP4600	Egypt-eg		N/A
00-04-96-44-58-88	AP4600	Egypt-eg		N/A
00-04-96-54-9F-BC	AP4600	Egypt-eg		N/A
00-04-96-54-9F-D4	AP4700	United States-us		✗
00-04-96-54-9F-DC	AP4700	Egypt-eg		✗
00-04-96-54-A0-38	AP4700	Egypt-eg		✗

Buttons: Save, Logout, Refresh, Edit, Syslog Config, LLDP Settings, Help

3 Refer to the *Configuration* screen for the following information:

MAC Address	Displays the radio's first MAC address when it is adopted by the controller.
AP Type	Displays the Access Port type.
Country	Displays the country the Access Port is configured to operate in.
Ip Filter List	Displays the list of IP filters assigned to this AP.
Syslog Mode	For the selected AAP, this option enables or disables logging to an external Syslog server.
LLDP Settings	Enables the Link Layer Discovery Protocol (LLDP), which is a protocol that enables devices to advertise their capabilities and media-specific configuration information.

- 4 To change the settings for a selected Access Port/Point, select an Access Port/Point from the table and click the *Edit* button.
- 5 To configure an external Syslog server on the AAP from the controller, click the *Syslog Config* button.

- Click the *LLDP Settings* button to enable Link Layer Discovery Protocol (LLDP).

Editing Access Port/Point Settings

To edit Access Port/Point Settings:

- Select *Network > Access Point* from the main menu tree.
- Click the *Configuration* tab.
- Select an Access Port/Point from the table and click the *Edit* button

Network > Access Point > Configure AP

Configure AP

Country: United States-us

VLAN Tagging

Enable VLAN Trunking Native VLAN ID: 1 (1 - 4094)

AP Native VLAN for LAN1: Untagged Management VLAN ID: 1 (1 - 4094)

Status:

For AP46xx OK Cancel Help

Network > Access Point > Configure AP

Configure AP

Country: United States-us

VLAN Tagging

Enable VLAN Trunking Native VLAN ID: 1 (1 - 4094)

AP Native VLAN for LAN1: Untagged Management VLAN ID: 1 (1 - 4094)

Radio Setup

A/BIG/N WLAN and Sensor Sensor only Spectrum Analysis mode (no WLAN)

BIG/N WLAN and Sensor BIG/N WLAN no Sensor

A/N WLAN and Sensor A/N WLAN no Sensor

A/BIG/N WLAN only, no Sensor Radios Off

Enter a list of IP Filter Rules

In filters:

Out filters:

Ip Filter Name:

Status:

For AP35xx OK Cancel Help

- Configure the Country and VLAN Tagging for the selected AP:

Country Select the Country that the Access Port will be configured to operate in.

Enable VLAN Trunking	Ensure that the <i>Enable VLAN Trunking</i> option is selected. Trunk lines are required to pass VLAN information between destinations. A trunk port, by default, is a member of all the VLANs existing on the access port and carries traffic for all those VLANs. Trunking is a function that must be enabled on both sides of a link.
Native VLAN ID	Assign a unique VLAN ID (from 1 to 4094) to each VLAN modified. The VLAN ID associates a frame with a specific VLAN and provides the information the access point needs to process the frame across the network. Therefore, it may be practical to assign a name to a VLAN representative of the area or type of network traffic it represents.
AP Native VLAN for LAN1	Select whether the native VLAN for the Access Port on LAN1 will be <i>Tagged</i> or <i>Untagged</i> .
Management VLAN ID	Enter a <i>Management VLAN ID</i> for LAN1 and LAN2. The Management VLAN is used to distinguish VLAN traffic flows for the LAN. The trunk port marks the frames with special tags as they pass between the access port and its destination. These tags help distinguish data traffic. Authentication servers (such as RADIUS and Kerberos) must be on the same Management VLAN. Additionally, DHCP and BOOTP servers must be on the same Management VLAN as well.

5 Select a template from the list below for configuring Access Points to WIPS sensors:

A/B/G/N WLAN and Sensor	Enables 802.11a, 802.11g, 802.11bgn and 802.11an for the WLAN and dedicates the AP as a sensor.
B/G/N WLAN and Sensor	Enables 802.11g and 802.11bgn for the WLAN and dedicates the AP as a sensor.
A/N WLAN and Sensor	Enables 802.11a and 802.11an for the WLAN and dedicates the AP as a sensor.
A/B/G/N WLAN only, no Sensor	Enables 802.11a, 802.11g, 802.11bgn and 802.11an for the WLAN and it does not enable the AP as a sensor.
Sensor only Spectrum Analysis mode (no WLAN)	Enables the AP as a sensor and does not enable any 802.11a/b/g/n traffic.
B/G/N WLAN no Sensor	Enables 802.11g and 802.11bgn traffic for the WLAN and it does not enable the AP as a sensor.
A/N WLAN no Sensor	Enables 802.11a and 802.11n traffic for the WLAN and it does not enable the AP as a sensor.
Radios Off	Disables all radios on the selected Access Port.

6 Enter a list of IP Filter Rules for the Access Port:

In Filters	Enter a comma-separated list of IP filters defined for the In direction.
Out Filters	Enter a comma-separated list of IP filters defined for the Out direction.

7 Select an IP Filter from the drop-down menu.

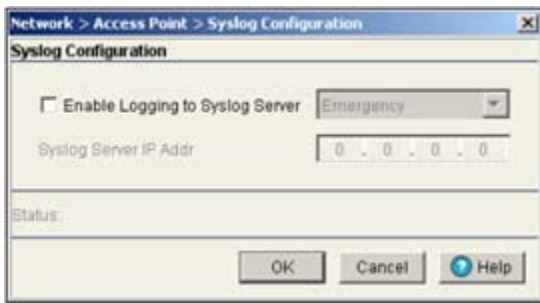
8 Select the *Enable LED for AAP* option to locate the Adaptive AP. The AP's LED will flash indicating its location in your setup.

Configuring a Syslog Server on the AAP from the controller

To configure an external Syslog server on the AAP from the controller:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *Configuration* tab.

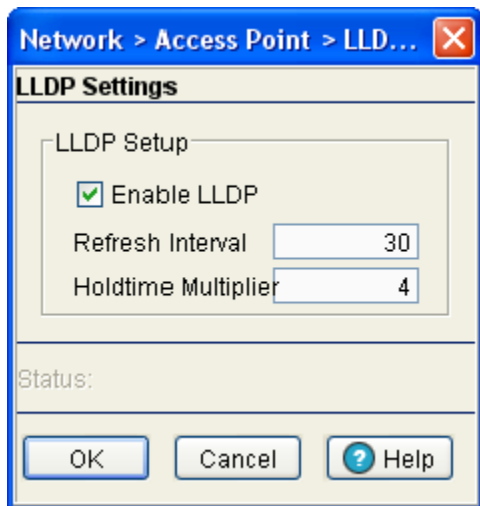
- 3 Click the *Syslog Config* button.



- 4 Check the *Enable Logging to Syslog Server* option to enable logging to an external Syslog server. Select the logging level from the drop-down menu.
- 5 Enter the IP address of the external Syslog server in the *Syslog Server IP Addr* field.
- 6 Click the *OK* button.

Configuring LLDP Settings for Access Port

Link Layer Discovery Protocol (LLDP) is a protocol that enables devices to advertise their capabilities and media-specific configuration. LLDP provides a standard method of discovering and representing the physical network connections of a given network management domain.



- 1 Check the *Enable LLDP* checkbox to enable or disable the transmission of LLDP advertisements.
- 2 Enter the refresh interval value in the *Refresh Interval* field. This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent.
- 3 Enter the holdtime multiplier value in the *Holdtime Multiplier* field. This parameter is a multiplier on the 'Refresh Interval' that determines the actual TTL value used in an LLD PDU.



NOTE

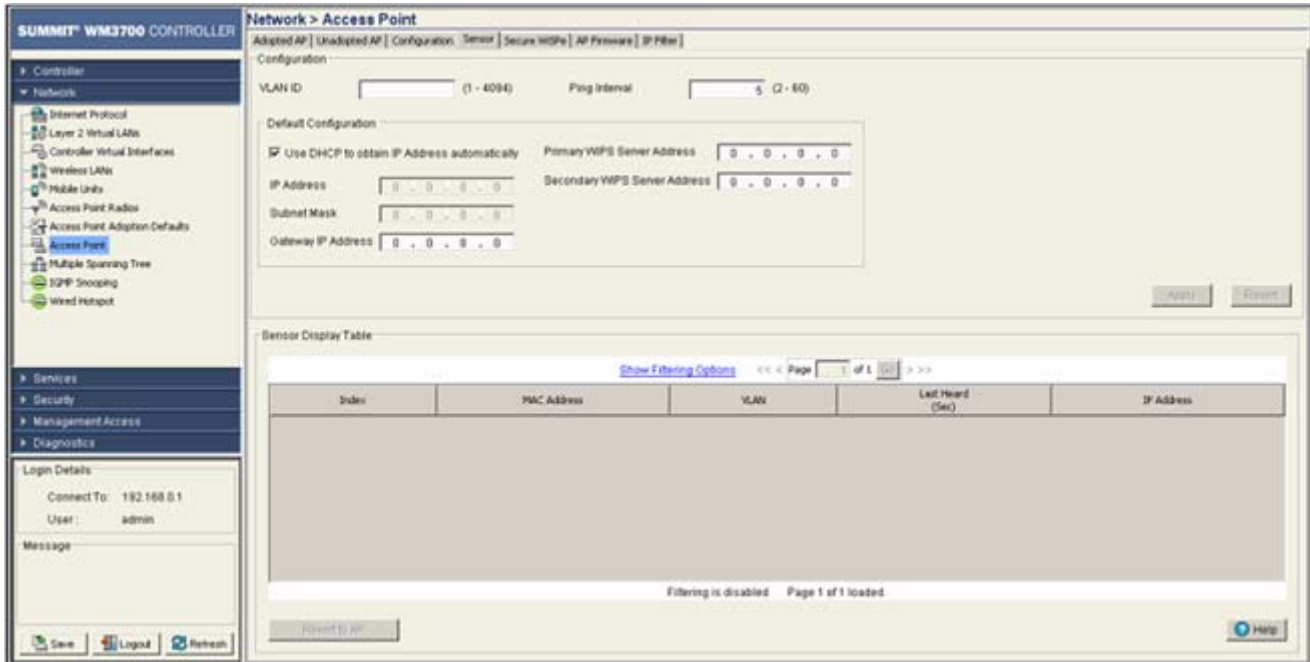
These settings apply only to the Altitude 4600 Series Access Ports.

Viewing Sensor Information

Use the *Sensor* tab to view information on Access Points configured as sensors and if needed revert them to Access Ports.

To view existing Sensor information:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *Sensor* tab.



- 3 Specify the global default *VLAN ID* and the *Ping Interval* for all sensors and click the *Apply* button.
- 4 In the *Default Configuration* section, give the default configuration values of the WIPS server. Unselect the *Use DHCP to obtain IP Address automatically* option to assign IP address of the VLAN manually and do not want DHCP to provide them. Selecting this disables the IP address field and the Subnet Mask field. Enter the *IP Address* and the *Subnet Mask* of the default VLAN in the respective fields. Also enter the *Gateway IP Address*, *Primary WIPS Server Address*, and the *Secondary WIPS Server Address*. The *Sensor Display Table* displays the following information:

Index	Displays the numerical value assigned to each sensor AP.
MAC Address	Displays the Media Access Control (MAC) address for each sensor AP.
VLAN	Displays the VLAN that each sensor AP is associated with.
Last Heard (sec)	Displays the number of seconds since the controller last received packets from each sensor AP.
IP Address	Displays the current IP address for each sensor AP.
Revert to AP	Select a sensor AP from the table and click the <i>Revert to AP</i> button to return to convert the AP back to a standard Access Port.

Configuring Secure WiSPe

To configure Secure WiSPe:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *Secure WiSPe* tab.

SUMMIT® WM3600 CONTROLLER

Network > Access Point

Adopted AP | Unadopted AP | Configuration | **Secure WiSPe** | AP Firmware | IP Filter

Global Configuration

Enter 8-64 characters

Default Pre Shared Secret: [*****]

Apply | Revert

Secure WiSPe Table

Show Filtering Options | View By Page | View all | Page 1 of 1

MAC Address	AP Type	Secure-Mode Enabled	Pre-Staging Enabled
00-04-96-44-51-8C	AP46X0	✘	✘

Filtering is disabled | Page 1 of 1 loaded.

Edit | Enable Secure Mode | Disable Secure Mode | Help

Left sidebar menu: Controller, Network (Internet Protocol, Layer 2 Virtual LANs, Controller Virtual Interfaces, Wireless LANs, Mobile Units, Access Point Radios, Access Point Adoption Defaults, **Access Point**, Multiple Spanning Tree, IGMP Snooping), Services, Security, Management Access, Diagnostics.

Login Details: Connect To: 10.255.108.36, User: admin

Message: [Empty]

Buttons: Save, Logout, Refresh

- 3 Enter a *Default Pre-Shared Secret* used for Secure WiSPe authentication. The shared secret must be between 8 and 64 characters. The default factory value is *defaultS*.
- 4 The *Secure WiSPe Table* displays the following information on each configured AP:

Controller	The <i>Controller</i> field displays the IP address of the cluster member associated with each AP. When clustering is enabled on the controller and Cluster GUI is enabled, the <i>Controller</i> field will be available on the AP configuration screen. For information on configuring enabling Cluster GUI, see “ Managing Clustering Using the Web UI ” on page 358.
MAC Address	Displays the MAC Addresses for each of the Access Ports.
AP Type	The AP Type displays the AP model (AP4600 Series Access Port only).
Secure Mode Enabled	Indicates if Secure Mode is enabled for each of the listed Access Ports. A green checkmark indicates Secure Mode is enabled and a red X indicates that Secure Mode is disabled.

Pre-Staging
Enabled

Indicates if Pre-Staging Mode is enabled for each of the listed Access Ports. A green checkmark indicates Pre-Staging is enabled and a red X indicates that Pre-Staging is disabled.

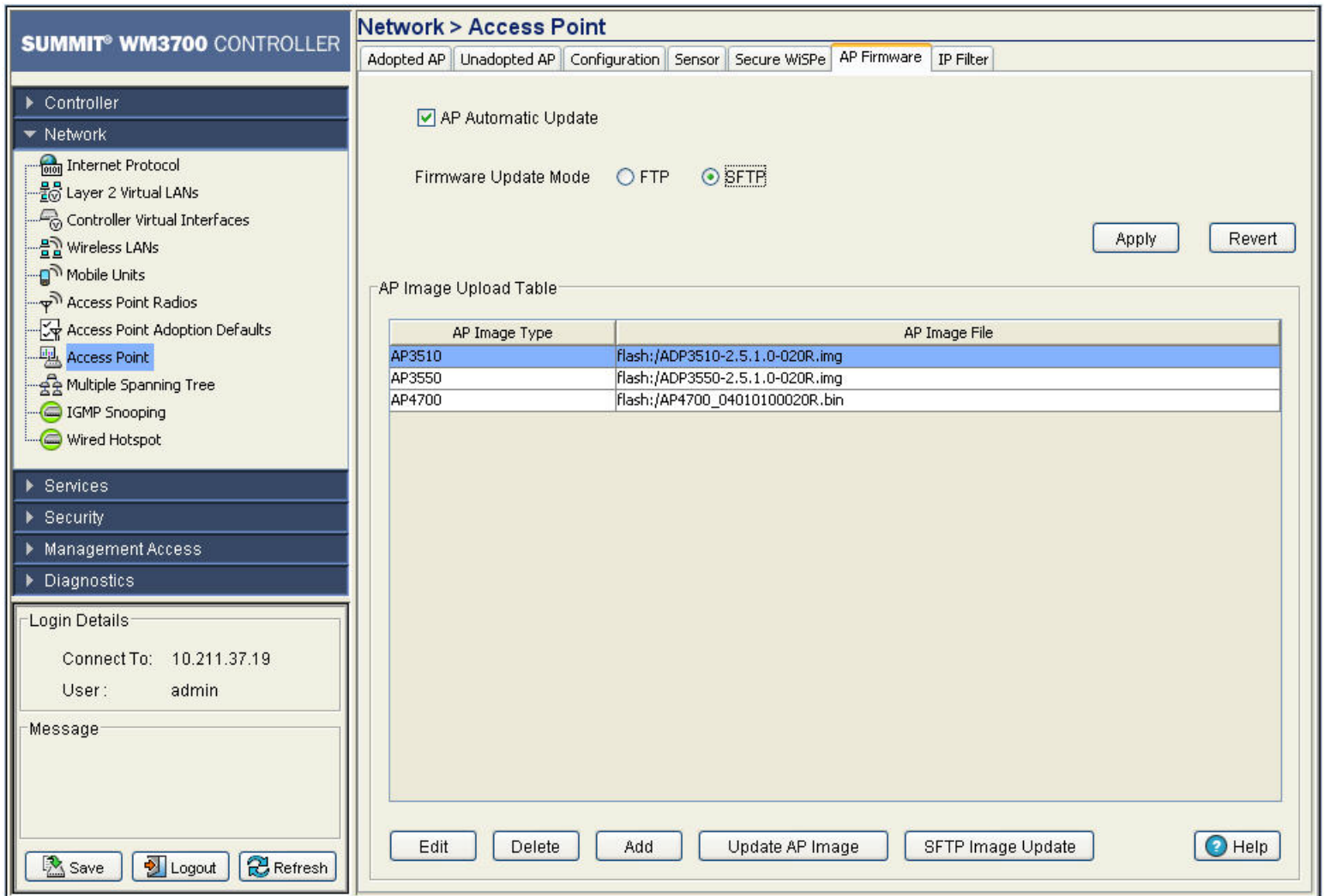
- 5 To edit the Secure WiSPe settings for an AP, select an AP from the *Secure WiSPe Table* and click the *Edit* button.
- 6 To enable Secure Mode, click the *Enable Secure Mode* button to enable secure-mode to a set of APs. The AP's MAC Address and mode will be saved in the running configuration. If secure-mode is set to enable, it means that WISP-e transactions for this AP will be secured.
- 7 To disable Secure Mode, click the *Disable Secure Mode* button to disable secure-mode to a set of APs. The AP's MAC Address and mode will be saved in the running configuration. If secure-mode is set to disable, it means that WISP-e transactions for this AP will not be secured.
- 8 When using clustering and the Cluster GUI feature is enabled, a pull-down menu will be available to select which cluster members' APs are displayed. To view APs from all cluster members, select *All* from the pull-down menu. To view APs radios from a specific cluster member, select that member's IP address from the pull-down menu.

Configuring Adaptive AP Firmware

Refer to the *AP Firmware* tab to view the Access Port and Adaptive AP firmware image associated with each adopted Access Port or Adaptive AP. The screen allows you to update the firmware image for Adaptive APs that associate with the controller.

To view AP firmware information:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *AP Firmware* tab.



- 1 Enable or disable AP Automatic Update (AP Automatic Update).

AP Automatic Update

Check this box to enable automatic update of Access Port or Adaptive AP firmware when an Access Port or Adaptive AP associates with the controller. The AP image file used for automatic update are specified in the *AP Image Upload Table* below.

Firmware Update Mode

Select *FTP* or *SFTP* for specifying the firmware update mode. If you select the *FTP* radio button, the *Update AP Image* and the *SFTP Image Update* buttons will be disabled.

2 View the firmware information displayed per Adaptive AP type with the following data:

AP Image Type	The AP image type is the model of Access Point or Adaptive AP, which the firmware is used with. Available image types are: <ul style="list-style-type: none">• AP3510• AP3550• AP4600 Series• AP4700 Series
AP Image File	Displays the filename of the image file associated with the <i>AP Image Type</i> .

3 To add a new AP firmware image, click the *Add* button.

4 To edit the details of an AP firmware image, highlight an AP image type and click the *Edit* button.

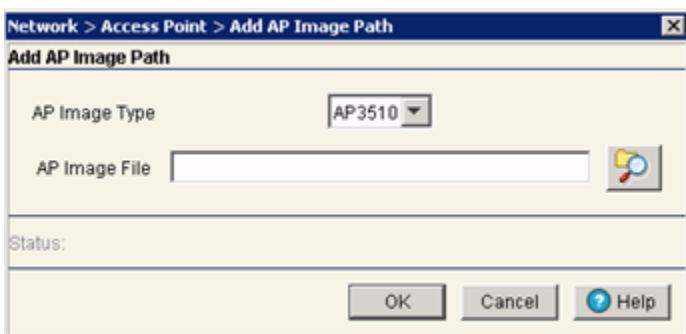
5 To delete an existing AP firmware image, highlight an AP image type and click the *Delete* button.

To modify the AP Firmware Image settings:

1 Select *Network > Access Point* from the main menu tree.

2 Click the *AP Firmware* tab.

3 Click the *Add* button to display a screen to configure the *AP Image Type* and *AP Image File*.



4 Specify the *AP Image Type*.

5 Specify the *AP Image File*. You can browse the controller file systems using the browser icon. AP images must be on the flash, system, nvram, or usb file systems in order for them to be selected.

6 Click the *OK* button to save the changes and return to the *AP Firmware* tab.

Editing an Existing AP Firmware Image

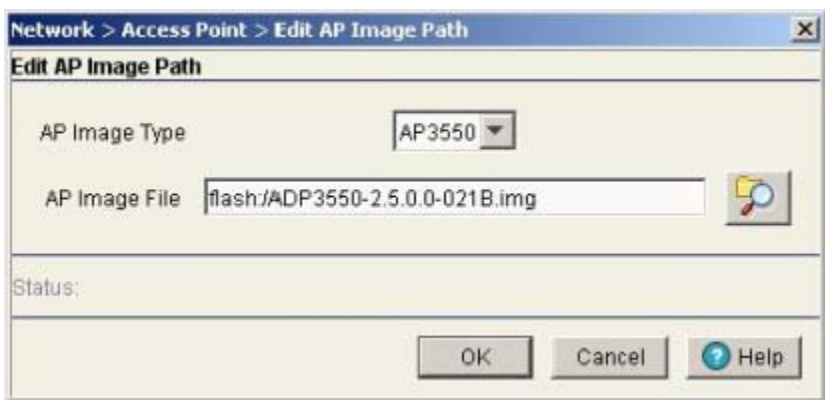
To modify the AP Firmware Image settings:

1 Select *Network > Access Point* from the main menu tree.

2 Click the *AP Firmware* tab.

3 Select an *AP Image Type* from the *AP Image Upload* table.

- 4 Click the *Edit* button to display a screen to change the *AP Image Type* or *AP Image File*.

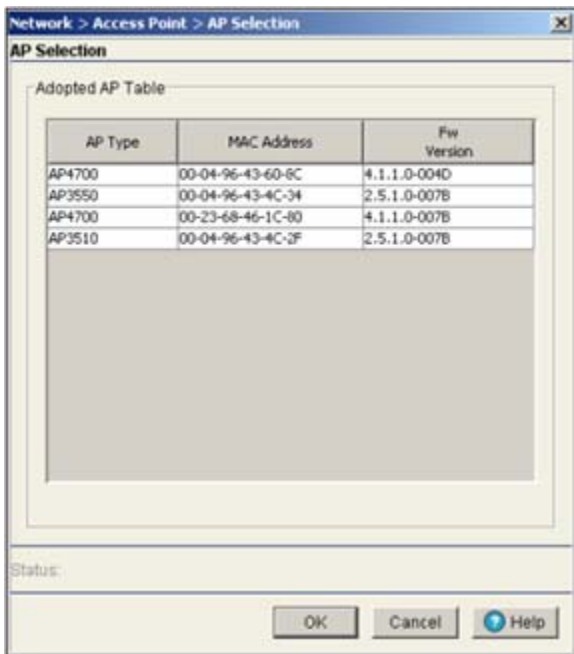


- 5 Modify the *AP Image Type* as necessary.
- 6 Modify the *AP Image File* as necessary. You can browse the controller file systems using the browser icon. AP images must be on the flash, system, nvram, or usb file systems in order for them to be selected.
- 7 Click the *OK* button to save the changes and return to the *AP Firmware* tab

Updating an existing AAP Image Firmware

Use the *Update AP Image* button to update a selected Adaptive AP image firmware. To update an AP image:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *AP Firmware* tab.
- 3 Select an AP image from the *AP Image Upload Table* and click the *Update AP Image* button.

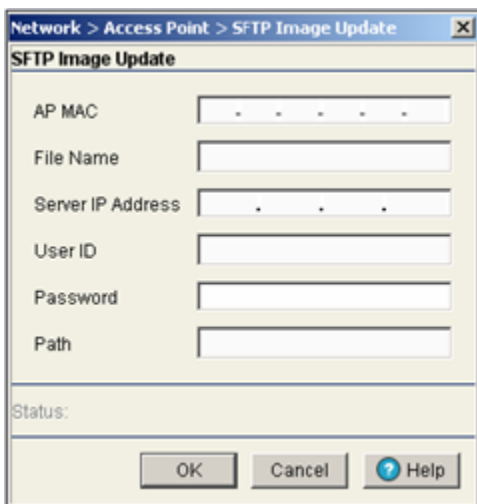


AP Type identifies the Access Port/Point model. *MAC Address* is the MAC address of the AP selected. *Fw Version* gives you the current firmware version on the Access Port. Use this information to assess whether the software requires an upgrade for better compatibility with the Controller.

Updating an AAP Image/Firmware using SFTP

You can update an AAP image from an external SFTP server using the *SFTP Image Update* button. To update using SFTP:

- 1 Select *Networks > Access Point* from the main menu tree.
- 2 Click the *AP Firmware* tab.
- 3 Click the *SFTP Image Update* button.



AP MAC Address is the device MAC address. Ensure that this is the actual hard-coded MAC address of the device. *File Name* is the name of the AP image. *Server IP Address* gives you the IP address of the SFTP server where all the AP images reside. *User ID* is the ID to log in to the SFTP server. *Password* is the SFTP password used while logging in. *Path* gives you the path of the AP image residing in the server.

Configuring IP Filtering

Refer to the *IP Filter* tab to view the IP filter settings for the controller. The screen allows you to update the IP filter settings of the controller.

To view IP Filtering information:

- 1 Select *Network > Access Point* from the main menu tree.
- 2 Click the *IP Filter* tab.

The screenshot shows the Summit WM3600 Controller web interface. The main content area displays the 'IP Filter' configuration page. The table below represents the data shown in the 'IP Filter Table'.

Name	Priority	Decision	Protocol	Src IP Start	Src IP End	Dst IP Start	Dst IP End	Dst	Dst

3 The *IP Filter Table* displays the following information on each configured IP filter:

Name	Displays the name for each of the IP filters.
Priority	Displays the numerical priority assigned to each IP filter.
Decision	Defines what to do for filtered IP addresses.
Protocol	Specify the protocol used for the filter policy. The options are <i>ALL</i> , <i>TCP</i> , <i>UDP</i> , <i>ICMP</i> , <i>PIM</i> , <i>GRE</i> , <i>RSVP</i> , <i>IDP</i> , <i>PUP</i> , <i>EGP</i> , <i>IPIP</i> , <i>ESP</i> , <i>AH</i> , <i>IGMP</i> , <i>IPVG</i> , <i>COMPR_H</i> and <i>RAW_IP</i> . The protocol number can also be used as the protocol name.
Src IP Start	Creates the beginning of source IP address range to be either allowed or denied IP packet forwarding. The source address is where the packet originated. Setting the <i>SRC IP End</i> value the same as the <i>SRC IP Start</i> allows or denies just this address without defining a range.
Src IP End	Providing this address completes a range of source (data origination) addresses that can either be allowed or denied access to the WLAN.
Dst IP Start	Creates the beginning of destination IP address range to be either allowed or denied IP packet forwarding. The source address is where the packet originated. Setting the <i>Dst IP End</i> value the same as the <i>Dst IP Start</i> allows or denies just this address without defining a range.

- Dst IP End Providing this address completes a range of destination addresses that can either be allowed or denied access to the WLAN.
- Dst Port Start Defines the port number representing the beginning protocol port range either allowed or denied permission to the target WLAN.
- Dst Port End Defines the port number representing the ending protocol port range either allowed or denied permission to the target WLAN.

4 To add a new IP filter policy, click the *Add* button.

5 To edit the details of an IP filter, highlight an IP filter and click the *Edit* button.

Network > Access Point > Apply Filter

Apply Filter

Name: test

Rule: 1

Decision: permit

Protocol: IPv6

Source IP Start: 0 . 0 . 0 . 0

Source IP End: 255 . 255 . 255 . 255

Destination IP Start: 0 . 0 . 0 . 0

Destination IP End: 255 . 255 . 255 . 255

Destination Port Start: 1

Destination Port End: 65535

Status:

OK Cancel ? Help

6 To delete an IP filter, highlight an IP filter and click the *Delete* button.

Multiple Spanning Tree

Multiple Spanning Tree Protocol (MSTP) provides a VLAN-aware protocol and algorithm to create and maintain a loop-free network. It allows the configuration of multiple spanning tree instances. This ensures a loop-free topology for one or more VLANs. It allows the network administrator to provide a different path for each group of VLANs to better utilize redundancy.

MSTP allows rapid convergence similar to *Rapid Spanning Tree Protocol (RSTP)*. RSTP is an independent protocol and MSTP does not use RSTP. Since MSTP allows VLANs to be grouped in an instance, each instance can have its own spanning-tree topology independent of other spanning-tree instances. This architecture provides multiple forwarding links for data traffic and load balancing, and therefore reduces the number of spanning-tree instances required to support a large number of VLANs.

Using MSTP, the network can be divided into regions. All controllers within a region use the same VLAN to instance mapping. The entire network runs a spanning tree instance called the *Common Spanning Tree* instance (CST) that interconnects regions as well as legacy (STP and RSTP) bridges. The regions run on a local instance for each configured MSTP instance.

The network-wide spanning tree for instance 0 is known as the *Common Spanning Tree (CST)*. A spanning tree for any other instance, which is local to a region, is known as an *Internal Spanning Tree (IST)*. The *Common and Internal Spanning Tree (CIST)* (which consists of the CST as well as all ISTs across regions) interconnects all bridges in the network.

The following definitions describe the STP instances that define an MSTP configuration:

- *Common Spanning Tree (CST)*—MSTP runs a single spanning tree instance (called the *Common Spanning Tree*) that interconnects all the bridges in a network. This instance treats each region as a single bridge. In all other ways, it operates exactly like *Rapid Spanning Tree (RSTP)*.
- *Common and Internal Spanning Trees (CIST)*—CIST contains all of the ISTs and bridges not formally configured into a region. This instance interoperates with bridges running legacy STP and RSTP implementations.
- *Multiple Spanning Tree Instance (MSTI)*—The MSTI is identified by an *MSTP identifier (MSTPid)* value from 1 to 15. This defines an individual instance of a spanning tree. One or more VLANs can be assigned to an MSTI. A VLAN cannot be assigned to multiple MSTIs. The multiple spanning tree instance 0 is always present. VLANs not explicitly assigned to an instance are assigned to instance 0.
- *MSTP Region*—These are clusters of bridges that run multiple instances of the MSTP protocol. Multiple bridges detect they are in the same region by exchanging their configuration digest (which is dependent on the VLAN to instance mapping), region name, and revision-level. If you need to have two bridges in the same region, the two bridges must have identical VLAN to instance mappings, region names, and revision-levels.

To configure the controller for MSTP support, configure the region name and the revision on each controller being configured. This region name is unique to each region. Then create one or more instances and assign IDs. VLANs are then assigned to instances. These instances must be configured on controllers that interoperate with the same VLAN assignments. Port cost, priority, and global parameters can then be configured for individual ports and instances.

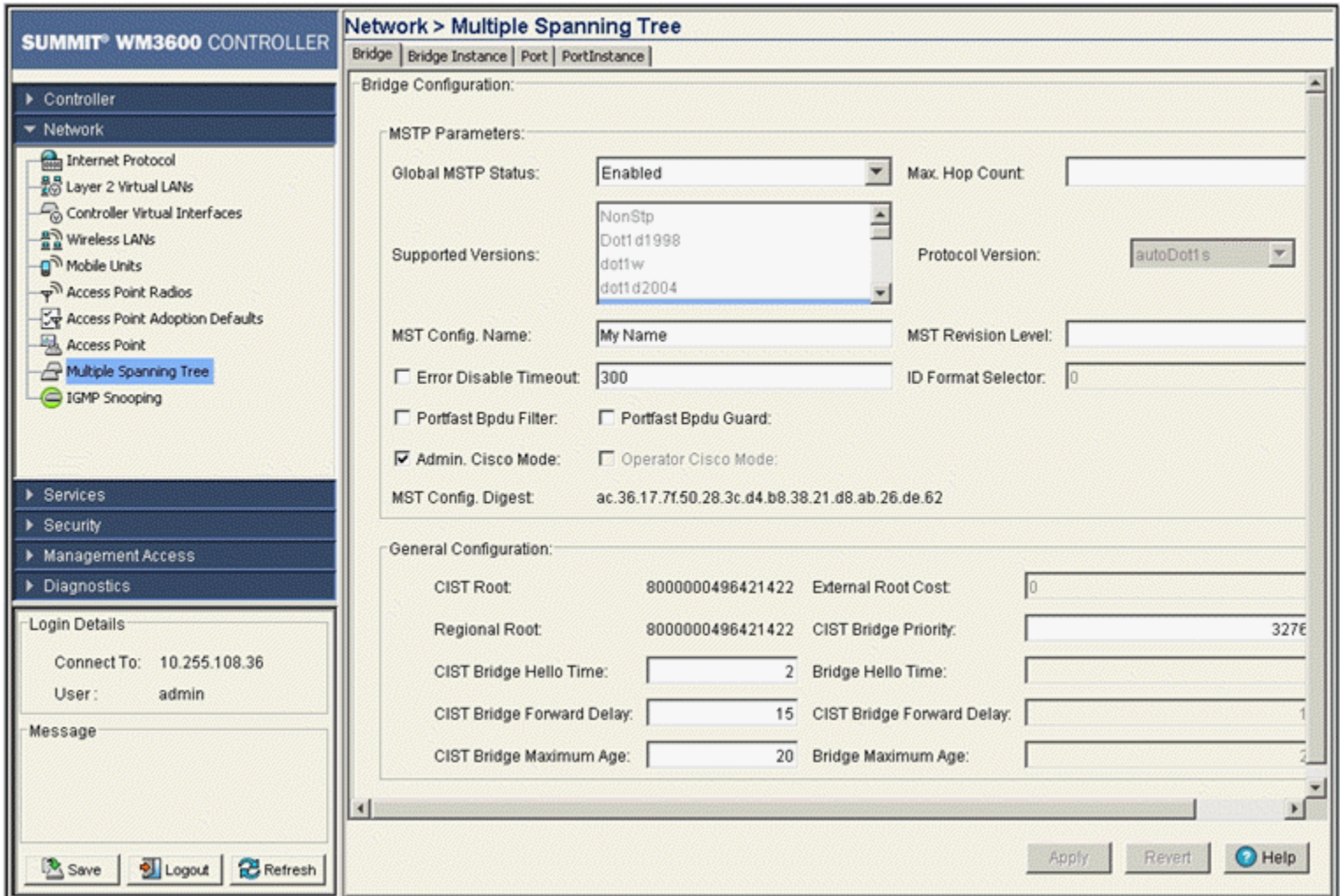
The Multiple Spanning Tree option contains separate tabs for the following activities:

- [Configuring a Bridge on page 281](#)
- [Viewing and Configuring Bridge Instance Details on page 285](#)
- [Configuring a Port on page 287](#)
- [Viewing and Configuring Port Instance Details on page 291](#)

Configuring a Bridge

Use the *Bridge* tab to configure the Bridge. This window displays bridge configuration details for the controller

To configure the MSTP bridge:



To configure the MSTP bridge:

- 1 Select *Network > Multiple Spanning Tree* from the main menu tree.
- 2 Select the *Bridge* tab (should be the displayed tab by default).
- 3 Refer to the *MSTP Parameter* field to view or set the following:

Global MSTP Status	Use the drop-down menu to define MSTP status. The default is Enabled.
Max Hop Count	Displays the maximum allowed hops for a BPDU (Bridge Protocol Data Unit) in an MSTP region. This value is used by all the MSTP instances.
Supported Versions	Displays the different versions of STP supported.

Protocol Version	<p>Displays the current protocol version in use. Available MSTP protocol versions are:</p> <ul style="list-style-type: none"> • <i>forceNonStp</i> • <i>forceLegacyDot1d</i> • <i>forceDot1w</i> • <i>autoDot1s</i> • <i>unknown</i>
MST Config. Name	<p>Enter a name for the MST region. This is used when configuring multiple regions within the network. Each controller running MSTP is configured with a unique MST region name. This helps when keeping track of MSTP configuration changes. Increment this number with each configuration change. The revision-level specifies the revision-level of the current configuration.</p>
MST Revision Level	<p>Assign an MST revision level number to the MSTP region to which the device belongs. Each controller running is configured with a unique MSTP name and revision number. This helps when keeping track of MSTP configuration changes. Increment this number with each configuration change. The revision level specifies the revision level of the current configuration.</p>
Error Disable Timeout	<p>Select this option to enable an error disable-timeout facility. The error disable-timeout is used to set a timeout value for ports disabled resulting from a BPDU guard.</p> <p>The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port.</p>
ID Format Selector	<p>Displays the ID format currently in use.</p>
portfast Bdpu Filter	<p>Select this checkbox to enable BPDU filter for all portfast-enabled ports. The Spanning Tree Protocol sends BPDUs from all the ports. Enabling the BPDU filter feature ensures portfast-enabled ports do not transmit or receive any BPDUs.</p>
Portfast Bdpu Guard	<p>Select this checkbox to enable BPDU guard for all portfast-enabled ports.</p> <p>When the BPDU Guard feature is set for bridge, all portfast-enabled ports of the bridge that have BPDU set to default shutdown the port on receiving a BPDU. Hence no BPDUs are processed.</p>
Admin Cisco Mode	<p>Select this checkbox to enable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP.</p>
Operator Cisco Mode	<p>Displays whether Cisco's version of MSTP is running. This is not a configurable parameter.</p>
MST Config Digest	<p>Displays the Configuration Digest derived from the MSTP Configuration table.</p>

4 Refer to the *General Configuration* field for the following:

CIST Root	<p>This displays the CIST (Common and Internal Spanning Tree) root bridge's bridge identifier. The bridge identifier consists of a priority value followed by the MAC address. The lower the path cost, the greater the likelihood of the bridge becoming the root.</p>
External Root Cost	<p>Displays the root cost of the CIST root.</p>
Regional Root	<p>Displays the regional roots MAC address.</p>
CIST Bridge Priority	<p>Set the bridge priority for the common instance. The value entered, determines the likelihood this bridge is selected as the root.</p> <p>The lower the priority the greater the likelihood of the bridge becoming a root.</p>

CIST Bridge HelloTime	<p>Set the CIST Hello Time (in seconds). After the defined interval all bridges in a bridged LAN exchange BPDUs.</p> <p>The hello time is the time interval (in seconds) the device waits between BPDU transmissions.</p> <p>A very low value leads to excessive traffic on the network, whereas a higher value delays the detection of a topology change. This value is used by all instances.</p>
Bridge Hello Time	<p>Displays the configured Hello Time. If this is the root bridge, the value is equal to the configured Hello Time.</p>
CIST Bridge Forward Delay	<p>Enter the CIST bridge forward delay value received from the root bridge. If this is the root bridge, the value will be equal to the Configured Forward Delay.</p> <p>The forward delay value is the maximum time (in seconds) the root device waits before changing states (from a listening state to a learning state to a forwarding state).</p> <p>This delay is required, as every device must receive information about topology changes before forwarding frames.</p> <p>In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops may result.</p>
CIST Bridge Forward Delay	<p>Displays the configured forward delay period.</p>
CIST Bridge Maximum Age	<p>Enter the CIST bridge maximum age received from the root bridge. The maximum age is the maximum time (in seconds) for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The max-age should be greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.</p>
Bridge Maximum Age	<p>Displays the BPDU maximum age value. If this is the root bridge, the value will be equal to the Configured Max Age.</p>

Viewing and Configuring Bridge Instance Details

The *Bridge Instance* tab displays the number of MSTP instance created and VLANs associated with it. To view and configure the MSTP bridge instance:

- 1 Select *Network > Multiple Spanning Tree* from the main menu tree.
- 2 Select the *Bridge Instance* tab.

The screenshot shows the Summit WM3600 Controller web interface. The main content area is titled "Network > Multiple Spanning Tree" and has tabs for "Bridge", "Bridge Instance", "Port", and "PortInstance". Below the tabs is a table with the following columns: "Id", "Bridge Priority", "Bridge ID", "Designated Root", "Internal", "Root Port", "Master Port", and "VLANs". The table is currently empty. At the bottom of the page, there are buttons for "Edit", "Delete", "Add", "Add VLANs", and "Delete VLANs". A "Help" button is also present in the bottom right corner. The left sidebar contains a navigation tree with "Multiple Spanning Tree" selected. Below the navigation tree, there is a "Login Details" section with "Connect To: 10.255.108.36" and "User: admin". At the bottom of the sidebar, there are buttons for "Save", "Logout", and "Refresh".

The *Bridge Instance* tab displays the following:

ID	Displays the ID of the MSTP instance.
Bridge Priority	Displays the bridge priority for the associated instance. The Bridge Priority is assigned to an individual bridge based on whether it is selected as the root bridge. The lower the priority, the greater likelihood the bridge becoming the root for this instance.
Bridge ID	Displays the bridge id of the bridge for this instance.
Designated Root	Displays the ID of the root bridge that sent the BPDU received on this port.
Internal Root Cost	Displays the configured path cost on a link connected to this port within the internal MSTP region.
Root Port	Displays the Port ID of the root port for this instance.

Master Port	Displays the Port ID of the master port, if any, for this instance.
VLANs	Displays the list of VLANs included in this MSTP instance.

- 3 Select an ID and click the *Delete* button to remove from the list.

Creating a Bridge Instance

To create a VLAN instance and associate it with a bridge as a numerical identifier:

- 1 Select *Network > Multiple Spanning Tree* from the main menu tree.
- 2 Select the *Bridge Instance* tab.
- 3 Click the *Add* button.

- 4 Enter a value between 1 and 15 as the Instance ID.
- 5 Click *OK* to save and commit the changes.
- 6 The *Bridge Instance* tab will now display the new instance ID.
- 7 Click *Cancel* to disregard the new Bridge Instance ID.

Associating VLANs to a Bridge Instance

- 1 Select *Network > Multiple Spanning Tree* from the main menu tree.
- 2 Select the *Bridge Instance* tab.
- 3 Select an ID from the table within the *Bridge Instance* tab and click the *Add VLANs* button.

- 4 Enter a VLAN ID between 1 to 4094 in the *VLAN ID* field. This VLAN ID is associated with the *Instance index*. You can add multiple VLANs to an instance.

- 5 Click *OK* to save and commit the new configuration.
- 6 Click *Cancel* to disregard the changes.

Configuring a Port

Use the *Port* tab to view and configure MSTP port parameters, including enabling/disabling the spanning tree algorithm on one or more ports (displaying the designated bridge and port/root information).

To view and configure MSTP port details:

- 1 Select *Network > Multiple Spanning Tree* from the main menu tree.
- 2 Select the *Port* tab.

SUMMIT WM3600 CONTROLLER

Network > Multiple Spanning Tree

Bridge | Bridge Instance | Port | PortInstance

Index	Admin MAC Enable	Oper MAC Enable	AutoEdge	Designated Bridge	Guard Root	Admin Portfast Bpdu Filter	Oper Portfast Bpdu Filter	Admin Portfast Bpdu Guard	Oper Portfast Bpdu	Port Versior
2001	✓	✓	✗	0000000496421422	✗	Default	✗	Default	✗	MSTP
2002	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2003	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2004	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2005	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2006	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2007	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2008	✓	✓	✗	0000000000000000	✗	Default	✗	Default	✗	MSTP
2009	✓	✓	✗	8000000496421422	✗	Default	✗	Default	✗	MSTP

Save Logout Refresh Edit

The *Port* tab displays the following information (ensure you scroll to the right to view the numerous port variables described):

Index	Displays the port index.
Admin MAC Enable	Displays the status of the Admin MAC. Change the status using the <i>Edit</i> button. A green check mark indicates the Admin MAC Enable status is active/enabled.
Oper MAC Enable	Displays the status of the Oper MAC Enable. You can change the status using the <i>Edit</i> button. A green check mark indicates that the Oper MAC Enable status is active/enabled.
AutoEdge	Displays whether the port can automatically detect whether it is an edge port.
Designated Bridge	Displays the ID of the bridge sent the best BPDU received on this port.
Guard Root	Displays whether the listed port index enforces root bridge placement. The guard root ensures that the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.
Admin PortFast Bpdu Filter	Displays the Portfast BPDU filter for the admin port. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter ensures portfast-enabled admin ports do not transmit or receive BPDUs.
Oper PortFast Bpdu Filter	Displays a PortFast BPDU filter for the oper port. Enabling the BPDU Filter feature ensures portfast-enabled oper ports do not transmit or receive BPDUs.
Admin PortFast Bpdu Guard	Displays the whether BPDU Guard is currently enabled for this port. When set for a bridge, all portfast-enabled ports having the bpdu-guard set to default shut down the port on receiving the BPDU. When this occurs, the BPDU is not processed.
Oper PortFast Bpdu Guard	Displays the whether BPDU Guard is currently enabled for this port. When the OperPort PortFast BPDU Guard feature is set for a bridge, all PortFast-enabled ports that have the bpdu-guard set to default shut down the port on receiving a BPDU. When this occurs, the BPDU is not processed.
Port Version	Displays the port version associated with this instance. It can be either of the following: <ul style="list-style-type: none">• STP• RSTP• MSTP
Port State	Port State displays the MSTP state for this port. A port must be enabled to be able to forward.
Port Enable	Displays the enable/disable MSTP designation of each port. A green check mark indicates the Oper MAC Enable status is active/enabled.

Port Path Cost	<p>Port Path Cost displays the path cost for the specified port index. The default path cost depends on the speed of the interface.</p> <table border="0"> <thead> <tr> <th>Speed</th> <th>Default path cost</th> </tr> </thead> <tbody> <tr> <td><=100000 bits/sec</td> <td>200000000</td> </tr> <tr> <td><=1000000 bits/sec</td> <td>20000000</td> </tr> <tr> <td><=10000000 bits/sec</td> <td>2000000</td> </tr> <tr> <td><=100000000 bits/sec</td> <td>200000</td> </tr> <tr> <td><=1000000000 bits/sec</td> <td>20000</td> </tr> <tr> <td><=10000000000 bits/sec</td> <td>2000</td> </tr> <tr> <td><=100000000000 bits/sec</td> <td>200</td> </tr> <tr> <td><=1000000000000 bits/sec</td> <td>20</td> </tr> <tr> <td>>1000000000000 bits/sec</td> <td>2</td> </tr> </tbody> </table>	Speed	Default path cost	<=100000 bits/sec	200000000	<=1000000 bits/sec	20000000	<=10000000 bits/sec	2000000	<=100000000 bits/sec	200000	<=1000000000 bits/sec	20000	<=10000000000 bits/sec	2000	<=100000000000 bits/sec	200	<=1000000000000 bits/sec	20	>1000000000000 bits/sec	2
Speed	Default path cost																				
<=100000 bits/sec	200000000																				
<=1000000 bits/sec	20000000																				
<=10000000 bits/sec	2000000																				
<=100000000 bits/sec	200000																				
<=1000000000 bits/sec	20000																				
<=10000000000 bits/sec	2000																				
<=100000000000 bits/sec	200																				
<=1000000000000 bits/sec	20																				
>1000000000000 bits/sec	2																				
Port Designated Cost	<p>Displays the port cost for each port on the controller. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.</p>																				
Designated Port	<p>Defines the port connection used to send and receive packets. By having only one designated port per segment, all looping issues should be resolved. Once the designated port has been selected, any other ports that connect to that segment become non-designated ports and block traffic from taking the defined path.</p>																				
Forward Transitions	<p>Forward Transitions displays the number of MSTP state transitions to the forwarding state that have occurred on this port.</p>																				
Protocol Migration	<p>The controller can interoperate with legacy 802.1d bridges running STP / RSTP. If the port receives a legacy 802.1D configuration BPDU, it only sends 802.1D BPDUs over its port from that point on. Enable this option to restart detection of whether the port is connected to an MSTP capable bridge or a legacy 802.1 bridge.</p>																				
Admin Edge Port	<p>A green checkmark defines the listed index enabled as an Admin Edge Port, and a red "X" defines the listed index as not being an Admin Edge Port. Enable it only on ports that connect to a single location.</p>																				
Oper Edge Port	<p>Oper Edge Port Displays whether the port is currently an edge port.</p>																				
Admin Point-to-Point	<p>Displays the point-to-point status as ForceTrue or ForceFalse. ForceTrue indicates this port should be treated as connected to a point-to-point link. ForceFalse indicates this port should be treated as having a shared connection.</p>																				
Oper Point-to-Point	<p>Displays whether the listed port index is configured to connect to another port through a point-to-point link. A green checkmark indicates the port as supporting point-to-point, and a red "X" indicates the port as having point-to-point disabled.</p>																				

3 Select an Id and click the *Edit* button to revise the selected MSTP port configuration.

Editing an MSTP Port Configuration

To edit and reconfigure MSTP Port parameters:

- 1 Select a row from the port table and click the *Edit* button.

The screenshot shows a dialog box titled "Network > Multiple Spanning Tree > Edit". The dialog contains the following fields and controls:

- Port Index: 2002
- Admin MAC Enable
- Port auto Edge
- Port Guard Root
- Admin PortFast BPDU Filter: Default
- Admin PortFast BPDU Guard: Default
- Port Version: MSTP
- Port Path Cost: 20000000
- Admin Point-to-Point status: ForceTrue
- Port Enable:
- Protocol Migration:
- Admin Edge Port:
- Status:
- Buttons: OK, Cancel, Help

The following MSTP Port parameters can be reconfigured:

Port Index	Displays the read-only Port Index.
Admin MAC Enable	Displays the status of the Admin MAC Enable. A green check mark indicates the status as enabled.
Port auto Edge	Select the checkbox to use the port as an edge port.
Port Guard Root	Select this checkbox to enable guard root for this port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.
Admin PortFast BPDU Filter	Enable this option to change the status of the Port Fast BPDU Filter.
Admin Port FastBPDU Guard	Enable this option to change the status of the Port Fast BPDU Guard.
Port Version	Select a value to reconfigure the port version.

Port Path Cost	Port Path Cost displays the path cost for the specified port index. The default path cost depends on the speed of the interface.																				
	<table border="0"> <thead> <tr> <th style="text-align: left;">Speed</th> <th style="text-align: left;">Default path cost</th> </tr> </thead> <tbody> <tr> <td><=100000 bits/sec</td> <td>200000000</td> </tr> <tr> <td><=1000000 bits/sec</td> <td>20000000</td> </tr> <tr> <td><=10000000 bits/sec</td> <td>2000000</td> </tr> <tr> <td><=100000000 bits/sec</td> <td>200000</td> </tr> <tr> <td><=1000000000 bits/sec</td> <td>20000</td> </tr> <tr> <td><=10000000000 bits/sec</td> <td>2000</td> </tr> <tr> <td><=100000000000 bits/sec</td> <td>200</td> </tr> <tr> <td><=1000000000000 bits/sec</td> <td>20</td> </tr> <tr> <td>>1000000000000 bits/sec</td> <td>2</td> </tr> </tbody> </table>	Speed	Default path cost	<=100000 bits/sec	200000000	<=1000000 bits/sec	20000000	<=10000000 bits/sec	2000000	<=100000000 bits/sec	200000	<=1000000000 bits/sec	20000	<=10000000000 bits/sec	2000	<=100000000000 bits/sec	200	<=1000000000000 bits/sec	20	>1000000000000 bits/sec	2
Speed	Default path cost																				
<=100000 bits/sec	200000000																				
<=1000000 bits/sec	20000000																				
<=10000000 bits/sec	2000000																				
<=100000000 bits/sec	200000																				
<=1000000000 bits/sec	20000																				
<=10000000000 bits/sec	2000																				
<=100000000000 bits/sec	200																				
<=1000000000000 bits/sec	20																				
>1000000000000 bits/sec	2																				
Admin Point-to-Point status	Defines the point-to-point status as ForceTrue or ForceFalse. ForceTrue indicates this port should be treated as connected to a point-to-point link. ForceFalse indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a controller or workstation is a point-to-point link.																				
Port Enable	Select this checkbox to use this port for the forwarding of packets on the controller.																				
Port Migration	The controller can interoperate with legacy 802.1d bridges running STP / RSTP. If the port receives a legacy 802.1D configuration BPDU, it only sends 802.1D BPDUs over its port from that point on. Enable this option to restart detection of whether the port is connected to an MSTP capable bridge or a legacy 802.1 bridge.																				
Admin Edge Port	Select the checkbox to define this port as an admin edge port.																				

- 2 Click *OK* to save and commit the new configuration.
- 3 Click *Cancel* to disregard the changes and revert back to the previous configuration.

Viewing and Configuring Port Instance Details

Use the *Port Instance* tab to view and configure MST parameters per port per instance, including Port Priority and Admin Internal Path Cost.

To view and configure the MSTP bridge instance:

- 1 Select *Network > Multiple Spanning Tree* from the main menu tree.
- 2 Select the *PortInstance* tab.

SUMMIT® WM3600 CONTROLLER

Network > Multiple Spanning Tree

Bridge | Bridge Instance | Port | PortInstance

Id	Index	State	Role	Internal Root Cost	Designated Bridge	Designated Port	Priority	AdminInternal Path Cost	OperInternal Path Cost
CIST	2001	Discarding	Disabled	0	0000000496421422	0000	128	0	20000000
CIST	2002	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2003	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2004	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2005	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2006	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2007	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2008	Discarding	Disabled	0	0000000000000000	0000	128	0	20000000
CIST	2009	Forwarding	Designated	0	8000000496421422	87d9	128	0	20000

Buttons: Save, Logout, Refresh, Edit, Help

The Port Instance table displays the following:

ID	Displays the instance ID.
Index	Displays the port index.
State	Displays the MSTP state for the port for that instance.
Role	Displays the MSTP state of the port.
Internal Root Cost	Displays the Internal Root Cost of a path associated with an interface. The lower the path cost, the greater likelihood of the interface becoming the root.
Designated Bridge	Displays the ID of the bridge that sent the best BPDU.
Designated Port	Designated Port displays the ID of the port that is the designated port for that instance.
Priority	Displays the port priority set for that port and instance.
AdminInternal Path Cost	Displays the configured Admin Internal Path Cost of a port. A value of 0 indicates that the user has not configured a path cost.

OperInternal Path Cost Displays the Operational Path Cost of a port. This displays the default cost if AdminInternal Path Cost is 0.

- 3 If necessary, select a CIST Index from the table and click the *Edit* button to change the port priority and internal path cost value. For additional information, see [“Editing a Port Instance Configuration” on page 293](#).

Editing a Port Instance Configuration

To edit and reconfigure Port Instance parameters:

- 1 Select a row from the port table and click the *Edit* button.

The screenshot shows a dialog box titled "Network > Multiple Spanning Tree > Edit". The dialog contains the following fields and values:

Port Instance ID:	CIST
Port Index:	2001
Port Priority:	128
Admin Internal Path Cost:	0
Operational Internal Path Cost:	200000

Below the fields is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Most of the MSTP Port Instance parameters can be reconfigured, as indicated below.

Port Instance ID	Read-only indicator of the instance ID used as a basis for other modifications.
Port Index	Read-only indicator of the port index used as a basis for other modifications.
Port Priority	If necessary, change the port priority value for the bridge. The lower the priority, the greater the likelihood of the port becoming a designated port.
Admin Internal Path Cost	Displays the configured Admin Internal Path Cost of a port. A value of 0 indicates that the user has not configured a path cost.
Operational Internal Path Cost	Displays the Operational Path Cost of a port. This displays the default cost if Admin Internal Path Cost is 0.

IGMP Snooping

The Internet Group Management Protocol (IGMP) is a protocol used for managing members of IP multicast groups. The controller listens to the IGMP network traffic and forwards the IGMP multicast packets to member portals on which the interested hosts are connected. On the wired side of the network, the controller floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

IGMP Snoop Configuration

Use the *IGMP Snoop Config* tab to view and configure IGMP Snoop Configuration).

To view and configure IGMP Snoop details:

- 1 Select *Network > IGMP Snooping* from the main menu tree.
- 2 Select the *IGMP Snoop Config* tab.

SUMMIT® WM3600 CONTROLLER

Network > IGMP Snooping

IGMP Snoop Config | Igmpp Snoop Querier Config

igmp Snoop Config

Snoop Enable Unknown Multicast Forward

Apply Revert

igmp Snoop Config

Show Filtering Options

Vlan Index	Snoop Enable	Unknown Multicast Forward	Learning Mode	Multicast Router Ports
1	✓	✗	pimDvmrp(1)	up1
2	✓	✗	pimDvmrp(1)	No port Discovered Yet
3	✓	✗	pimDvmrp(1)	No port Discovered Yet
4	✓	✗	pimDvmrp(1)	No port Discovered Yet
5	✓	✗	pimDvmrp(1)	No port Discovered Yet
6	✓	✗	pimDvmrp(1)	No port Discovered Yet
7	✓	✗	pimDvmrp(1)	No port Discovered Yet
8	✓	✗	pimDvmrp(1)	No port Discovered Yet
9	✓	✗	pimDvmrp(1)	No port Discovered Yet
10	✓	✗	pimDvmrp(1)	No port Discovered Yet
11	✓	✗	pimDvmrp(1)	No port Discovered Yet
12	✓	✗	pimDvmrp(1)	No port Discovered Yet
13	✓	✗	pimDvmrp(1)	No port Discovered Yet
14	✓	✗	pimDvmrp(1)	No port Discovered Yet
15	✓	✗	pimDvmrp(1)	No port Discovered Yet
16	✓	✗	pimDvmrp(1)	No port Discovered Yet
17	✓	✗	pimDvmrp(1)	No port Discovered Yet
18	✓	✗	pimDvmrp(1)	No port Discovered Yet

Filtering is disabled

Edit Help

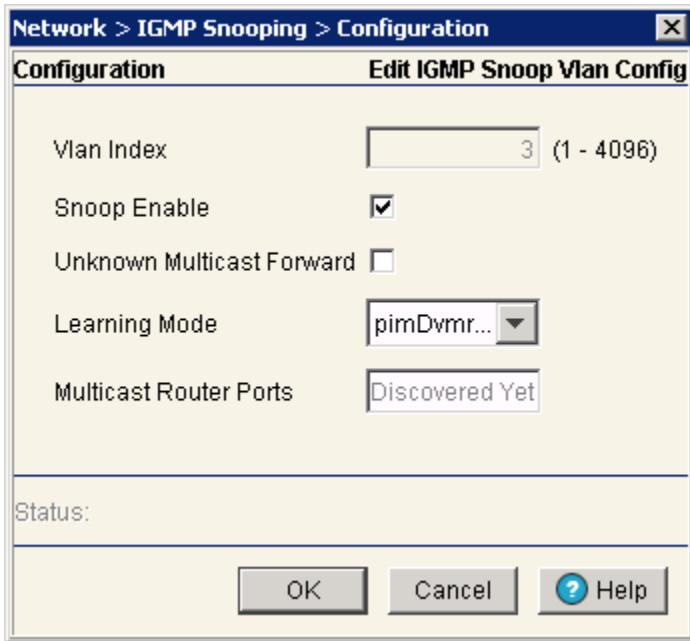
Save Logout Refresh

The *IGMP Snoop Config* tab displays the following information:

Snoop Enable	Select to enable IGMP Snooping on the controller. If disabled, snooping on a per VLAN basis is also disabled.
Unknown Multicast Forward	Select to enable the controller to forward Multicast packets from unregistered Multicast Groups. If disabled, Unknown Multicast Forward on a per VLAN basis is also disabled.
Apply	Click to Apply changes made to the running configuration.
Revert	Revert back to previous state from the running configuration.
Vlan Index	The VLAN index on which IGMP Snooping is enabled.
Snoop Enable	The status of IGMP Snooping. Disabled for the selected VLAN if the screen displays a red cross mark.

Unknown Multicast Forward	The status of forwarding IGMP Multicast packets from unregistered Multicast Groups. Disabled for selected VLAN if the screen displays a red cross mark.
Learning Mode	Indicates how the controller learns IGMP Snooping information. Can be one of pimDvmrp or static.
Multicast Router Ports	Lists the ports used for Multicast Routing. Can be one of the available ge ports.

- Optionally, select a VLAN Index from among those listed, and select *Edit* to revise the Snoop Enable, Unknown Multicast Forward, Learning Mode and Multicast Router Ports.



- Select *OK* to save the edits to the IGMP configuration. Selecting *Cancel* reverts the IGMP snooping configuration to its previous settings.

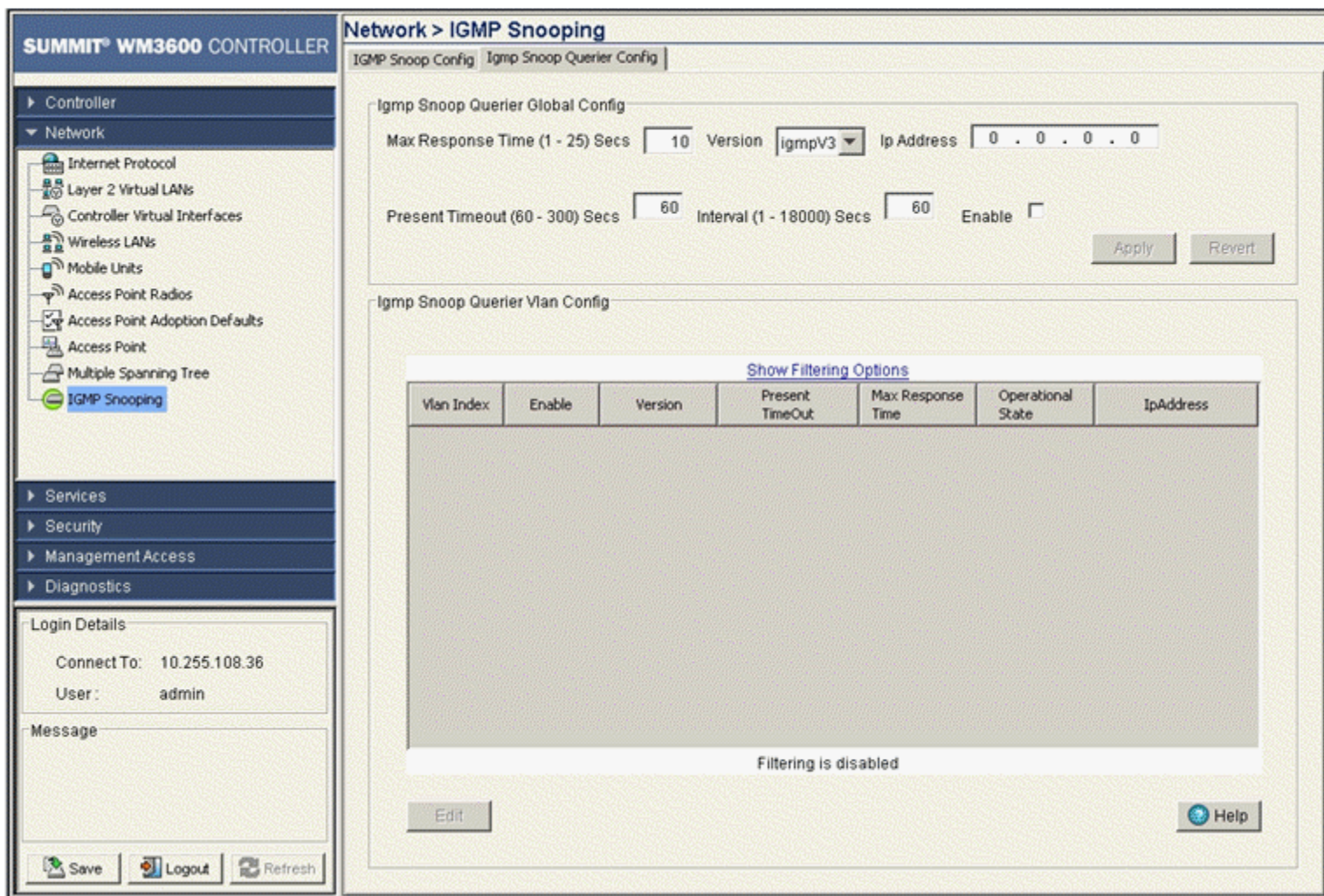
IGMP Snoop Querier Configuration

Use the *IGMP Snoop Querier Config* tab to view and configure IGMP Snoop Querier Configuration.

The IGMP Snoop Querier is used to keep host memberships alive. It is primarily used in a network where there is a Multicast Streaming Server and hosts that subscribe to the Multicast server and there is no IGMP Querier present. The controller can perform the role of an IGMP Querier. An IGMP Querier sends out periodic IGMP Query packets. Interested hosts reply with IGMP Report packet. IGMP Snooping is only done on wireless portals. IGMP Multicast packets are flooded on wired ports.

To view and configure IGMP Snoop Querier Configuration details:

- 1 Select *Network > IGMP Snooping* from the main menu tree.
- 2 Select the *IGMP Snoop Querier Config* tab



The *IGMP Snoop Querier Config* tab displays the following information:

Max Response Time	Specifies the maximum allowed time before sending a responding report. When no reports are received from a portal, that portal information is removed from the Snooping Table. The controller will only forward Multicast Packets to portals that are present in the Snooping Table. For IGMP reports from wired ports, the controller forwards these reports to the Multicast Router Ports.
Version	Sets the IGMP version compatibility. Select from IGMP v1, v2, or v3.
IP Address	This address is applied as the source address in the IGMP Query packet. This value is used as the default VLAN Querier IP address.

Present Timeout	This is the time duration after which the controller's IGMP Querier is activated. A Querier is used to accommodate any query loss due to a Multicast Router being down or not accessible. It is also used to accommodate any local network query loss. The Querier generates IGMP queries on receipt of which the interested hosts reply with an IGMP report. On receipt of an IGMP report, the Snooping Table on the controller is updated with the host's portal information. Any IGMP packet from the Multicast Server is then forwarded to the particular portal.
Interval	This is the common interval in seconds between two IGMP Queries generated by the IGMP Querier. This is valid for all VLANs.
VLAN Index	The index of the selected VLAN.
Enable	The enable state of IGMP Snoop Querier on this VLAN.
Version	The IGMP version in use.
Present Timeout	The time duration in seconds after which the controller's querier takes over the role of IGMP querier for this VLAN.
Max Response Time	The maximum time allowed in seconds before sending a responding report for a host.
Operational State	The current operational state of IGMP Querier for this VLAN. Displays 'querier' if IGMP Snoop Querier is enabled on this VLAN. Displays 'disabled' otherwise.
IP Address	The IP address to be inserted in IGMP Query packets generated by the IGMP Querier for this VLAN.

Wired Hotspot

Hotspot functionality allows service providers or shop owners to provide Internet access to guest users. Hotspots are often found at restaurants, train stations, airports, libraries, coffee shops, book stores, fuel stations, and other public places. Users will not have Internet access until they are authenticated. When a user tries to access a web page through a browser, the request is redirected to a login page where the user has to enter a valid login name and password. Upon successful authentication, the user is provided with full Internet access until the session expires. Wired hotspots can be used where wireless connections are not used or not feasible.



NOTE

The L2 firewall should be enabled for the Wired Hotspot feature to work. The L3 entity table, which is used to get the MAC address is updated when the L2 firewall is updated.



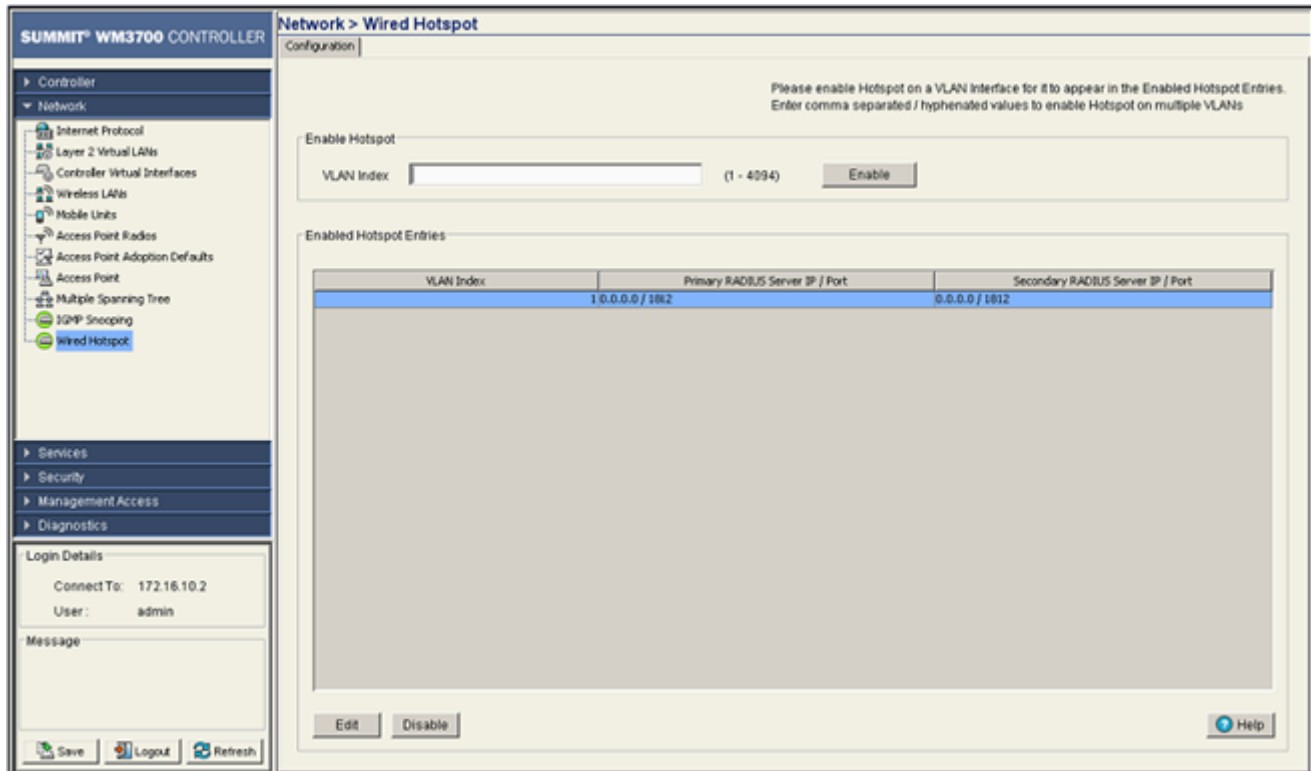
NOTE

At any point of time hotspot can be enabled on 32 VLANs only.

Wired Hotspot Configuration

Use the *Network > Wired Hotspot* screen to configure the wired hotspot. To configure the wired hotspot:

- 1 Select *Network > Wired Hotspot* from the main menu tree.
- 2 Select the *Configuration* tab.



The *Configuration* tab displays the following information:

VLAN Index	Enter a VLAN index between 1 and 4094.
Enable	Click the <i>Enable</i> button to enable a hotspot.
VLAN Index	The VLAN index on which the hotspot is enabled.
Primary RADIUS Server IP/Port	This is the IP address of the Primary RADIUS server and the port on which the Primary RADIUS server is listening.
Secondary RADIUS Server IP/Port	This is the IP address of the Secondary RADIUS server and the port on which the Secondary RADIUS Server is listening.
Edit	Click the <i>Edit</i> button to configure the internal and the external hotspots as well as to configure the RADIUS Server.
Delete	Click the <i>Delete</i> button to delete an enabled hotspot entry.

Configuring an Internal Hotspot

Using the *Internal* option means the user develops the hotspot using the internal Web server. The HTML pages are pre-created to collect login credentials through *Login.htm*, to send them to a RADIUS server, and display a *Welcome.htm* or a *Failure.htm* depending on the result of the authentication attempt.



NOTE

When using an internal hotspot, ensure that traffic can pass on TCP port 444 between the controller's internal Web server and the hotspot clients.

To create a hotspot maintained by the controller's own internal resources:

- 1 Select *Network > Wired Hotspot* from the main menu tree. Select an existing hotspot entry from those displayed within the *Configuration* tab and click the *Edit* button. The following screen is displayed.

- 2 Click the *Login* tab and enter the title, header, footer, Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when users log in to the controller-maintained hotspot.

Header Text	Displays the HTML header displayed on the Login page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Footer Text	Displays the HTML footer text displayed on the Login page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Small Logo URL	Displays the URL for a small logo image displayed on the Login page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu.
Main Logo URL	Displays the URL for the main logo image displayed on the Login page when using the controller's internal Web server. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.

Descriptive Text Specify any additional text containing instructions or information for the users who access the Login page. This option is only available if *Internal* is chosen from the drop-down menu above. The default text is: "Please enter your username and password."

- 3 Click the *Welcome* tab and enter the title, header, footer, Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when users successfully authenticate with the controller-maintained hotspot.

Title Text The Title Text specifies the HTML title text displayed on the Welcome page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Header Text The Header Text is the HTML header text displayed on the Welcome page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Footer Text The Footer Text is the HTML footer text displayed on the Welcome page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Small Logo URL The Small Logo URL is the URL for a small logo image displayed on the Welcome page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Main Logo URL The Main Logo URL is the URL for the main logo image displayed on the Welcome page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Descriptive Text Specify any additional text containing instructions or information for the users who access the Welcome page on the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above. The default text is: "You now have network access. Click the disconnect link below when you want to end this session."

- 4 Click the *Failed* tab and enter the title, header, footer, Small Logo URL, Main Logo URL, and Descriptive Text you would like to display when users fail authentication with the controller-maintained hotspot.

Title Text The Title Text is the HTML title displayed on the Failed page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Header Text The Header Text specifies the HTML header displayed on the Failed page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Footer Text The Footer Text is the HTML footer text displayed on the Failed page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Small Logo URL The Small Logo URL is the URL for a small logo image displayed on the Failed page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Main Logo URL The Main Logo URL is the URL for the main logo image displayed on the Failed page when using the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above.

Descriptive Text Specify any additional text containing instructions or information for the users who access the Failed page on the internal Web server. This option is only available if *Internal* is chosen from the drop-down menu above. The default text is: "Either the username and password are invalid, or service is unavailable at this time."

- 5 Click the *Terms* tab to set the terms and conditions for display to the user.

Title Text	Specifies the title displayed on the Terms and Conditions screen. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Header Text	Specifies the header text displayed on the Terms and Conditions screen. This option is only available if <i>Internal</i> is chosen from the drop-down menu above.
Descriptive Text	Displays the terms and conditions.

- 6 Click the *Restore Defaults* button to revert to the default settings in the Internal (Generated) Web Page.
- 7 Refer to the *Allow List* field, and enter any IP address (for internal or external websites) that may be accessed by the Hotspot user without authentication.



NOTE

In multi-controller hotspot environments if a single controller's internal pages are configured for authentication on the other controllers, those controllers will redirect to their own internal pages instead. In these environments it is recommended to use an external server for all of the controllers.

- 8 Check the *Use System Name in Hotspot URL* to use the *System Name* specified on the main Controller configuration screen as part of the hotspot address.
- 9 Check the *Logout on Browser Close* button to log out hotspot users from the network when they close their web browsers.
- 10 Specify the maximum *Hotspot Simultaneous Users* to set a limit on the number of concurrent unique hotspot users for the selected VLAN.
- 11 Use the *Accounting* drop-down menu to retrieve accounting information from the controller-managed network. You can select *None*, *Radius*, or *Syslog* from the menu for retrieving the accounting information.
- 12 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 13 Click *OK* to use the changes to the running configuration and close the dialog.
- 14 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring an External Hotspot

Selecting the *External* option entails hosting your own external Web server using advanced Web content (using XML, Flash). To create a hotspot maintained by an external server:

- 1 Select *Network > Wired Hotspot* from the main menu tree.
- 2 Select an existing hotspot entry from those displayed within the *Configuration* tab and click the *Edit* button. Ensure *External* is selected from within the *This VLAN's Web Pages are of the* drop-down menu.

- 3 Refer to the *External Web Pages* field and provide the Login, Welcome, and Failed Page URLs used by the external Web server to support the hotspot.

Login Page URL Define the complete URL for the location of the Login page. The Login screen will prompt the hotspot user for a username and password to access the Welcome page. For example, the Login page URL can be the following:

`http://192.168.150.5/login.html?ip_address=192.168.30.1`. Here, 192.168.150.5 is the Web server IP address and 192.168.30.1 is the controller IP address.

Welcome Page URL Define the complete URL for the location of the Welcome page. The Welcome page assumes that the hotspot user has logged in successfully and can access the Internet. For example, the Login page URL can be the following:

`http://192.168.150.5/welcome.html?ip_address=192.168.30.1`. Here, 192.168.150.5 is the Web server IP address and 192.168.30.1 is the controller IP address.

Failed Page URL Define the complete URL for the location of the Failed page. The Failed screen assumes that the hotspot authentication attempt has failed, you are not allowed to access the Internet and you need to provide correct login information to access the Web. For example, the Login page URL can be the following:

`http://192.168.150.5/fail.html?ip_address=192.168.30.1`. Here, 192.168.150.5 is the Web server IP address and 192.168.30.1 is the controller IP address.



NOTE

When using hotspot features in a cluster environment, additional steps must be taken when specifying the external URLs. In order for the browser to return the login information correctly, the IP address and port must be specified as part of the URL in the following format: `http://external_url<login | welcome | fail>.html?ip_address=a.b.c.d&port=x`

- 4 Refer to the *Allow List* field, and enter any IP address (for internal or external websites) that may be accessed by the Hotspot user without authentication.



NOTE

If the Web-server is located on a VLAN other than the one on which the MUs will be associated, specify the IP address for the VLAN on which the server is located within the Allow List.

- 5 Check the *Use System Name in Hotspot URL* to use the *System Name* specified on the main Controller configuration screen as part of the hotspot address.
- 6 Specify the maximum *Hotspot Simultaneous Users* to set a limit on the number of concurrent unique hotspot users for the selected VLAN.
- 7 Check the *Logout on Browser Close* button to logout hotspot users from the network when they close their web browsers.
- 8 Use the *Accounting* drop-down menu to retrieve accounting information from the controller-managed network. You can select *None*, *Radius*, or *Syslog* from the menu for retrieving the accounting information.
- 9 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to use the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring an Advanced Hotspot

A customer may wish to use advanced Web content (XML, Flash) but might not have (or would not want to use) an external Web server, choosing instead to host the Web pages on the controller's HTTP Web server. Selecting the *Advanced* option allows for importing the Web pages from an external source (like an FTP server) and hosting them on the controller.

To use the *Advanced* option to define the wired hotspot:

- 1 Select *Network > Wired Hotspot* from the main menu tree.
- 2 Select an existing hotspot entry from those displayed within the *Configuration* tab.

- 3 Click the *Edit* button. Ensure that *Advanced* is selected from the *This WLAN's Web Pages are of the* drop-down menu.

**NOTE**

Advanced hotspot configuration is not permissible using the controller Web UI. Refer to the controller CLI or other advanced configuration options to define a hotspot with advanced properties. However, the controller can still install and maintain directories containing Web page content.

- 4 Once the properties of the advanced hotspot have been defined, the file can be installed on the controller and used to support the hotspot. The following parameters are required to upload the file:
- Specify a source hotspot configuration file. The file used at startup automatically displays within the *File* parameter.
 - Refer to the *Using* drop-down menu to configure whether the hotspot file transfer is conducted using FTP or TFTP.
 - Enter the *IP Address* of the server or system receiving the source hotspot configuration. Ensure that the IP address is valid or risk jeopardizing the success of the file transfer.
 - Enter the *Port* on which the server is listening.
 - If using FTP, enter the *User ID* credentials required to transfer the configuration file from an FTP server.
 - If using FTP, enter the *Password* required to send the configuration file from an FTP server.
 - Specify the appropriate *Path* name to the hotspot configuration on the local system disk or server.
 - Once the location and settings for the advanced hotspot configuration have been defined, click the *Install* button to use the hotspot configuration with the controller.

- 5 Refer to the *Allow List* field, and enter any IP address (for internal or external websites) that may be accessed by the Hotspot user without authentication.
- 6 Check the *Use System Name in Hotspot URL* to use the *System Name* specified on the main Controller configuration screen as part of the hotspot address.
- 7 Specify the maximum *Hotspot Simultaneous Users* to set a limit on the number of concurrent unique hotspot users for the selected WLAN.
- 8 Check the *Logout on Browser Close* button to log out hotspot users from the network when they close their web browsers.
- 9 Use the *Accounting* drop-down menu to retrieve accounting information from the controller-managed network. You can select *None*, *Radius*, or *Syslog* from the menu for retrieving the accounting information.
- 10 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 11 Click *OK* to use the changes to the running configuration and close the dialog.
- 12 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring a RADIUS Server

- 1 Select *Network > Wired Hotspot > Edit > Radius Configuration*. The *Radius Configuration* screen opens up. The *Radius Configuration* screen contains tabs for defining the Radius server settings.

- 2 Refer to the *Radius* field and define the following credentials for a primary and secondary Radius server.

RADIUS Server Address	Enter the IP address of the primary and secondary servers acting as the Radius user authentication data source.
-----------------------	---

RADIUS Port	Enter the TCP/IP port number for the primary and secondary servers acting as the Radius user authentication data source. The default port is 1812.
RADIUS Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary Radius server.
Server Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the controller to time out on a request to the primary or secondary server.
Server Retries	Enter a value between 1 and 100 seconds to indicate the number of times the controller attempts to reach the primary or secondary Radius server before giving up.
Dynamic Authorization	Check this option to enable RADIUS Dynamic Authorization. RADIUS Dynamic Authorization enables the RADIUS administrator to send the disconnect and change of authorization packets to the controller (NAS) for wired hosts.

**NOTE**

The Radius server's Timeout and Retries should be less than what is defined for an MU's timeout and retries. If the MU's time is less than the server's, a fall back to the secondary server will not work.

3 Refer to the *Accounting* field and define the following credentials for a primary and secondary Radius servers.

Accounting Server Address	Enter the IP address of the primary and secondary server acting as the Radius accounting server.
Accounting Port	Enter the TCP/IP port number for the primary and secondary server acting as the Radius accounting data source. The default port is 1813.
Accounting Shared Secret	Provide a shared secret (password) for user credential authentication with the primary or secondary Radius accounting server.
Accounting Timeout	Enter a value (between 1 and 300 seconds) to indicate the number of elapsed seconds causing the controller to time out a request to the primary or secondary accounting server.
Accounting Retries	Enter a value between 1 and 100 to indicate the number of times the controller attempts to reach the primary or secondary Radius accounting server before giving up.
Accounting Mode	Use the Accounting Mode drop-down menu to define the accounting mode as either <i>Start-Stop</i> , <i>Stop Only</i> , or <i>Start-Interim-Stop</i> . Define the interval (in seconds) used with the selected accounting mode.

4 Refer to the *Advanced* field to define the authentication protocol used with the Radius Server.

PAP	PAP— <i>Password Authentication Protocol</i> sends a username and password over a network to a server that compares the username and password to a table of authorized users. If the username and password are matched in the table, server access is authorized.
CHAP	CHAP is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
DSCP/TOS	Optionally mark packets with a <i>DiffServ CodePoint</i> (DSCP) in its header. The DSCP value is stored in the first 6 bits of the Type of Service (ToS) field that is part of the standard IP header. The DCSP values are associated with a forwarding treatment called <i>Per Hop Behaviors</i> (PHB). Service can be provisioned (if necessary) by assigning a DCSP point code from 1–6.

-
- 5 Click *OK* to save the changes made to this screen.
 - 6 Click *Cancel* to revert back to the last saved configuration and move back to the *Network > Wired Hotspot > Edit* screen.

6

CHAPTER

Controller Services

This chapter describes the Services main menu information available for the following controller configuration activities:

- [Displaying the Services Interface on page 309](#)
- [DHCP Server Settings on page 311](#)
- [Configuring Secure NTP on page 333](#)
- [Configuring Controller Redundancy and Clustering on page 345](#)
- [Layer 3 Mobility on page 359](#)
- [Configuring Self Healing on page 366](#)
- [Configuring Controller Discovery on page 370](#)
- [Locationing on page 376](#)

Displaying the Services Interface

Refer to the *Services* main menu interface to review a summary describing the availability of several central features within the Services main menu item.

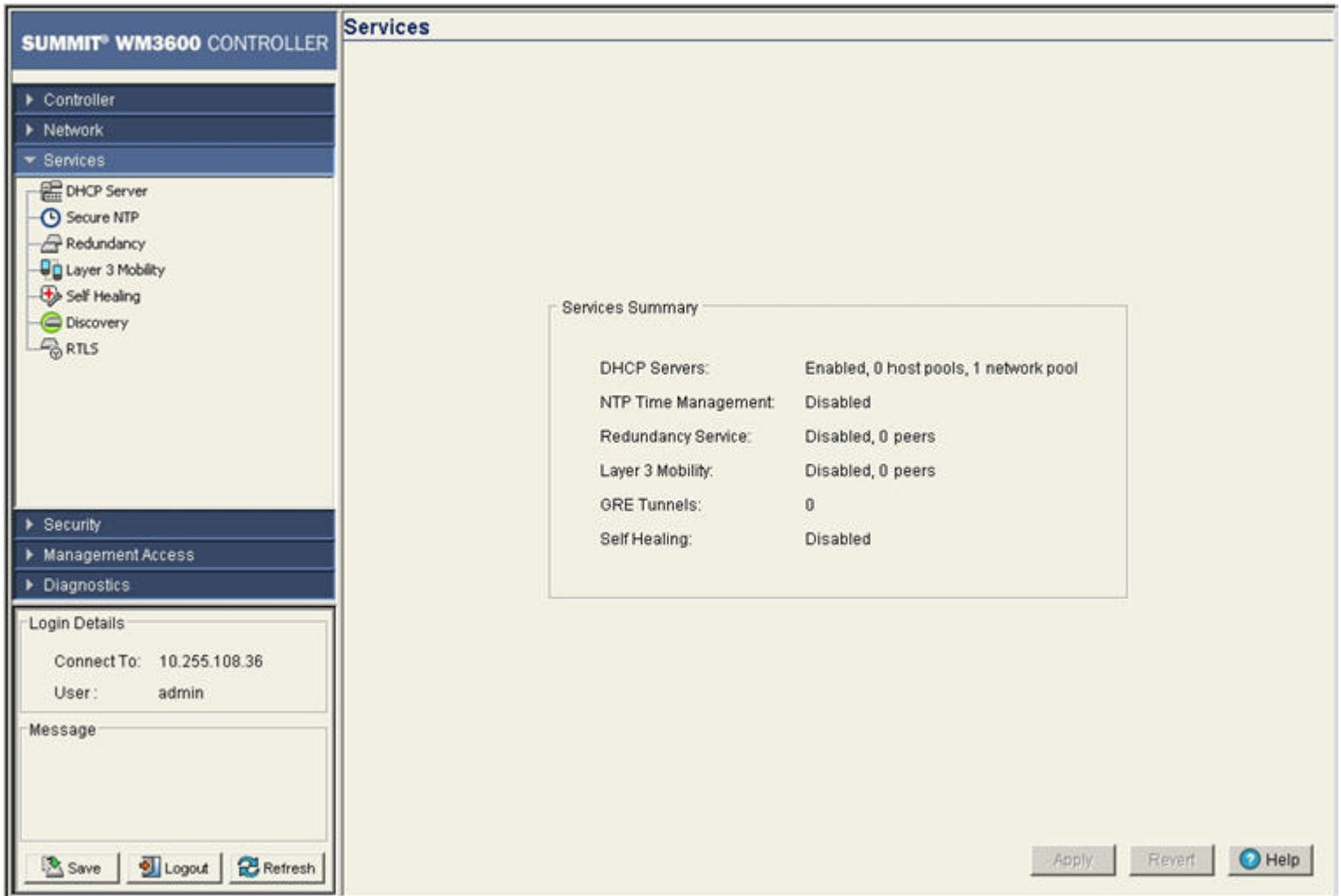


NOTE

When the controller's configuration is successfully updated (using the Web UI), the affected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the affected screen's Status field. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To display a *Services Summary*:

- 1 Select *Services* from the main menu tree.



- 2 Refer to the *Services Summary* field for the following information relating to configurable values within the Services main menu item.

DHCP Servers	Displays whether DHCP is enabled and the current configuration. For information on configuring DHCP Server support, see “DHCP Server Settings” on page 311.
NTP Time Management	Displays whether time management is currently enabled or disabled. <i>Network Time Protocol</i> (NTP) manages time and/or network clock synchronization within the controller managed network. NTP is a client/server implementation.
Redundancy Service	Displays whether Redundancy is currently enabled or disabled. One or more controllers can be configured as members of a redundancy group to significantly reduce the chance of a disruption in service to WLANs and associated MUs in the event of failure of a controller or intermediate network failure. For more information, see “Configuring Controller Redundancy and Clustering” on page 345.

Layer 3 Mobility	Displays whether Layer 3 Mobility is currently enabled or disabled. Layer 3 mobility is a mechanism which enables an MU to maintain the same Layer 3 address while roaming throughout a multi-VLAN network. This enables the transparent routing of IP datagrams to MUs during their movement, so data sessions can be initiated while they roam (in for voice applications in particular). Layer 3 mobility enables TCP/UDP sessions to be maintained in spite of roaming among different IP subnets. For more information on configuring Layer 3 Mobility, see “Layer 3 Mobility” on page 359 .
GRE Tunnels	Displays the number of GRE tunnels currently configured on the controller. Tunneling involves encapsulating a packet that supports one protocol within another packet, which may run on the same protocol or on a different protocol. It is generally used to support evolving networks for security requirements. Generic Routing Encapsulation (GRE) is one of the many commonly used protocols for IP tunneling.
Self Healing	Displays whether Self Healing is currently enabled. Self healing enables radios to take action when one or more radios fail. To enable the feature, the user must specify radio neighbors that would self heal if a neighbor goes down. The neighbor radios do not have to be of the same type. An 11bg radio can be the neighbor of an 11a radio and either of them can self heal when one fails. For information on configuring self healing, see “Configuring Self Healing” on page 366 .

DHCP Server Settings

The DHCP Server Settings section contains the following activities:

- [Configuring the Controller DHCP Server on page 311](#)
- [Viewing the Attributes of Existing Host Pools on page 318](#)
- [Configuring Excluded IP Address Information on page 320](#)
- [Configuring the DHCP Server Relay on page 321](#)
- [Viewing DDNS Bindings on page 324](#)
- [Viewing DHCP Bindings on page 325](#)
- [Reviewing DHCP Dynamic Bindings on page 326](#)
- [Configuring the DHCP User Class on page 328](#)
- [Configuring DHCP Pool Class on page 331](#)

Configuring the Controller DHCP Server

The controller contains an internal *Dynamic Host Configuration Protocol* (DHCP) Server. DHCP can provide the dynamic assignment of IP addresses automatically. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask and gateway.

When a DHCP server allocates an address for a client, the client is assigned a lease (which expires after an interval defined by the administrator). Before the lease expires, clients are expected to renew the lease to continue to use the addresses assigned. Once a lease has expired, the client to which that lease was assigned is no longer permitted to use the leased IP address.



NOTE

DHCP Server setting updates are only implemented when the controller is restarted.



NOTE

When using the controller's internal DHCP server ensure that traffic can pass on UDP ports 67 & 68 between the controller and clients receiving DHCP information.

To configure DHCP:

- 1 Select *Services > DHCP Server* from the main menu tree.

SUMMIT® WM3600 CONTROLLER

Services > DHCP Server

Configuration | Host Pool | Excluded | Relay | DDNS Bindings | Bindings | Dynamic Bindings | User Class | Pool Class

Enable DHCP Server

Ignore BOOTP

Ping timeout: (1 - 10 seconds)

Apply Revert

Network Pool

Pool Name	Network	Lease Time(dd:hh:mm)	Domain
WLab	10.255.108.0/24	1:0:0	

Edit Delete Add Options DDNS Options Setup Help

Save Logout Refresh

Login Details
Connect To: 10.255.108.36
User: admin

Message

- 2 Select the *Enable DHCP Server* checkbox to enable the controller's internal DHCP Server for use with global pools.
- 3 Select the *Ignore BOOTP* checkbox to bypass a BOOTP request.
- 4 Define an interval (from 1 -10 seconds) for the *Ping timeout* variable. The controller uses the timeout to intermittently ping and discover whether the client requested IP address is already used.

5 Refer to the following as displayed within *Network Pool* field.

Pool Name	Displays the name of the IP pool from which IP addresses can be issued to DHCP client requests on the current interface. The pool is the range of IP addresses available.
Network	Displays the network address for the clients.
Lease Time (dd:hh:mm)	When a DHCP server allocates an address for a DHCP client, the client is assigned a lease (which expires after a designated interval defined by the administrator). The lease time is the time an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. This is useful, for example, in education and customer environments where MU users change frequently. Use longer leases if there are fewer users.
Domain	Displays the domain name for the current interface.

- 6 Click the *Edit* button to modify the properties displayed on an existing DHCP pool. For more information, see [“Editing the Properties of an Existing DHCP Pool” on page 313](#).
- 7 To delete an existing DHCP pool from the list of those available, highlight the pool from within the Network Pool field and click the *Delete* button.
- 8 Click the *Add* button to create a new DHCP pool. For more information, see [“Adding a New DHCP Pool” on page 314](#).
- 9 Click the *Options* button to associate values to options, as defined using the Options Setup functionality. The values associated to options are local to the pool with which they are associated. For more information, see [“Configuring DHCP Global Options” on page 317](#).
- 10 Click the *DDNS* button to configure a DDNS domain and server address used with the list of available pools. For more information, see [“Configuring DHCP Server DDNS Values” on page 317](#).
- 11 Click the *Options Setup* button to define the option name, code and type. Associate values to them (by clicking the Options button) only after the options are defined.
- 12 Click *Apply* to save changes to the screen. Navigating away from the screen without clicking Apply results in all changes to the screen being lost.
- 13 Click the *Revert* button to display the last saved configuration. Unapplied changes are not saved and must be re-entered.

Editing the Properties of an Existing DHCP Pool

The properties of an existing pool can be modified to suit the changing needs of your network.

To modify the properties of an existing pool:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select an existing pool from those displayed (within the Network Pool field) and click the *Edit* button.
- 3 Modify the name of the IP pool from which IP addresses can be issued to client requests on this interface.
- 4 Modify the *Domain* name as appropriate for the interface using the pool.
- 5 Modify the *NetBios Node* used with this particular pool. The NetBios Node could have one of the following types:

- A *b-broadcast* (broadcast node) broadcasts to query network nodes for the owner of a NetBIOS name.
 - A *p-peer* (peer-to-peer node) uses directed calls to communicate with a known NetBIOS name server, such as a *Windows Internet Name Service* (WINS) server, for the IP address of a NetBIOS machine.
 - A *m-mixed* is a mixed node that uses broadcasted queries to find a node and queries a known p-node name server for the address.
 - A *h-hybrid* is a combination of two or all of the nodes mentioned above.
- 6 Change the name of the boot file used for this pool within the *Boot File* parameter.
 - 7 From the *Network* field, use the *Associated Interface* drop-down menu to modify (if necessary) the controller interface used for the newly created DHCP configuration. Use VLAN1 as a default interface if no others have been defined.
 - 8 Additionally, define the *IP Address* and *Subnet Mask* used for DHCP discovery and requests between the DHCP Server and DHCP clients.

**NOTE**

The network IP address and subnet mask of the pool are required to match the addresses of the Layer 3 interface for addresses to be supported on that interface.

- 9 Within the *Lease Time* field, define one of the two kinds of leases the DHCP Server assigns to its clients:
 - *Infinite*—If selected, the client can use the assigned address indefinitely.
 - *Actual Interval*—Select this checkbox to manually define the interval for clients to use the DHCP server assigned addresses. The default lease time is 1 day, with a minimum setting of 1 minute.
- 10 Within the *Servers* field, change the server type used with the pool and use the *Insert* and *Remove* buttons to add and remove the IP addresses of the routers used.
- 11 Modify the *Included Ranges* (starting and ending IP addresses) for this particular pool.
Use the *Insert* and *Remove* buttons as required to define the range of supported IP addresses.
A network pool without any include range is as good as not having a pool, because it won't be useful in assigning addresses.
- 12 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 13 Refer to the *Status* field.
The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 14 Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding a New DHCP Pool

Add a new DHCP pool as needed to suit the address distribution requirements of your network.

To add a DHCP pool:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Click the *Add* button at the bottom of the screen.

Services > DHCP Server > Configuration Add Pool

Pool Name Domain

NetBios Node Boot File

Network

Associated Interface

IP Address Subnet Mask

Lease Time(dd:hh:mm)

Infinite

01:00:00

Servers

Default Routers

DNS Servers

NetBios(WINS) Servers

Bootp Next Server

Default Routers

Insert

Remove

Included Ranges

Start IP	End IP

Insert

Remove

Status:

OK Cancel ? Help

- 3 Enter the name of the IP pool from which IP addresses can be issued to client requests on this interface.
- 4 Provide the *Domain* name as appropriate for the interface using the pool.

- 5 Enter the *NetBios Node* used with this particular pool. The NetBios Node could have one of the following types:
 - A *b-broadcast* (broadcast node) uses broadcasting to query nodes on the network for the owner of a NetBIOS name.
 - A *p-peer* (peer-to-peer node) uses directed calls to communicate with a known NetBIOS name server, such as a *Windows Internet Name Service* (WINS) server, for the IP address of a NetBIOS machine.
 - An *m-mixed* is a mixed node that uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address.
 - An *h-hybrid* is a combination of two or all of the nodes mentioned above.
- 6 Enter the name of the boot file used for this pool within the *Boot File* parameter.
- 7 From the *Network* field, use the *Associated Interface* drop-down menu to define the controller interface is used for the newly created DHCP configuration. Use VLAN1 as a default interface if no others have been defined.

Additionally, define the *IP Address* and *Subnet Mask* used for DHCP discovery and requests between the DHCP Server and DHCP clients.

**NOTE**

The IP address and subnet mask of the pool are required to match the addresses of the Layer 3 interface in order for the addresses to be supported through that interface.

- 8 Within the *Lease Time* field, define one of the two kinds of leases the DHCP Server assigns to its clients:
 - *Infinite*—If selected, the client can use the assigned address indefinitely.
 - *Actual Interval*—Select this checkbox to manually define the interval for clients to use DHCP supplied addresses. The default lease time is 1 day, with a minimum setting of 60 seconds and a maximum value of 946080000 seconds.
- 9 Within the *Servers* field, change the server type used with the pool and use the *Insert* and *Remove* buttons to add and remove the IP addresses of the routers used.
- 10 Provide the *Included Ranges* (starting and ending IP addresses) for this particular pool.

Use the *Insert* and *Remove* buttons as required to define the range of supported IP addresses.

A network pool without any include range is as good as not having a pool, because it won't be useful in assigning addresses.
- 11 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 12 Refer to the *Status* field.

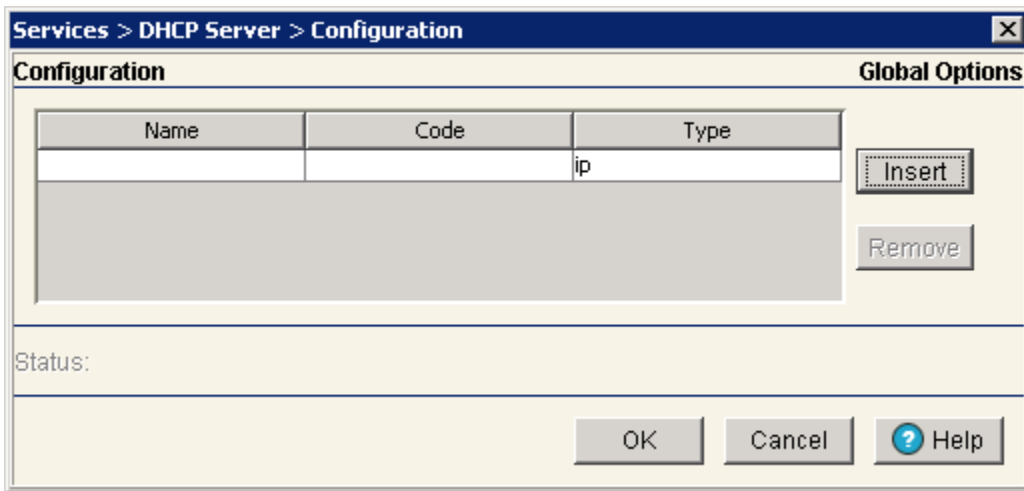
The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 13 Click *Cancel* to close the dialog without committing updates to the running configuration

Configuring DHCP Global Options

The DHCP Server screen's Configuration and Host Pool tabs can be used to display an additional *Global Options* screen.

To define new global name and value and send it to other peer controllers in the mobility domain:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Highlight an existing pool name from within either the Configuration or Host Pool tab and click the *Options Setup* button at the bottom of the screen.



- 3 Click the *Insert* button to display an editable field wherein the name and value of the DHCP option can be added.
- 4 *Name* the option as appropriate, assign a *Code* (numerical identifier) and use the *Type* drop-down options to specify a value of *ip* or *ascii* to the DHCP global option. Highlight an entry from within the Global Options screen and click the *Remove* button to delete the name and value.
- 5 Click *OK* to save and add the changes to the running configuration and forward the updates to the other peer controllers comprising the mobility domain.
- 6 Refer to the *Status* field.
The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration

Configuring DHCP Server DDNS Values

The DHCP Server screen's Configuration tab can be used to display an additional *DDNS* screen. Use this screen to define a DDNS domain name and address for use with the controller.

To configure a global domain name and DDNS server address:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Highlight an existing pool name from within either the Configuration or Host Pool tabs and click the *DDNS* button at the bottom of the screen.

- 3 Enter a *Domain Name* which represents the forward zone in the DNS server. For example *test.net*.
- 4 Define the *TTL* (Time to Live) to specify the validity of DDNS records. The maximum value is 864000 seconds.
- 5 Use the *Automatic Update* drop-down menu to specify whether the automatic update feature is on or off. Select *Server update* to enable a DDNS update from the DHCP server. Select *Client update* to get the DDNS updates from DHCP clients.
- 6 Select the *Enable Multiple User Class* checkbox if multiple user class support is needed.
- 7 Use the *DDNS Servers* field to define the IP addresses of the DNS servers.
- 8 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 9 Refer to the *Status* field.

The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.

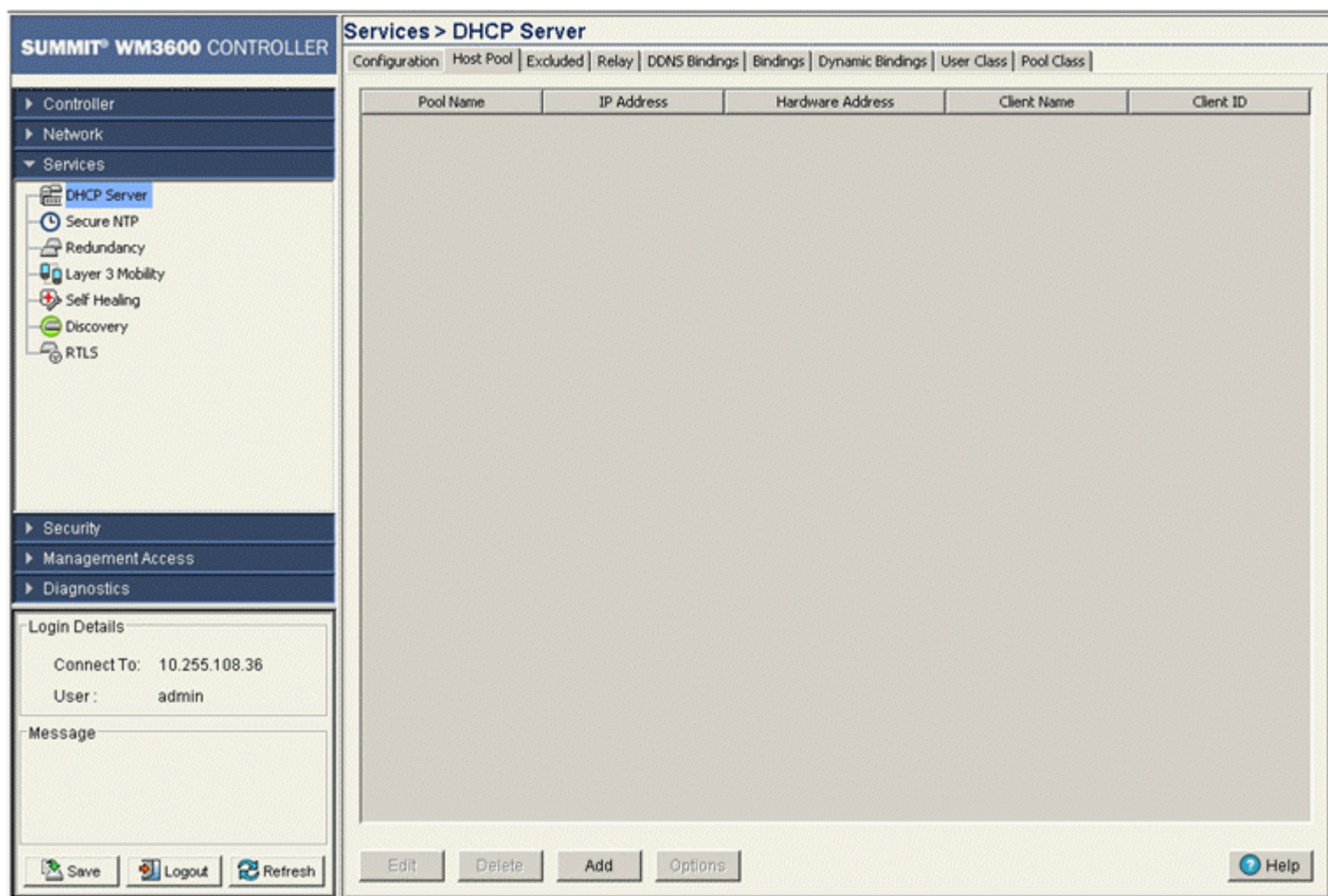
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing the Attributes of Existing Host Pools

Refer to the *Host Pool* tab within the DHCP Server screen to view how the host pools reserve IP addresses for specific MAC addresses. This information can be an asset in determining if a new pool needs to be created or an existing pool requires modification.

To view the attributes of existing host pools:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *Host Pool* tab.



- 3 Refer to the following information to assess whether the existing group of DHCP pools is sufficient:

Pool Name	Displays the name of the IP pool from which IP addresses can be issued to DHCP client requests on this interface. The pool is the range of IP addresses for which addresses can be assigned.
IP Address	Displays the IP address for the client on this interface using the pool name listed.
Hardware Address	Displays the type of interface used to pass DHCP discover and request exchanges between the controller DHCP server and DHCP Clients. The Hardware Address field also displays the address of the DHCP client for whom the static IP is reserved.
Client Name	Displays the name of the client requesting DHCP Server support over this interface. This name is read only cannot be modified using the host pool edit option.
Client ID	Displays the client Identifier. Based on this identifier static IP is assigned. Hardware address and client identifier should not be configured on a same host pool. A pool name cannot have both a client identifier and MAC address.

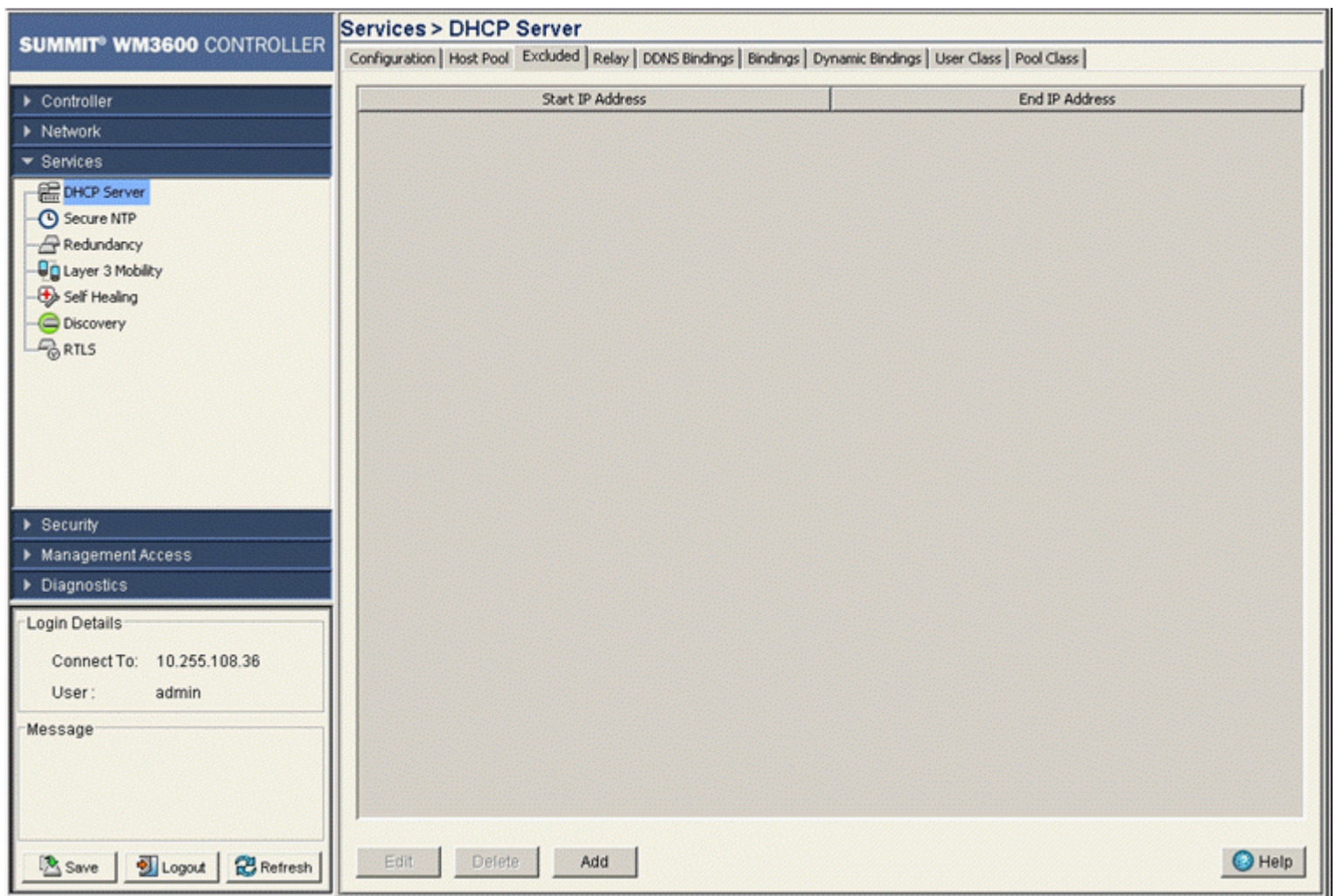
- 4 Click the *Edit* button to modify the properties displayed on an existing DHCP pool. For more information, see [“Editing the Properties of an Existing DHCP Pool” on page 313](#).
- 5 To delete an existing DHCP pool from the list of those available, highlight the pool from within the Pool Name field and click the *Delete* button.
- 6 Click the *Add* button to create a new DHCP pool. For more information, see [“Adding a New DHCP Pool” on page 314](#).
- 7 Click the *Options* button to insert a global pool name into the list of available pools. For more information, see [“Configuring DHCP Global Options” on page 317](#).
- 8 Click the *DDNS* button to configure a DDNS domain and server address that can be used with the list of available pools. For more information, see [“Configuring DHCP Server DDNS Values” on page 317](#).

Configuring Excluded IP Address Information

The DHCP Server may have some IP addresses unavailable when assigning IP address ranges for a pool. If IP addresses have been manually assigned and fixed, they need to be made available for the administrator to exclude from possible selection.

To view excluded IP address ranges:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Click the *Excluded* tab.



The Excluded tab displays “fixed” IP addresses statically assigned and unavailable for assignment with a pool.

- 3 Click the *Edit* button to modify the IP address range displayed. For more information, see [“Editing the Properties of an Existing DHCP Pool” on page 313](#).
- 4 To delete an existing DHCP pool from the list of those available to the controller, highlight the pool from within the Network Pool field and click the *Delete* button.
- 5 Click the *Add* button to create a new IP address range for a target host pool. For more information, see [“Adding a New DHCP Pool” on page 314](#).

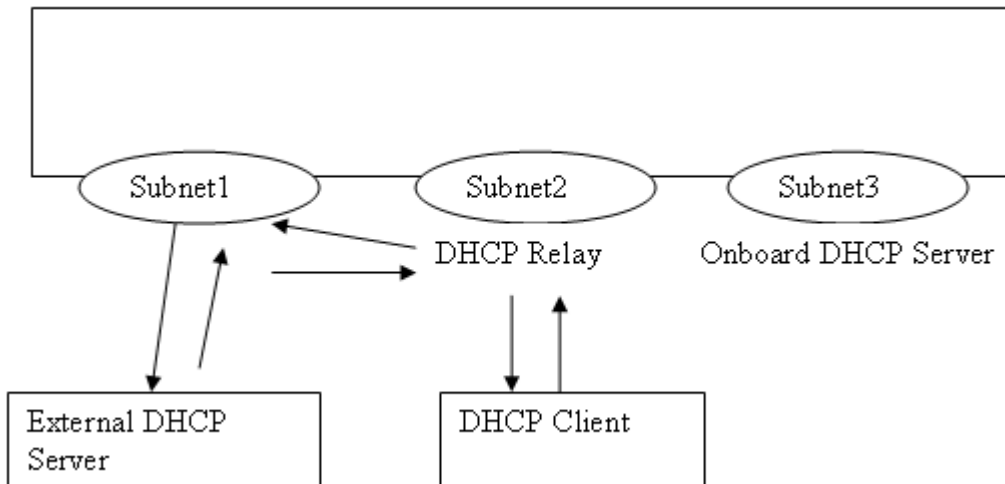
Configuring the DHCP Server Relay

Refer to the *Relay* tab to view the current DHCP Relay configurations for available controller VLAN interfaces. The Relay tab also displays the VLAN interfaces for which the DHCP Relay is enabled/configured. The Gateway Interface address information is helpful in selecting the interface suiting the

data routing requirements between the External DHCP Server and DHCP client (present on one of the controller's available VLANs).

**NOTE**

DHCP Server and relay can run on different controller VLAN interfaces.

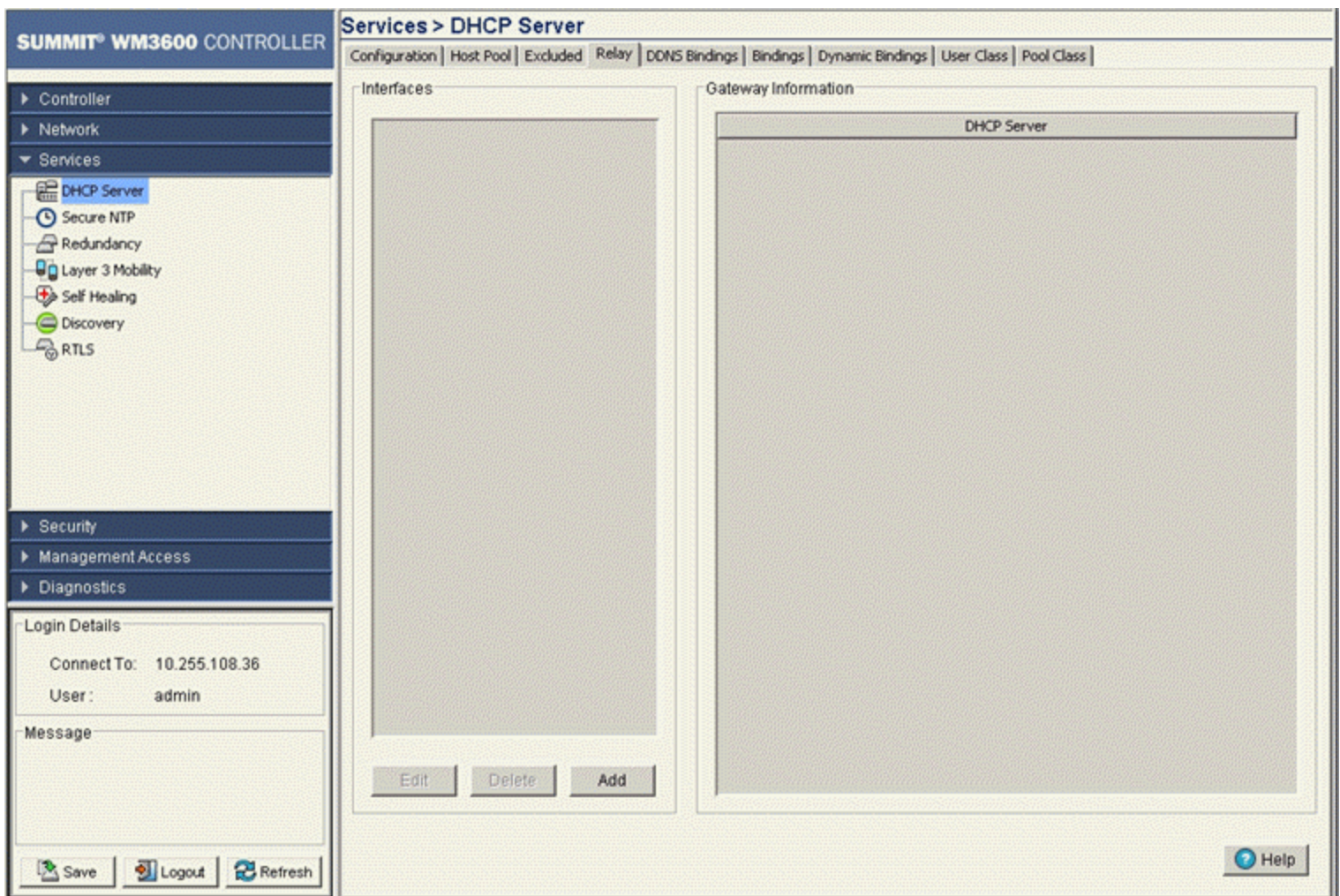


In the illustration above, a DHCP relay address has been configured on subnet 2. The CLI equivalent is "ip helper-address <subnet1 External DHCP Server IP > <subnet1 Interface Name>". When configuring a DHCP Relay address, specify the other interface where the external DHCP Server can be reached. In this example, that interface is subnet1. The DHCP relay agent must listen on both subnet1 and subnet2. Consequently, the DHCP Server cannot run on either subnet1 or subnet2 (it must be both).

However, you can run an onboard DHCP server on subnet3 to provide DHCP requests for clients in subnet3. This is independent of the DHCP relay configuration. You cannot run onboard DHCP Server on subnet1 to provide IP addresses to DHCP clients requesting IP addresses using DHCP relay.

To view and configure DHCP relay information:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Click the *Relay* tab.



- 3 Refer to the *Interfaces* field for the names of the interfaces available to route information between the DHCP Server and DHCP clients. If this information is insufficient, consider creating a new IP pool or edit an existing pool.
- 4 Click the *Edit* button to modify the properties displayed on an existing DHCP pool. Refer to step 7 for the information that can be modified for the DHCP relay.
- 5 To delete an existing DHCP pool from the list of those available to the controller, highlight the pool from within the Network Pool field and click the *Delete* button.



NOTE

The interface VLAN and gateway interface should have their IP addresses set. The interface VLAN and gateway interface should not have DHCP client or DHCP Server enabled. DHCP packets cannot be relayed to an onboard DHCP Server. The interface VLAN and gateway interface cannot be the same.

- 6 Click the *Add* button to create a new DHCP pool.

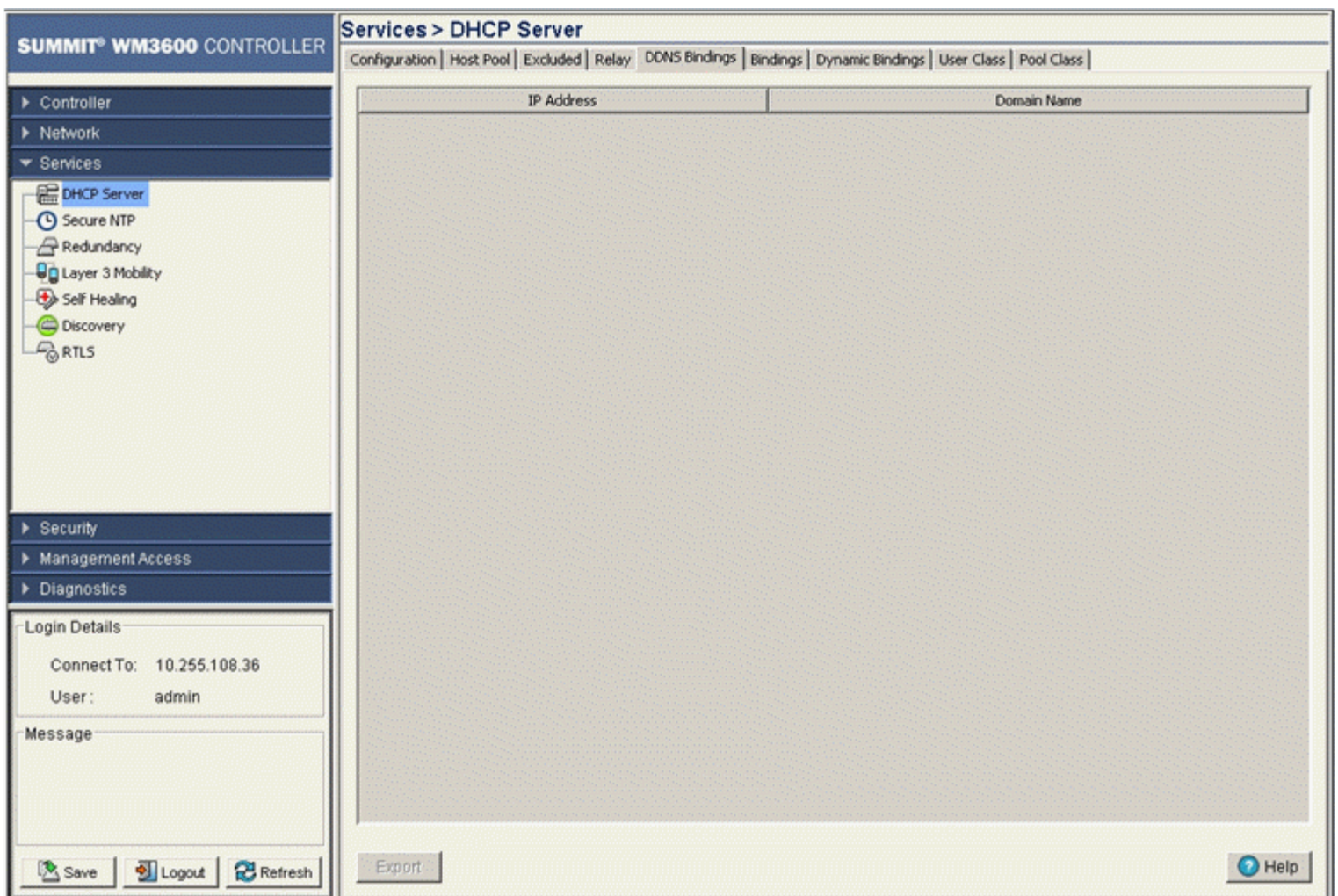
- a Use the *Interface* drop-down menu to assign the interface used for the DHCP relay. As VLANs are added to the controller, the number of interfaces available grows.
- b Add *Servers* as needed to supply DHCP relay resources.
- c Click *OK* to save and add the changes to the running configuration and close the dialog.
- d Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing DDNS Bindings

The *DDNS Bindings* tab displays mappings between client IP addresses and domain names. DDNS keeps a domain name linked to a changing IP address. Typically, when a user connects to a network, the user's ISP assigns an unused IP address from a pool of IP addresses (usually done through a DHCP server). This address is only valid for a limited time. The mechanism of dynamically assigning IP addresses increases the pool of assignable IP addresses. DNS is a service, which maintains a database to map a given name to an IP address used for communication on the Internet. The dynamic assignment of IP addresses makes it necessary to update the DNS database to reflect the current IP address for a given name.

To view controller DDNS binding information:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *DDNS Bindings* tab.



- 3 Refer to the contents of the *DDNS Bindings* tab for the following information:

IP Address	Displays the IP address assigned to the client.
Domain Name	Displays the domain name mapping corresponding to the IP address listed in the left-hand side of the tab.

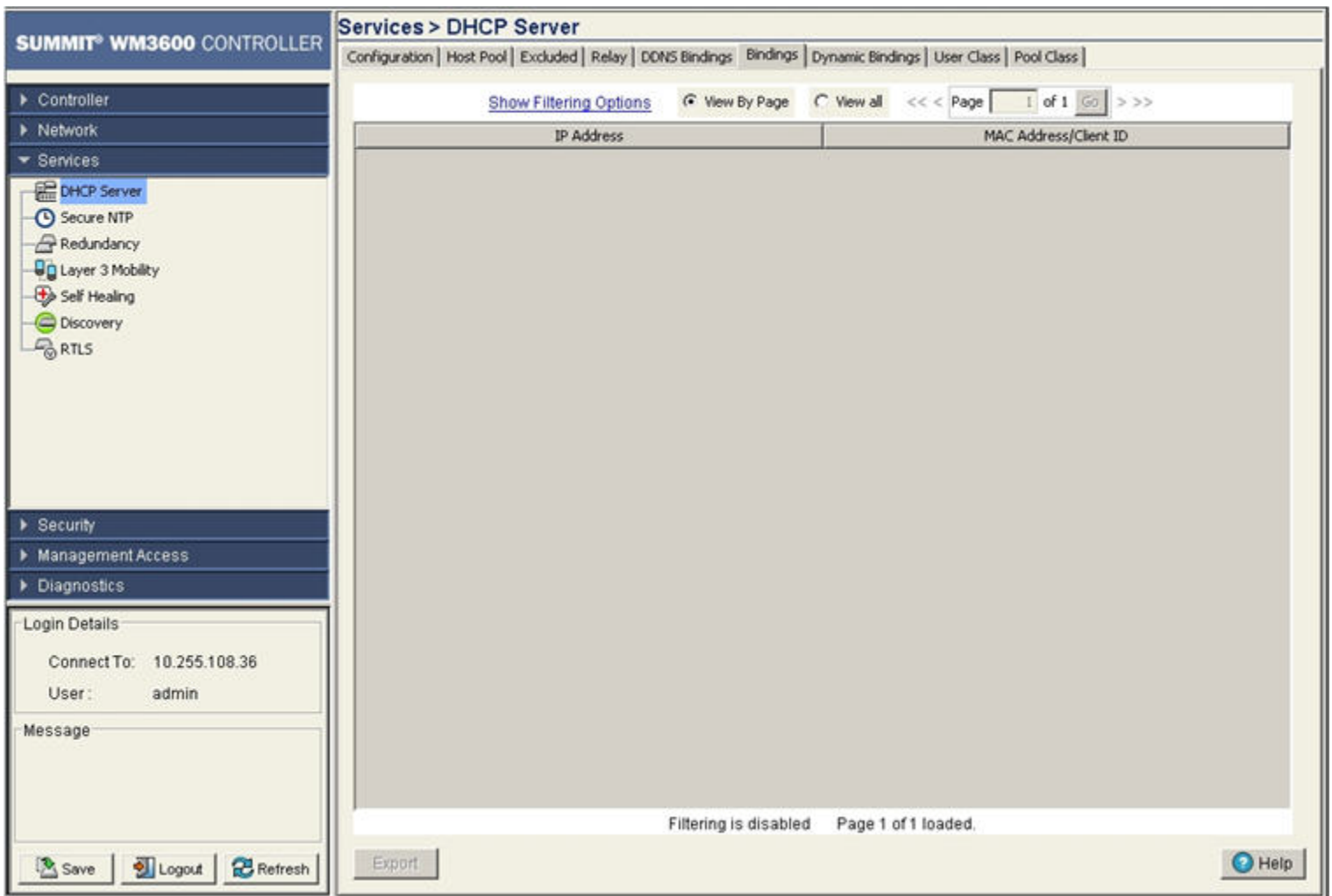
- 4 Click the *Export* button to display a screen used to export DDNS Binding information to a secure location.

Viewing DHCP Bindings

The Bindings tab displays addresses and expiration times. There are two types of bindings, manual and automatic. Manual bindings map a hardware address to a IP address statically. Automatic bindings dynamically map a hardware address to an IP address from a pool of available addresses.

To view detailed binding information:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *Bindings* tab.



- 3 Refer to the contents of the Bindings tab for the following information:

IP Address	Displays an IP address for each client with a listed MAC address. This column is read-only and cannot be modified.
MAC Address / Client ID	Displays the MAC address (client hardware ID) of the client using the controller's DHCP Server to access controller resources. The MAC address is read-only and cannot be modified.

- 4 Click the *Export* button to display a screen used to export the DHCP Binding information to a secure location.

Reviewing DHCP Dynamic Bindings

Dynamic DHCP bindings automatically map a hardware address to an IP address from a pool of available addresses. The Dynamic Bindings tab displays only automatic bindings.

To view detailed Dynamic DHCP Binding Status information:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *Dynamic Bindings* tab.

The screenshot shows the Summit WM3600 Controller interface. The main content area displays the 'Dynamic Bindings' tab for a DHCP Server. The table below shows the data for dynamic bindings:

IP Address	MAC Address/Client ID	Expiration
10 . 255 . 108 . 101	00-02-A5-B8-AF-9F	Thu May 27 14:10:35 2010 PDT
10 . 255 . 108 . 180	00-1D-6A-0E-7E-FD	Thu May 27 14:21:54 2010 PDT
10 . 255 . 108 . 181	00-09-5B-41-58-4C	Thu May 27 14:23:31 2010 PDT
10 . 255 . 108 . 183	00-15-70-E9-CE-73	Thu May 27 11:33:42 2010 PDT
10 . 255 . 108 . 184	00-15-70-54-64-E1	Thu May 27 11:23:55 2010 PDT
10 . 255 . 108 . 193	00-23-68-0F-43-B8	Thu May 27 11:28:30 2010 PDT
10 . 255 . 108 . 199	00-04-96-43-50-71	Thu May 27 12:06:01 2010 PDT

At the bottom of the interface, there are buttons for 'Delete', 'Delete All Dynamic Leases', 'Export', and 'Help'. The status bar indicates 'Filtering is disabled' and 'Page 1 of 1 loaded'.

3 Refer to the contents of the Dynamic Bindings tab for the following:

- | | |
|-------------------------|---|
| IP Address | Displays the IP address for each client whose MAC Address is listed in the MAC Address / Client ID column. This column is read-only and cannot be modified. |
| MAC Address / Client ID | Displays the MAC address (client hardware ID) of the client using the controller's DHCP Server to access controller resources. The MAC address is read-only and cannot be modified. |
| Expiration | Displays the expiration of the lease used by the client for controller DHCP resources. This column is read-only and cannot be modified. |

- 4 Select an address from those displayed and click the *Delete* button to remove the client from the list displayed. The Delete button is enabled only when one or more rows are selected for deletion.
- 5 Click the *Delete All Automatic Leases* button to delete all the automatic leased DHCP connections. This button is enabled when one or more rows exist.
- 6 Click the *Export* button to display a screen used to export the DHCP Binding information to a secure location.

Configuring the DHCP User Class

The DHCP server assigns IP addresses to clients based on user class option names. Clients with a defined set of user class option names are identified by their user class name.

The DHCP server assigns IP addresses from multiple IP address ranges. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

To view the attributes of existing host pools:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *User Class* tab to view the DHCP user class and its associated user class option names.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation menu with categories: Controller, Network, Services (expanded), Security, Management Access, and Diagnostics. Under Services, DHCP Server is selected. The main content area is titled 'Services > DHCP Server' and has several tabs: Configuration, Host Pool, Excluded, Relay, DDNS Bindings, Bindings, Dynamic Bindings, User Class (selected), and Pool Class. The 'User Class' tab displays two large text areas: 'User Class Name' and 'User Class Option Name'. The 'User Class Name' area is empty. The 'User Class Option Name' area contains eight rows labeled 'Option Value 1' through 'Option Value 8', each with an empty input field. Below these fields is a checkbox labeled 'Multiple User Class Options' which is unchecked. At the bottom of the main content area are three buttons: 'Edit', 'Delete', and 'Add'. The bottom of the interface features a 'Save' button, a 'Logout' button, a 'Refresh' button, and a 'Help' button.

- 3 The *User Class Name* field displays the client names grouped by the class name.
- 4 The *User Class Option Name* field displays the names defined for a particular client. Select the *Multiple User Class Options* checkbox to associate the user class option names with a multiple user class.
- 5 Click the *Add* button create a new user class name (client). For more information, see [“Adding a New DHCP User Class”](#) on page 329.

- 6 Click the *Edit* button to modify the properties displayed for an existing DHCP User Class Name. For more information, see [“Editing the Properties of an Existing DHCP User Class”](#) on page 330.
- 7 To delete an existing DHCP user class and its associated option names from the list available to the DHCP server, select the user class from the *User Class Name* field and click *Delete*.

Adding a New DHCP User Class

A DHCP user class name can be configured with a maximum of 8 user class option values.

To view and configure the user class options associated with the particular class:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *User Class* tab.
- 3 Click the *Add* button from the *User Class Name* section.

The screenshot shows a dialog box titled "Services > DHCP Server > Configuration" with a close button (X) in the top right corner. The dialog is split into two panes: "Configuration" on the left and "User Class Information" on the right. The "User Class Information" pane contains a text field for "User Class Name" with the value "Class Name". Below this are eight text fields for "Option Value 1" through "Option Value 8", with "Option Value 1" containing the number "1". At the bottom of the "User Class Information" pane is a checkbox labeled "Multiple User Class Options" which is currently unchecked. Below the panes is a "Status:" label. At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

The DHCP server groups clients based on user class option values. DHCP Clients with the defined set of user class option values are identified by class.

- a Enter the *User Class Name* to create a new client. The DHCP user class name should not exceed 32 characters.
- b Enter *Option Values* for the devices associated with the DHCP user class name. The value should not exceed 32 characters.
- c Select the *Multiple User Class Option* checkbox to enable multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options.
- d Click *OK* to save and add the new configuration.

- e Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- f Click *Cancel* to close the dialog without committing updates to the running configuration.

Editing the Properties of an Existing DHCP User Class

The properties of an existing DHCP user class can be modified to suit the changing needs of your network. To modify the properties of an existing DHCP user class:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *User Class* tab.
- 3 Select an existing DHCP user class name from the list and click the *Edit* button from the *DHCP User Class Name* section.

- a The *User Class Name* is a display field and cannot be modified.
- b Either add or modify the *Option Values* as required to suit the changing needs of your network. The option values should not exceed 50 characters.
- c Select the *Multiple User Class Option* checkbox to enable multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers which support multiple user class options.
- d Click *OK* to save and add the new configuration and close the dialog window.
- e Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.

- f Click *Cancel* to close the dialog without committing updates to the running configuration.

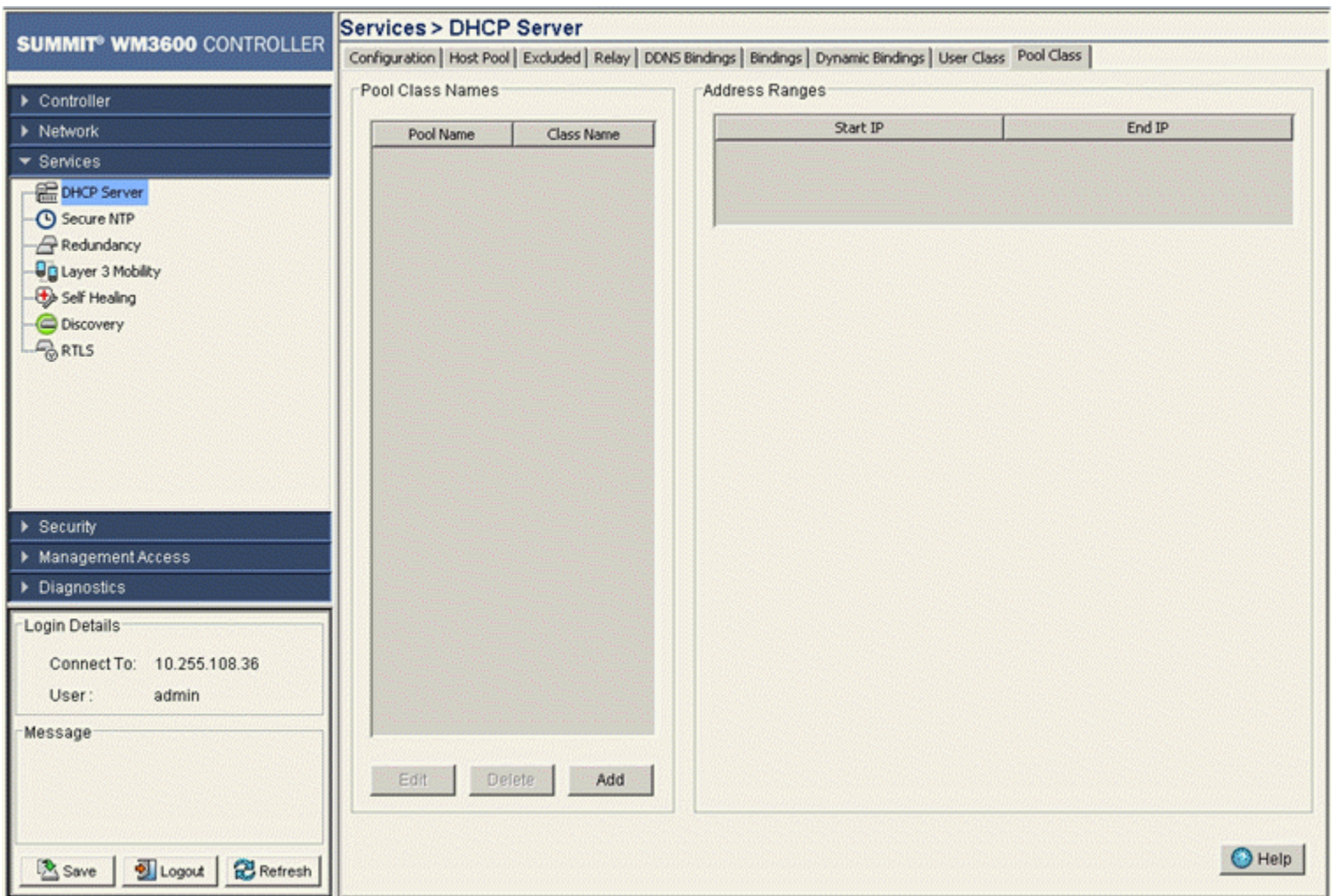
Configuring DHCP Pool Class

The DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses.

DHCP clients are matched against classes. If the client matches one of the classes assigned to the pool, it's assigned the IP address from the range assigned to the class. If the client does not match any of the classes in the pool, it's assigned the IP address from the pool's default range (if configured).

To view the attributes of existing host pools:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *Pool Class* tab to view the DHCP pool class details.



- 3 Refer to the *Pool Class Names* field to configure a pool class. A preconfigured pool and class must exist to configure a pool class.
The *Address Ranges* section displays the address ranges associated with the pool class.
- 4 Click the *Edit* button to modify the properties displayed for an existing DHCP Pool Class Name. For more information, see [“Editing an Existing DHCP Pool Class” on page 332](#).

- 5 To delete an existing DHCP pool class name and its associated address range, select the pool class name from the *Pool Class Names* field and click the *Delete* button.
- 6 Click the *Add* button create a new pool class name. For more information, see [“Adding a New DHCP Pool Class” on page 332](#).

Editing an Existing DHCP Pool Class

The *Edit DHCP Pool Class Configuration* dialog is used to edit the association of a DHCP pool name to a DHCP class name. It is also used to configure a maximum of 4 pool class address range. To revise an existing DHCP pool class name:

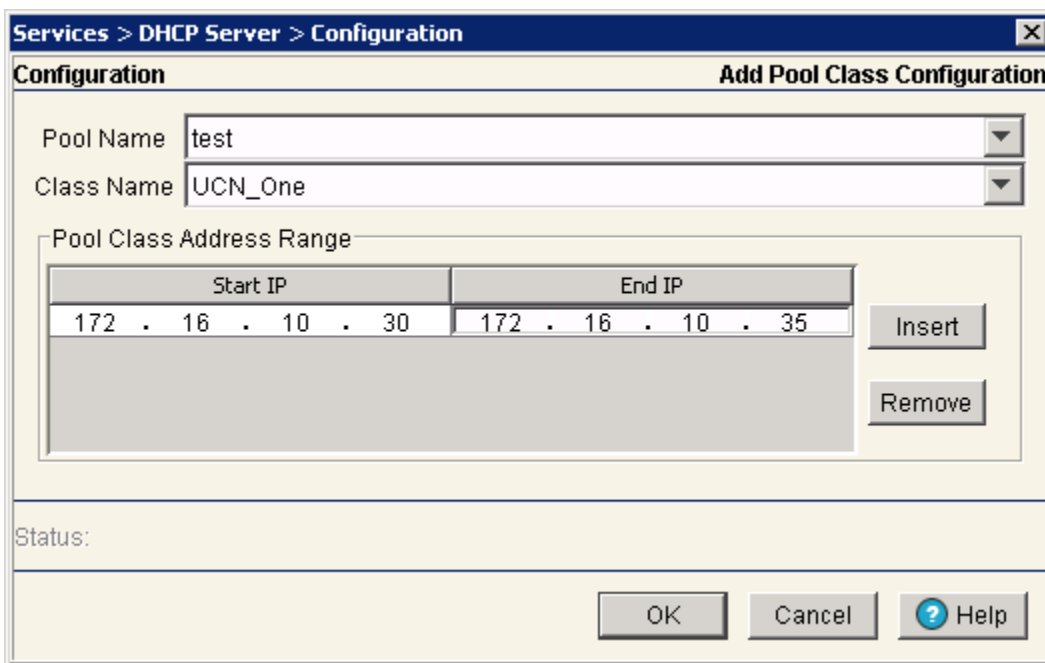
- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *Pool Class* tab.
- 3 Click the *Edit* button from the *Pool Class Names* section.
- 4 Refer to the read-only *Pool Name* to ensure modifications are made to the correct pool name.
- 5 Use the *Class Name* field to associate an existing class, created using [“Adding a New DHCP User Class” on page 329](#).
- 6 Refer to the *Pool Class Address Range* field to revise an address range. A maximum of 4 address ranges can be assigned to a class.
 - a Use the *Insert* button to revise the Start IP and End IP address range for a class.
 - b Select an address range and click *Remove* to delete that particular address range.
- 7 Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to save the new configuration and close the dialog window.
- 9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding a New DHCP Pool Class

The *Add DHCP Pool Class Configuration* dialog is used to associate an existing class, created using [“Adding a New DHCP User Class”](#), to an existing pool, created using [“Adding a New DHCP Pool”](#). It is also used to configure a maximum of 4 pool class address range. To add a new DHCP pool class:

- 1 Select *Services > DHCP Server* from the main menu tree.
- 2 Select the *Pool Class* tab.

- 3 Click the *Add* button from the *Pool Class Names* section.



- 4 Use the *Pool Name* field to define a new pool name. Enter the pool name created using [“Adding a New DHCP Pool”](#) on page 314.
- 5 Use the *Class Name* field to associate an existing class, created using [“Adding a New DHCP User Class”](#) on page 329.
- 6 The *Pool Class Address Range* field is used to assign address range to the class inside the pool. A maximum of 4 address ranges can be assigned to a class.
 - a Use the *Insert* button to enter the Start IP and End IP address range for a class.
 - b Select a address range and click *Remove* to delete that particular address range.
- 7 Refer to the *Status* field. It displays the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to save the new configuration and close the dialog window.
- 9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Secure NTP

Secure Network Time Protocol (SNTP) is central for networks that rely on their controller to supply system time. Without an SNTP implementation, controller time is unpredictable, which can result in data loss, failed processes and compromised security. With network speed, memory and capability increasing at an exponential rate, the accuracy, precision and synchronization of network time is essential in a controller managed enterprise network. The controller can either use a dedicated server to supply system time or can use several forms of SNTP messaging to sync system time with network traffic authenticated and secure for controller interoperation.



NOTE

Often, the controller NTP status will not be adequately updated after modifying the NTP configuration. Periodically check the controller NTP status when making changes to ensure the proper time is displayed, as it may take awhile for the controller to update the proper NTP status.

The SNTP configuration activity is divided among the following tasks:

- [Defining the SNTP Configuration on page 334](#)
- [Configuring Symmetric Key on page 336](#)
- [Defining an NTP Neighbor Configuration on page 338](#)
- [Viewing NTP Associations on page 341](#)
- [Viewing NTP Status on page 343](#)

Defining the SNTP Configuration

Symmetric keys are algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption. The encryption key is related to the decryption key, as they may be identical or there is a simple mechanism to go between keys. The keys represent a shared secret between the controller and its time resource.

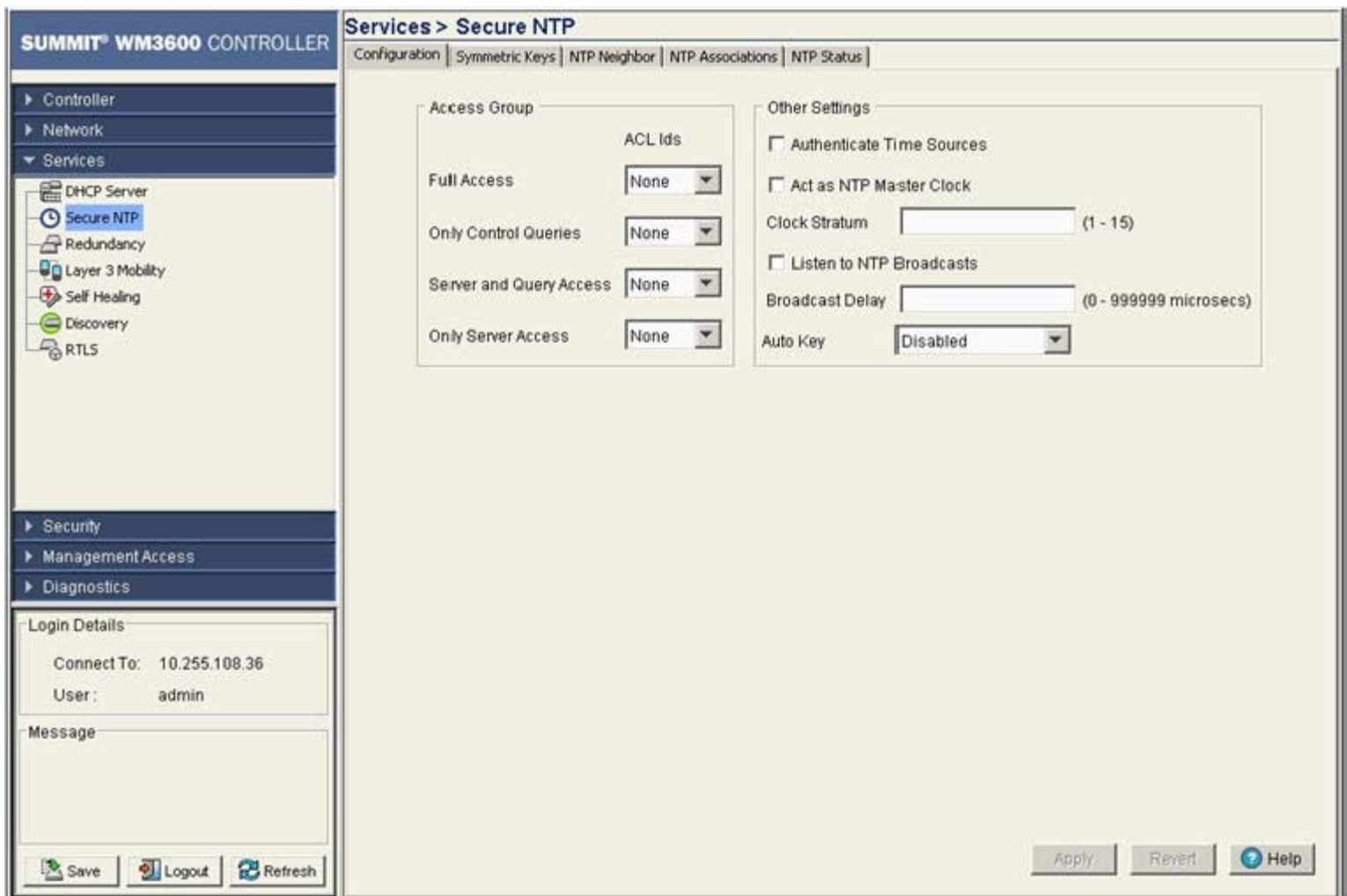


NOTE

When using the SNTP service, ensure that traffic can pass on UDP port 123 between the controller and the NTP server.

To define the SNTP configuration:

- 1 Select *Services > Secure NTP* from the main menu tree.
- 2 Select the *Configuration* tab.



- 3 An ACL Id must be created before it is selectable from any of the drop-down menus. Refer to the *Access Group* field to define the following:

Full Access	Supply a numeric ACL ID from the drop-down menu to provide the ACL full access.
Only Control Queries	Supply a numeric ACL ID from the drop-down menu to provide the ACL only control query access to SNTP resources.
Server and Query Access	Enter a numeric ACL ID from the drop-down menu to provide the ACL Server and Query access to SNTP resources.
Only Server Access	Provide a numeric ACL ID from the drop-down menu to provide the ACL only server access to SNTP resources.

4 Refer to the *Other Settings* field to define the following:

Authenticate Time Sources	Select this checkbox to ensure credential authentication takes place between the SNTP server and the controller. When this checkbox is selected, the Apply and Revert buttons become enabled to save or cancel settings.
Act As NTP Master Clock	When this checkbox is selected, the Apply and Revert buttons become enabled to save or cancel settings within the Other Settings field.
Clock Stratum	Define how many hops (from 1 to 15) the controller is from a SNTP time source. The controller automatically chooses the SNTP resource with the lowest stratum number. The SNTP supported controller is careful to avoid synchronizing to a server that may not be accurate. Thus, the SNTP enabled controller never synchronizes to a machine not synchronized itself. The SNTP enabled controller compares the time reported by several sources, and does not synchronize to a time source whose time is significantly different than others, even if its stratum is lower.
Listen to NTP Broadcasts	Select this checkbox to allow the controller to listen over the network for SNTP broadcast traffic. Once enabled, the controller and the SNTP broadcast server must be on the same network.
Broadcast Delay	Enter the estimated round-trip delay (between 1 and 999999 seconds) for SNTP broadcasts between the SNTP broadcast server and the controller. Define the interval based on the priority of receiving accurate system time frequently. Typically, no more than one packet per minute is necessary to synchronize the controller to within a millisecond of the SNTP broadcast server.
Auto Key	Use an <i>Auto Key</i> drop-down menu to specify whether the key is disabled, enabled only on the host or enabled only on the client.

5 Click *Apply* to save changes to the screen. Navigating away from the screen without clicking the *Apply* button results in all the changes to the screen being discarded.

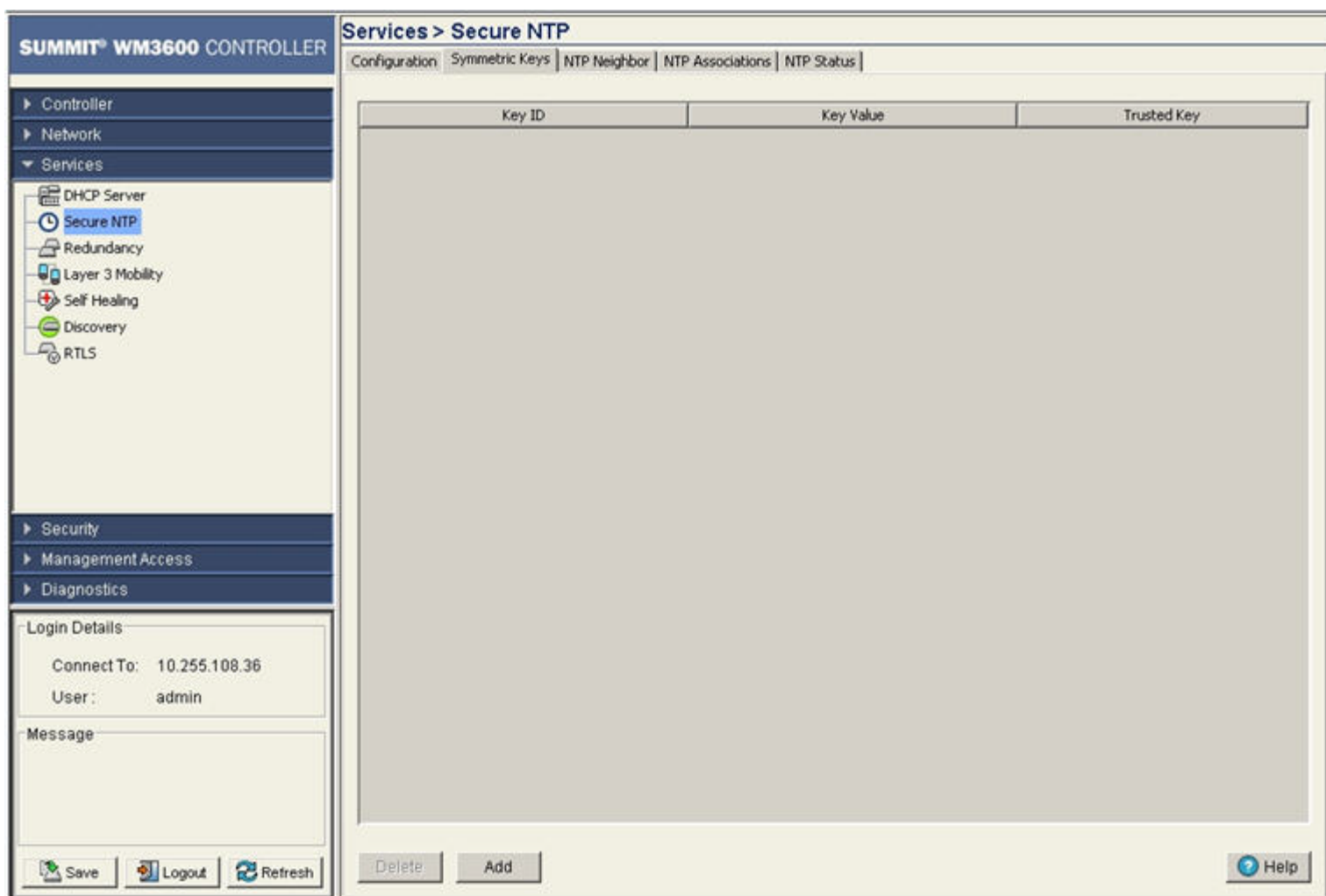
6 Click the *Revert* button to undo the changes to the screen and revert to the last saved configuration.

Configuring Symmetric Key

Symmetric keys are algorithms for cryptography that use trivially related cryptographic keys for both decryption and encryption. The encryption key is related to the decryption key, as they may be identical or there is a simple mechanism to go between keys. The keys represent a shared secret between the controller and its time resource.

To review existing Symmetric Key configurations, and (if necessary) add a new one:

- 1 Select *Services > Secure NTP* from the main menu tree.
- 2 Select the *Symmetric Keys* tab.



- 3 Refer to the *Symmetric Key* screen to view the following information.

Key ID	Displays a Key ID between 1-65534. The Key ID is an abbreviation allowing the controller to reference multiple passwords. This makes password migration easier and more secure between the controller and its NTP resource.
Key Value	Displays the authentication value used to secure the credentials of the server providing system time to the controller.
Trusted Key	If a checkmark appears, a trusted key has been associated with a domain name. A trusted key is added when a public key is known, but cannot be securely obtained. Adding the trusted key allows information from the server to be considered secure. The authentication procedures requires both the local and remote servers share the same key and key identifier. Therefore, using key information from a trusted source is important.

- 4 Select an existing key and click the *Delete* button to permanently remove it from the list of Key IDs.
- 5 Click the *Add* button to create a new Symmetric Key that can be used by the controller.

**CAUTION**

After an NTP synchronization using a Symmetric Key, the NTP status will not automatically be updated.

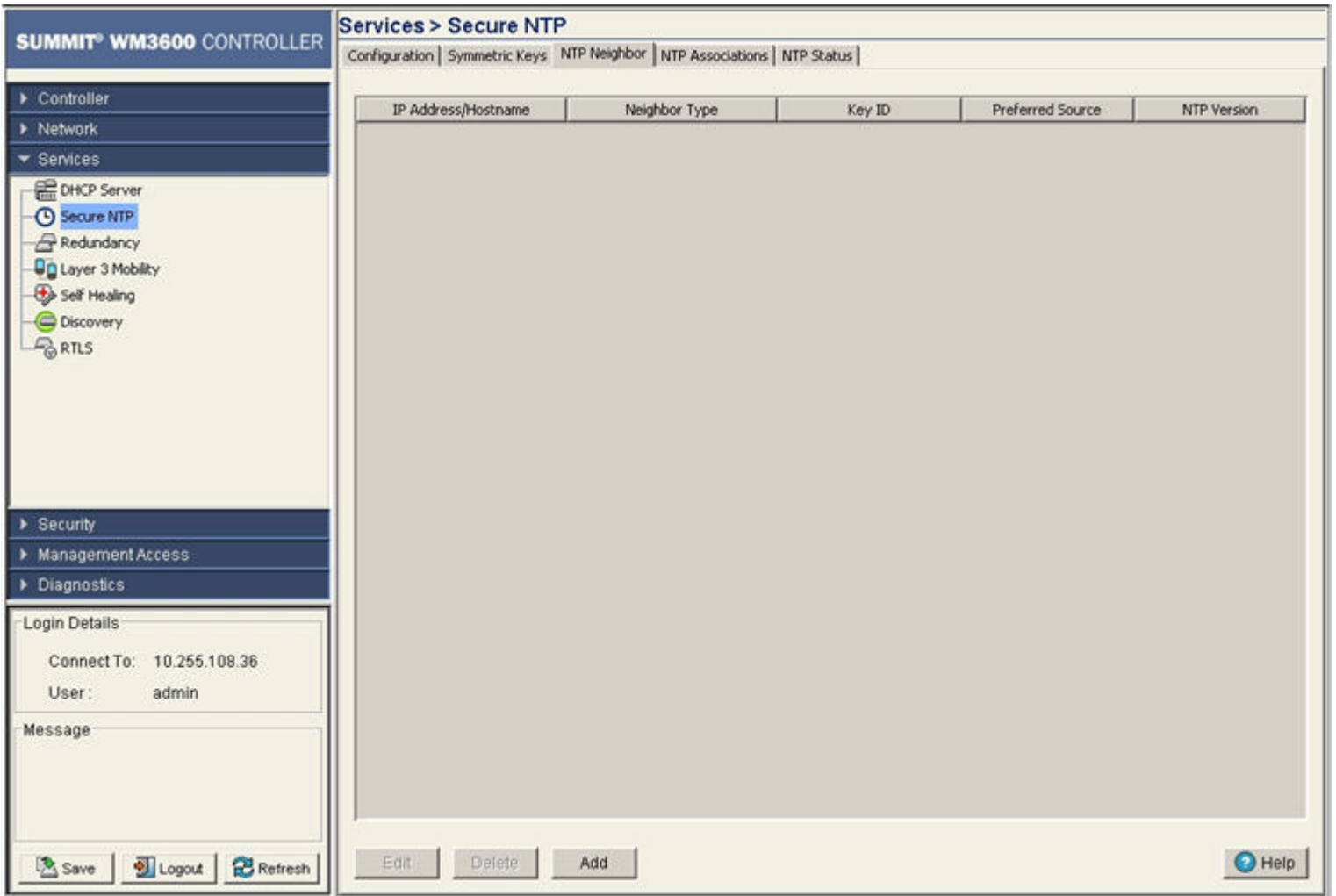
- 6 Enter a Key ID between 1-65534. The *Key ID* is a Key abbreviation allowing the controller to reference multiple passwords.
This makes password migration easier and more secure between the controller and its NTP resource.
- 7 Enter an authentication *Key Value* used to secure the credentials of the NTP server providing system time to the controller.
- 8 Select the *Trusted Key* checkbox to use a trusted key.
A trusted key should be used when a public key is known, but cannot be securely obtained. Adding a trusted key allows data to be considered secure between the controller and its SNTP resource.
- 9 Refer to the *Status* field.
The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

Defining an NTP Neighbor Configuration

The controller’s NTP association can be either a neighboring peer (the controller synchronizes to another associated device) or a neighboring server (the controller synchronizes to a dedicated SNTP server resource). Refer to the *NTP Neighbor* tab to assess the controller’s existing configurations (both peer and server) and, if necessary, modify the attributes of an existing peer or server configuration or create a new neighbor peer or server SNTP configuration.

To review the controller's existing NTP neighbor configurations:

- 1 Select *Services > Secure NTP* from the main menu tree.
- 2 Select the *NTP Neighbor* tab.



- 3 Refer to the following information (as displayed within the NTP Neighbor tab) to assess whether an existing neighbor configuration can be used as is, if an existing configuration requires modification or a new configuration is required.

IP Address/ Hostname	Displays the numeric IP address of the resource (peer or server) providing controller SNTP resources. Ensure the server is on the same subnet as the controller to provide SNTP support.
Neighbor Type	Displays whether the NTP resource is a Peer (another associated peer device capable of SNTP support) or a Server (a dedicated NTP server resource). This designation is made when adding or editing an NTP neighbor.
Key ID	Displays whether AutoKey Authentication or Symmetric Key Authentication is used to secure the interaction between the controller and its NTP resource. This designation is made when adding or editing an NTP neighbor.
Preferred Source	Displays whether this NTP resource is a preferred NTP resource. Preferred sources (those with a checkmark) are contacted before non-preferred resources. There can be more than one preferred source.

NTP Version Displays an NTP version between 1 and 4. Currently version three and four implementations of NTP are available. The latest version is NTPv4, but the official Internet standard is NTPv3.

- 4 Select an existing neighbor and click the *Edit* button to modify the existing peer or server designation, IP address, version, authentication key ID and preferred source designation.
- 5 Select an existing entry and click the *Delete* button to remove it from the table.
- 6 Click the *Add* button to define a new peer or server configuration that can be added to the existing configurations displayed within the NTP Neighbor tab. For more information, see [“Adding an NTP Neighbor”](#) on page 340.

Adding an NTP Neighbor

To add a new NTP peer or server neighbor configuration to those available for synchronization:

- 1 Select *Services > Secure NTP* from the main menu tree.
- 2 Select the *NTP Neighbor* tab.
- 3 Click the *Add* button.

The screenshot shows a dialog box titled "Services > Secure NTP > Add Neighbor". The dialog has a title bar with a close button (X). The main area is titled "Add Neighbor" and contains several radio button options and input fields. The "Peer" radio button is selected. Below it are "Broadcast Server", "IP Address" (with a dotted input field), "Hostname" (with an empty text input field), and "NTP Version" (with a dropdown menu). Underneath are "No Authentication" (selected), "AutoKey Authentication", and "Symmetric Key Authentication" radio buttons. There is a "Key ID" text input field and a "Preferred Source" checkbox. At the bottom, there is a "Status:" label and three buttons: "OK", "Cancel", and "Help".

-
- 4 Select the *Peer* checkbox if the SNTP neighbor is a peer to the controller (non FTP server) within the controller's current subnet.
 - 5 Select the *Server* checkbox if the neighbor is a server within the controller's current subnet.
 - 6 Select the *Broadcast Server* checkbox to allow the controller to listen over the network for NTP broadcast traffic.

The controller's NTP configuration can be defined to use broadcast messages instead of messaging between fixed NTP synchronization resource addresses. Use a NTP broadcast to listen for NTP synchronization packets within a network. To listen to NTP broadcast traffic, the broadcast server (and controller) must be on the same subnet. NTP broadcasts reduce configuration complexity since both the controller and its NTP resources can be configured to send and receive broadcast messages.



NOTE

If this checkbox is selected, the AutoKey Authentication checkbox is disabled, and the controller is required to use Symmetric Key Authentication for credential verification with its NTP resource. Additionally, if this option is selected, the broadcast server cannot be selected as a preferred source.

- 7 Enter the *IP Address* of the peer or server providing SNTP synchronization.
- 8 Select the *Hostname* checkbox to assign a hostname to the server or peer for further differentiation of other devices with a similar configuration.
- 9 Use the *NTP Version* drop-down menu to select the version of SNTP to use with this configuration. Currently version three and version four implementations of NTP are available. The latest version is NTPv4, but the official Internet standard is NTPv3.
- 10 If necessary, select the *No Authentication* checkbox to allow communications with the NTP resource without any form of security. This option should only be used with known NTP resources.
- 11 Select the *AutoKey Authentication* checkbox to use an Auto key protocol based on the public key infrastructure (PKI) algorithm. The SNTP server uses a fast algorithm and a private value to regenerate key information on the arrival of a message. The controller sends its designated public key to the server for credential verification and the two exchange messages. This option is disabled when the Broadcast Server checkbox is selected.
- 12 Select the *Symmetric Key Authentication* checkbox to use a single (symmetric) key for encryption and decryption. Since both the sender and the receiver must know the same key, it is also referred to as shared key cryptography. The key can only be known by the sender and receiver to maintain secure transmissions.
- 13 Enter an *Key ID* between 1-65534. The Key ID is a Key abbreviation allowing the controller to reference multiple passwords.
- 14 Select the *Preferred Source* checkbox if this NTP resource is a preferred NTP resource. Preferred sources are contacted before non-preferred resources. There can be more than one preferred source.
- 15 Refer to the *Status* field. The Status is the current state of the requests made from the applet. Requests are any "SET/GET" operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 16 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 17 Click *Cancel* to close the dialog without committing updates to the running configuration.

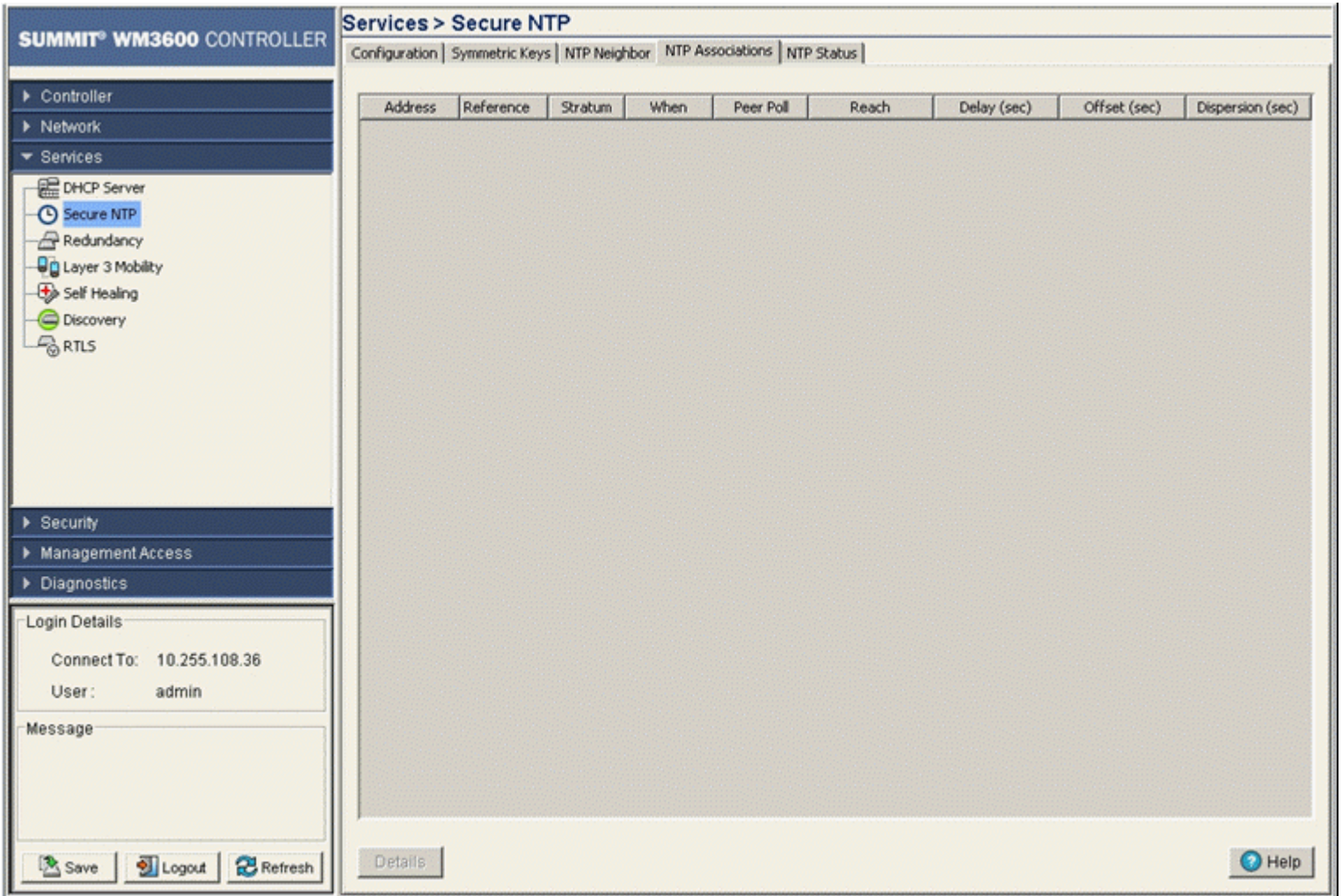
Viewing NTP Associations

The interaction between the controller and an SNTP server constitutes an association. SNTP associations can be either a peer association (the controller synchronizes to the another system or allows another

system to synchronize to it), or a server association (only the controller synchronizes to the SNTP resource, not the other way around).

To review the controller’s current SNTP associations:

- 1 Select *Services > Secure NTP* from the main menu tree.
- 2 Select the *NTP Associations* tab.



- 3 Refer to the following SNTP Association data for each SNTP association displayed:

Address	Displays the numeric IP address of the SNTP resource (Server) providing SNTP updates to the controller.
Reference Clock	Displays the address of the time source the controller is synchronized to.
Stratum	Displays how many hops the controller is from a SNTP time source. The controller automatically chooses the SNTP resource with the lowest stratum. The SNTP supported controller is careful to avoid synchronizing to a server that may not be accurate. Thus, the NTP enabled controller never synchronizes to a machine not synchronized itself. The SNTP enabled controller compares the time reported by several sources, and does not synchronize to a time source whose time is significantly different than others, even if its stratum is lower.
When	Displays the date and time when the SNTP association was initiated. Has the association been trouble free over that time?

Peer Poll	Displays the maximum interval between successive messages, in seconds to the nearest power of two.
Reach	Displays the status of the last eight SNTP messages. If an SNTP packet is lost, the lost packet is tracked over the next eight SNTP messages.
Delay (sec)	Displays the round-trip delay (in seconds) for SNTP broadcasts between the SNTP server and the controller.
Offset (sec)	Displays the calculated offset between the controller and SNTP server. The controller adjusts its clock to match the server's time value. The offset gravitates toward zero over time, but never completely reduces its offset to zero.
Dispersion (sec)	Displays how scattered the time offsets are (in seconds) from an SNTP time server

- 4 Select an existing NTP association and click the *Details* button to display additional information useful in discerning whether the association should be maintained.

The screenshot shows a web interface window titled "Services > Secure NTP > Details" with a close button (X) in the top right corner. The main content area displays a table of NTP association details for the IP address 172.16.10.100. The table is organized into two columns of key-value pairs. At the bottom of the window, there is a "Status:" label and three buttons: "Refresh", "Close", and "Help".

Details		172.16.10.100	
IP Address	172.16.10.100	Root Dispersion	0.00
Association	configured	Reach	0
Sanity	sane	Delay	0.00
Validity	true	Offset	0.0000
Authority	unknown	Dispersion	0.00
Leap State	sub	Precision	2 ⁻¹⁷
Stratum	16	Reference Time	00000000.00000000 (Feb 07 06:28:16 UTC 2036)
Reference Id	BCST	Org Time	00000000.00000000 (Feb 07 06:28:16 UTC 2036)
Host Mode	broadcast	Receive Time	00000000.00000000 (Feb 07 06:28:16 UTC 2036)
Peer Mode	unspec	Transmit Time	00000000.00000000 (Feb 07 06:28:16 UTC 2036)
Host Poll	6	Filter Delay	0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
Peer Poll	10	Filter Offset	0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
Root Delay	0.00	Filter Error	16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00

Status:

Refresh Close Help

Viewing NTP Status

Refer to the *NTP Status* tab to display performance (status) information relative to the controller's current NTP association. Verifying the controller's SNTP status is important to assess which resource

the controller is currently getting its system time from, as well as the time server’s current differences in time attributes as compared to the current controller time.

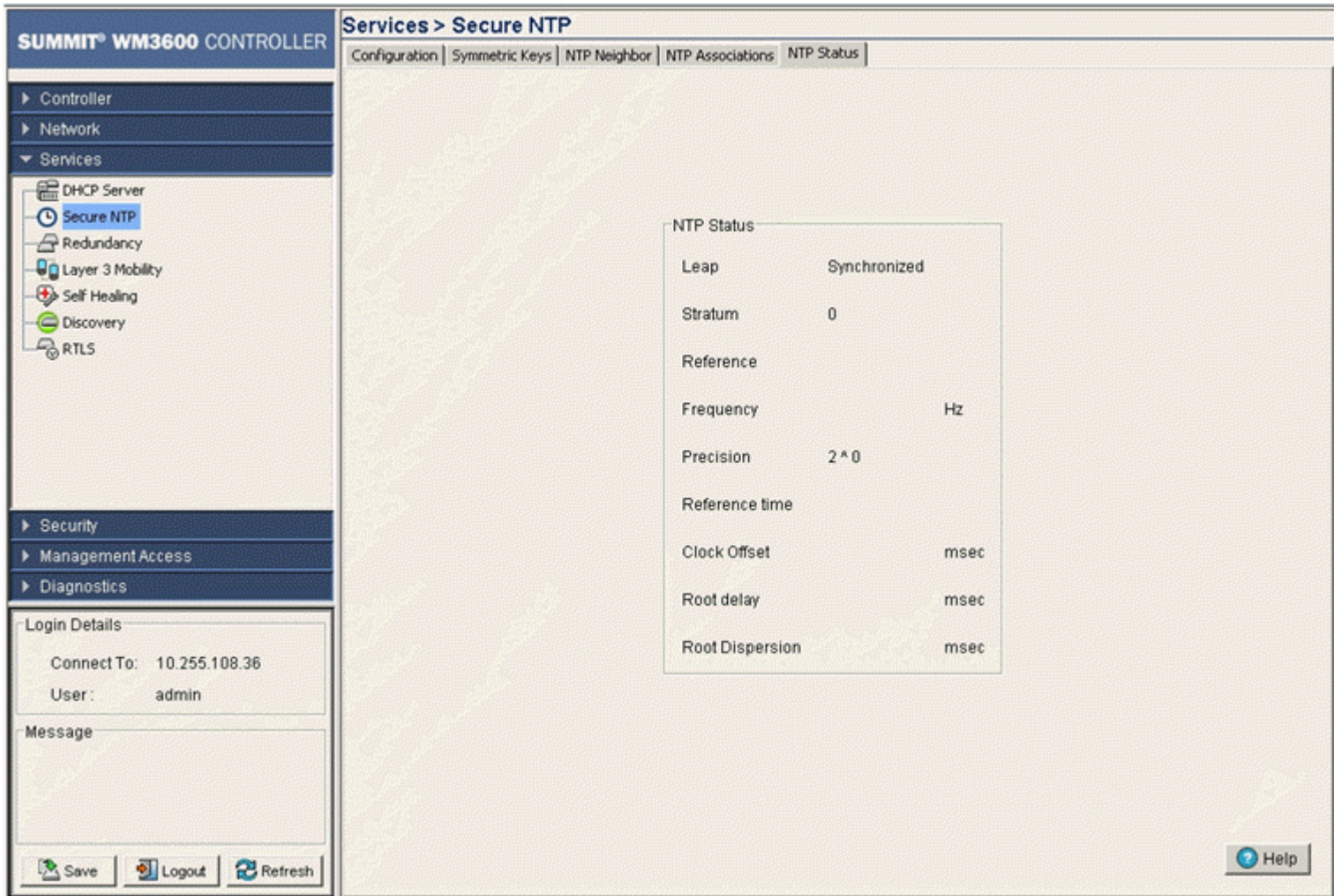


CAUTION

After an NTP synchronization using a Symmetric Key, the NTP status will not automatically update.

To review the controller’s current NTP associations:

- 1 Select *Services > Secure NTP* from the main menu tree.
- 2 Select the *NTP Status* tab.



- 3 Refer to the *SNTP Status* field to review the accuracy and performance of the controller’s ability to synchronize with a NTP server:

Leap	Indicates if a second will be added or subtracted to SNTP packet transmissions, or if the transmissions are synchronized.
Stratum	Displays how many hops the controller is from its current NTP time source.
Reference	Displays the address of the time source the controller is synchronized to.
Frequency	An SNTP server clock’s skew (difference) for the controller

Precision	Displays the precision (accuracy) of the controller's time clock (in Hz). The values that normally appear in this field range from -6 for mains-frequency clocks to -20 for microsecond clocks found in some workstations.
Reference time	Displays the time stamp at which the local clock was last set or corrected.
Clock Offset	Displays the time differential between controller time and the NTP resource.
Root delay	The total round-trip delay in seconds. This variable can take on both positive and negative values, depending on the relative time and frequency offsets. The values that normally appear in this field range from negative values of a few milliseconds to positive values of several hundred milliseconds.
Root Dispersion	Displays the nominal error relative to the primary time source in seconds. The values that normally appear in this field range from 0 to several hundred milliseconds.

Configuring Controller Redundancy and Clustering

Configuration and network monitoring are two tasks a network administrator faces as a network grows in terms of the number of managed nodes (controllers, routers, wireless devices etc.). Such scalability requirements lead network administrators to look for managing and monitoring each node from a single centralized management entity. The controller not only provides a centralized management solution, it provides centralized management from any single controller in the network without restricting or dedicating one controller as a centralized management node. This eliminates dedicating a management entity to manage all redundancy members and eliminates the possibility of a single point of failure.

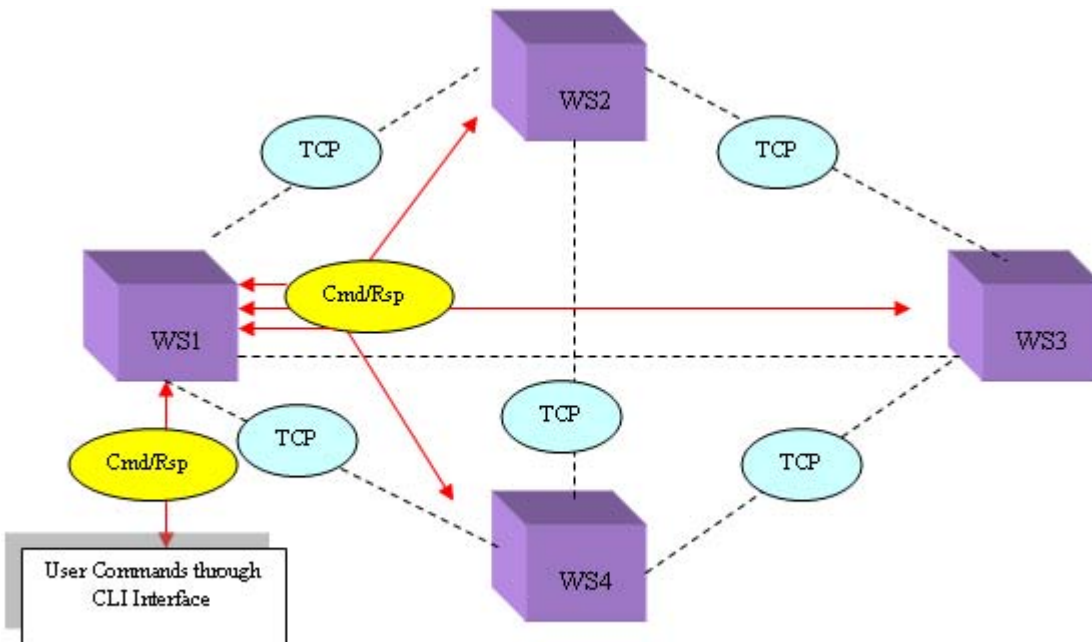
A redundancy group (cluster) is a set of controllers (nodes) uniquely identified by group/cluster ID. Within the redundancy group, members discover and establish connections to other group members. The redundancy group has full mesh connectivity using TCP as the transport layer connection.

Up to 12 controllers can be configured as members of a redundancy group to significantly reduce the chance of a disruption in service to WLANs and associated MUs in the event of failure of a controller or intermediate network failure. All members can be configured using a common file (cluster-config) using DHCP options. This functionality provides an alternative method for configuring members collectively from a centralized location, instead of configuring specific redundancy parameters on individual controllers.

Configure each controller in the cluster by logging in to one participating controller. The administrator does not need to login to each redundancy group member, as one predicating controller can configure each member in real-time without "pushing" configurations between controllers. A new CLI context called "cluster-cli" is available to set the configuration for all members of the cluster. All controller CLI commands are considered cluster configurable.

In the following example, there are four controllers (WS1, WS2, WS3 and WS4) forming a redundancy group. Each controller has established a TCP connection with the others in the group. There is an additional CLI context called cluster-context. A user/administrator can get into this context by executing a "cluster-cli enable" under the CLI interface (future releases will have this support in the Web UI and SNMP interfaces). When the user executes this command on WS1, WS1 creates a virtual session with the other controllers in the redundancy group (WS2, WS3 and WS4). Once the virtual session is created, any command executed on WS1 is executed on the other controllers at the same time.

This is done by the cluster-protocol running on WS1, by duplicating the commands and sending them to the group over the virtual connection:



After sending the command to other members, the cluster-management protocol (at WS1) waits for a response from the members of the redundancy group. Upon receiving a response from each member, WS1 updates the user's screen and allows the user to enter/execute the next command.

The wait time required to collect responses from other controllers is predefined, so if any one or more members does not respond to a given command within the defined interval, the command originating controller displays whatever responses have been collected and ignores the delayed responses. This time-based response mechanism eliminates the possibility of indefinite response hangs and allows for quicker redundancy group configuration.

There is no fixed master-slave relationship between members. Typically, a controller can be considered a master for the command it originates. Responding members can be considered slaves with respect to that command.

This virtual master-slave relationship makes this design unique when compared to existing centralized management systems. Having a virtual master-slave relationship eliminates a single point of failure, since a user can make use of any controller as the group centralized management entity (using the cluster-management context).



NOTE

When using the redundancy feature, make sure that UDP traffic on port 51515 is open between the redundant controllers.

To view status and membership data and define a redundancy group configuration, refer to the following:

- [Configuring Redundancy Settings on page 347](#)

- Reviewing Redundancy Status on page 350
- Configuring Redundancy Group Membership on page 353
- Redundancy Group License Aggregation Rules on page 357
- Managing Clustering Using the Web UI on page 358

Configuring Redundancy Settings

To configure controller redundancy:

- 1 Select *Services > Redundancy* from the main menu tree.

The Redundancy screen displays with the Configuration tab selected.

SUMMIT® WM3600 CONTROLLER

Services > Redundancy

Configuration | Status | Member

Enable Redundancy

Redundancy Controller IP: 0 . 0 . 0 . 0

Mode: Primary Standby

Redundancy ID: 1 (1-65535)

Discovery Period: 30 (10-60 sec)

Heartbeat Period: 5 (1-255 sec)

Hold Time: 15 (10-255 sec)

Critical Resource: 0 . 0 . 0 . 0

Handle STP convergence Enable DHCP Redundancy

Auto Revert

After: 5 min. (1-1800)

Enable Dynamic AP Load Balance

Runtime Schedule

Start Date: 06/01/2008 (MM/DD/YYYY)

Start Time: 00:00 (HH:MM)

MU Threshold: 32

Interval: 1 (1-366 days)

Enable Cluster GUI

History

State	Time	Trigger	Description
Disabled	Mon May 03 11:28:36 2010 PDT	Disabled	Redundancy Disabled



NOTE

MUs on an independent WLAN will not see any disruptions on a controller fail-over.

2 Refer to the *Configuration* field to define the following:

Enable Redundancy	Select this checkbox to enable/disable clustering. Clustering must be disabled to set a redundancy related parameter. All the modifiable values are grayed out if enabled
Redundancy Controller IP Mode	Define the destination IP address used to send heartbeats and update messages. A member can be in either in <i>Primary</i> or <i>Standby</i> mode. In the redundancy group, all 'Active' members adopt Access Ports/Points except the 'Standby' members who adopt Access Ports/Points only when an 'Active' member has failed or sees an Access Port/Point not adopted by a controller.
Redundancy ID	Define an ID for the cluster group. All the controllers configured in the cluster should have the same Cluster ID. The valid range is 1-65535.
Discovery Period	Use the <i>Discovery Period</i> to configure a cluster member discovery interval. During the discovery time, a controller discovers the existence of other controllers within the redundancy group. Configure an interval between 10 and 60 seconds. The default value is 30 seconds.
Heartbeat Period	The <i>Heartbeat Period</i> is the interval heartbeat messages are sent. Heartbeat messages discover the existence and status of other members within the group. Configure an interval between 1 and 255 seconds. The default value is 5 seconds.
Hold Time	Define the <i>Hold Time</i> for a redundancy group. If there are no heartbeats received from a peer during the hold time, the peer is considered down. In general, the hold period is configured for three times the heartbeat period. Meaning, if three consecutive heartbeats are not received from the peer, the peer is assumed down and unreachable. The hold time is required to be longer than the heartbeat interval. Configure a hold time between 10 and 255 seconds. The default is 15 seconds.
Critical Resource	Enter the IP address of the Critical Resource. When the heartbeat is lost, this resource will be checked for reachability. The critical resource can be any gateway, server or host. If the critical resource is not reachable and the heartbeat is still lost, the controller will deadopt APs and continue to deadopt APs until instructed otherwise.
Handle STP convergence	Select the <i>Handle STP convergence</i> checkbox to enable <i>Spanning Tree Protocol</i> (STP) convergence for the controller. In general, this protocol is enabled in layer 2 networks to prevent network looping. If the network is enabled for STP to prevent looping, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance Access Ports/Points at startup.
Enable DHCP Redundancy	Enables DHCP Redundancy for member controllers. DHCP Redundancy allows an administrator to have only one DHCP server running at any time in a cluster. The clustering protocol enables all peers participating in DHCP redundancy to determine the active DHCP server among them. The controller with lowest Redundancy IP is selected as the active DHCP server for the cluster. This selected active DHCP server can be either a primary or standby controller. The other controllers do not provide DHCP service as long as the selected DHCP server controller is active.

Auto Revert Check this box to enable the *Auto Revert* feature and specify the time (in minutes) for the controller to revert. Configure the interval between 1 and 1800 minutes. The default revert time is 5 minutes.

When a primary controller fails, the standby controller takes over APs adopted by the primary. If the auto revert feature is enabled, when the failed primary controller comes back up, the standby starts a timer based on the auto-revert interval. At the expiry of auto-revert interval (if the primary controller is still up), the standby controller releases all adopted APs and goes back to a monitoring mode. The expiry timer either will be stopped or restarted if the primary controller goes down and comes up during the auto-revert interval.

Revert Now Reverts an active fail-over standby controller to a passive standby controller. When a user presses this button, the standby controller will un-adopt all its adopted APs and move into a standby (passive) mode only if all configured members are up again. The revert function does not push APs to the primary controller unless the primary controller has failed over.



NOTE

Redundancy uses UDP port 51515 for both source and destination port. The TCP connection uses 51515 as the destination port, the source port is selected from the range of 32768 to 61000.

3 To enable *Dynamic AP Load Balancing* check the *Enable Dynamic AP Load Balancing* box and configure the parameters below:

Runtime/Schedule	Select Runtime or Schedule to determine when load balancing will run. If Runtime is selected, load balancing will initiate anytime a new active controller is added to the redundancy group. If Schedule is selected you can configure a start date and time to execute load balancing. This feature is not available when Dynamic Load Balancing is enabled.
Start Date	If Schedule is selected as the load balancing mode, enter a start date for load balancing to take place.
Start Time	If Schedule is selected as the load balancing mode, enter a start time for load balancing to take place.
Interval	If Schedule is selected as the load balancing mode, enter an interval (in days) for how often load balancing should take place. The valid range is between 1 and 180 days.
MU Threshold	The MU threshold specifies the number of minimum number of active MUs on an AP to stop the AP from resetting for load balancing.

4 Once Dynamic Load Balancing parameters are set, click the *Dynamic AP LB Now* button to run Dynamic AP Load Balancing.

5 Managing clustering in the Web UI is done through the *Cluster GUI* feature. Check the *Enable Cluster GUI* checkbox to enable this feature. The *Cluster GUI* feature updates many key screens in the Web UI allowing you to see APs and MUs managed by all active members of a cluster.

6 Refer to the *History* field to view the current state of the redundancy group.

State	Displays the new state (status) of the redundancy group after a Trigger event has occurred.
Time	Displays the Timestamp (time zone specific) when the state change occurred.

Trigger	Displays the event causing the redundancy group state change on the controller.
Description	Displays a redundancy event description defining the redundancy group state change on the controller. Typical states include Redundancy Disabled or Redundancy Enabled.

- 7 Click *Apply* to save any changes to the screen. Navigating away from the screen without clicking the *Apply* button results in all the changes on the screen being discarded.
- 8 Click the *Revert* button to undo the changes to the screen and revert to the last saved configuration.

Reviewing Redundancy Status

The controller is capable of displaying the status of the collective membership of the cluster. Use this information to assess the overall health and performance of the group.



NOTE

When ETH2 of one of the group members is unplugged, the other members report that this member as gone, but an AP will continue to be adopted by the controller with no ETH2 connectivity.

To configure controller redundancy memberships:

- 1 Select *Services > Redundancy* from the main menu tree.

The Redundancy screen displays with the Configuration tab selected.

2 Select the *Status* tab.

SUMMIT® WM3600 CONTROLLER

Services > Redundancy

Configuration | **Status** | Member

Status			
Protocol Version	2.0	Controller running image version	4.2.1.0-008R
Redundancy state is	Disabled	Connectivity Status	n/a
AP Licenses in group	n/a	AP Licenses in Controller	16
AP46X0 in group	n/a	AP46X0 on this Controller	n/a
AP35X0/AP7131 in group	1	AP35X0/AP7131 on this Controller	1
Adoption capacity in group	n/a	Adoption capacity on this Controller	n/a
Rogue Access Points in group	n/a	Rogue Access Points on this Controller	n/a
Radios in group	n/a	Radios on this Controller	n/a
Self-healing Radios in group	n/a	Self-healing Radios on this Controller	n/a
Mobile Units in group	n/a	Mobile Units on this Controller	n/a
DHCP Server in group	n/a		

Apply Revert Help

3 Refer to the *Status* field to assess the current state of the redundancy group.

Protocol Version	The Protocol Version is one of the parameters used to determine whether two peers can form a group. The Protocol Version should be set to an identical value for each controller in the redundancy group.
Redundancy state is	Displays the state of the redundancy group. When the redundancy feature is disabled, the state is “Disabled.” When enabled, it goes to a “Startup” state. From “Startup” it goes to a “Discovery” state immediately if the STP convergence is not enabled. Otherwise, it remains in “Startup” for a period of 50 seconds (the standard STP convergence time). During the discover state, the controller exchanges heartbeats and update messages to discover other members and define the redundancy group license. After discerning memberships, it moves to an Active state. There is no difference in state execution for Primary and Standby modes.
AP Licenses in group	Displays the number of Access Ports that can be adopted in the redundancy group. This value is calculated when a member starts-up, is added, is deleted or a license changes (downgrade and upgrade.) This value is equal to the highest license level of its members. It is NOT the sum of the license level of its members. For information on licensing rules impacting redundancy group members, see “Redundancy Group License Aggregation Rules” on page 357.

Access Ports in group	Displays the total number of Access Ports adopted by the entire membership of the redundancy group.
Adaptive Access Ports in group	Displays the combined number of adaptive access ports in the redundancy group.
Adoption capacity in group	Displays the combined AP adoption capability for each controller radio comprising the cluster. Compare this value with the adoption capacity on this controller to determine if the cluster members have adequate adoption capabilities.
Rogue Access Ports in group	Displays the cumulative number of rogue APs detected by the members of the group. Compare this value with the number of rogues detected by this AP to discern whether an abundance of rogues has been located by a particular controller and thus escalates a security issue with a particular controller.
Radios in group	Displays the combined number (sum) of radios amongst all the members of the redundancy group.
Self-healing radios in group	Displays the number of radios within the cluster that have self-healing capabilities enabled. Compare this value with the total number of radios within the group to determine how effectively the radios within the cluster can self-heal if problems exist.
Mobile Units in group	Displays the combined number of MU associations for the members of the redundancy group. Compare this number with the number of MUs on this controller to determine how effectively MU associations are distributed within the cluster.
DHCP Server in Group	Displays the total number of DHCP Servers available for DHCP resources for the combined cluster membership.
Controller running image version	Displays the version of the image running on the controller.
Connectivity Status	Displays the current connectivity status of the cluster membership.
AP Licenses in controller	Displays the number of licenses installed to adopt Access Ports on the current controller.
AAP Licenses in controller	Displays the number of licenses installed to adopt Adaptive Access Ports on the current controller.
Access Ports on this controller	Displays the total of the number of Access Ports adopted by this controller.
Adaptive Access Ports on this controller	Displays the combined number of Adaptive Access Ports on this controller.
Adoption capacity on this controller	Displays the AP adoption capability for this controller. Compare this value with the adoption capacity for the entire cluster to determine if the cluster members (or this controller) have adequate adoption capabilities. For information on licensing rules impacting redundancy group members, see "Redundancy Group License Aggregation Rules" on page 357 .
Rogue Access Ports on this controller	Displays the number of rogue APs detected by this controller. Compare this value with the cumulative number of rogues detected by the group to discern whether an abundance of rogues has been located by a particular controller and thus escalates a security issue.
Radios on this controller	Displays the number of radios used with this controller.
Self-healing radios on this controller	Displays the number of radios on this controller with self-healing enabled. Compare this value with the total number of radios within the group to determine how effectively radios can self-heal if problems exist.
Mobile Units on this controller	Displays the number of MUs currently associated with the radio(s) used with this controller. Compare this number with the number of MUs within the group to determine how effectively MUs are distributed within the cluster.

- The *Apply* and *Revert* buttons are unavailable for use with the Status screen, as there are no editable parameters to save or revert.

Configuring Redundancy Group Membership

The redundancy group should be disabled before conducting an Add/Delete operation. There are a minimum of 2 members needed to comprise a Redundancy Group, including the initiating controller

To configure controller redundancy memberships:

- Select *Services > Redundancy* from the main menu tree.
The Redundancy screen displays with the Configuration tab selected.
- Select the *Member* tab.

SUMMIT® WM3600 CONTROLLER

Services > Redundancy

Configuration | Status | Member

Redundancy Members

Number of members established: 0

IP Address	Status	Last Seen	AP46X0 Adoption Count	AP35X0/AP7131 Adoption Count	AP License Count	Mode
------------	--------	-----------	-----------------------	------------------------------	------------------	------

Details Delete Add Help

Save Logout Refresh

- Refer to the following information within the Member tab:

IP Address Displays the IP addresses of the redundancy group member.

Status	<p>Displays the current status of this group member. This status could have the following values:</p> <ul style="list-style-type: none"> • <i>Configured</i>—The member is configured on the current wireless service module. • <i>Seen</i>—Heartbeats can be exchanged between the current controller and this member. • <i>Invalid</i>—Critical redundancy configuration parameter(s) of the peer (heartbeat time, discovery time, hold time, Redundancy ID, Redundancy Protocol version of this member) do not match this controller's parameters. • <i>Not Seen</i>—The member is no longer seen by this controller. • <i>Established</i>—The member is fully established with this current module and licensing information already been exchanged between this controller and the member. • <i>Unknown</i>—No status information could be obtained.
Last Seen	Displays the time when this member was last seen by the controller.
AP Adoption Count	Displays the number of Access Ports adopted by this member.
AAP Adoption Count	Displays the number of Adaptive APs adopted by this member.
AP License Count	Displays the number of Access Port licenses installed on this member.
AAP License Count	Displays the number of Adaptive AP licenses installed on this member.
Mode	The Redundancy Mode could be Active or Standby depending on the mode configuration on the member. Refer to the Configuration screen to change the mode.

- 4 Select a row, and click the *Details* button to display additional details for this member. For more information, see [“Displaying Redundancy Member Details” on page 354](#).
- 5 Select a row and click the *Delete* button to remove a member from the redundancy group. The redundancy group should be disabled before conducting an Add or Delete operation.
- 6 Click the *Add* button to add a member to the redundancy group. The redundancy group should be disabled to conduct an Add or Delete operation. For more information, see [“Adding a Redundancy Group Member” on page 356](#).

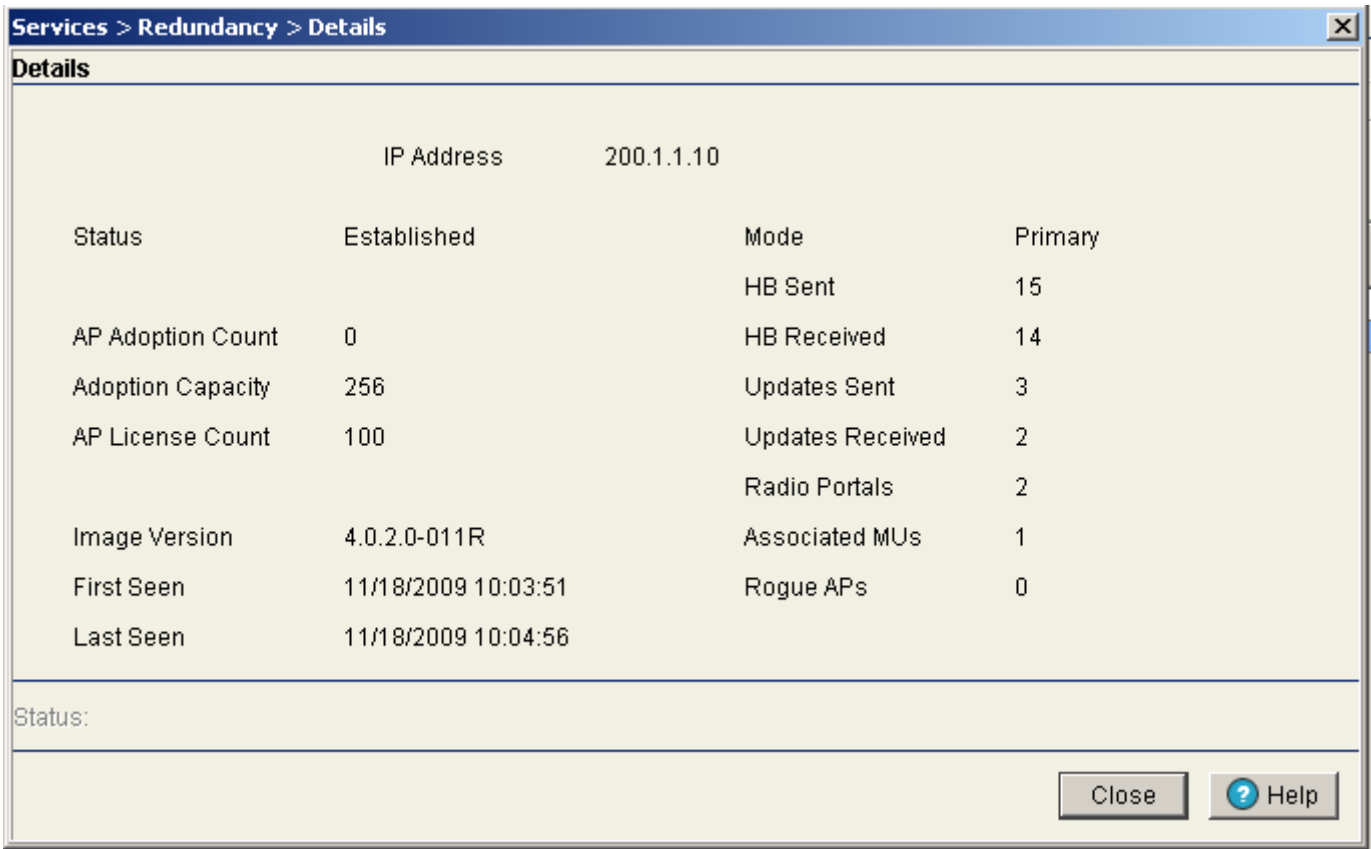
Displaying Redundancy Member Details

Use the *Details* screen (in conjunction with its parent Member screen) to display additional (more detailed) information on the group member selected within the Member screen.

To review the details:

- 1 Select *Services > Redundancy* from the main menu tree.
The Redundancy screen displays with the Configuration tab selected.
- 2 Select the *Member* tab.

3 Highlight a member of the group and select the *Details* button.



4 Refer to the following redundancy member information:

IP Address	Displays the IP addresses of the members of the redundancy group. There are a minimum of 2 members needed to define a redundancy group, including this current module.
Status	<p>Displays the current status of this group member. This status could have the following values:</p> <ul style="list-style-type: none"> • <i>Configured</i>—The member is configured on the current wireless service module. • <i>Seen</i>—Heartbeats can be exchanged between the current controller and this member. • <i>Invalid</i>—Critical redundancy configuration parameter(s) of the peer (heartbeat time, discovery time, hold time, Redundancy ID, Redundancy Protocol version of this member) do not match this controller's parameters. • <i>Not Seen</i>—The member is no longer seen by this controller. <p><i>Established</i>—The member is fully established with this current module and licensing information already been exchanged between this controller and the member.</p>
Adoption Count	Displays the number of Access Ports/Points adopted by this member.
Adoption Capacity	Displays the maximum number of Access Ports/Points this member is licensed to adopt. For information on licensing rules impacting redundancy group members, see "Redundancy Group License Aggregation Rules" on page 357.

Mode	The Redundancy Mode could be Active or Standby depending on the mode configuration on the member. Refer to the Configuration screen to change the mode.
License Count	Displays the number of port licenses available for this controller. For information on licensing rules impacting redundancy group members, see “Redundancy Group License Aggregation Rules” on page 357 .
Image Version	Displays the image version currently running on this member. Is the selected version complementary with this controller’s version?
First Seen	Displays the time this member was first seen by the controller.
Last Seen	Displays the time this member was last seen by the controller.
HB Sent	Displays the number of heartbeats sent from the controller to this member since the last reboot of the controller.
HB Received	Displays the number of heartbeats received by the controller since the last reboot.
Updates Sent	Displays the number of updates sent from the controller since the last reboot. Updates include, authorization level, group authorization level and number of Access Ports/Points adopted.
Updates Received	Displays the number of updates received by the current controller from this member since the last reboot.
Radio Portals	Displays the number of radio portals detected on each redundancy member listed.
Associated MUs	Display the number of MUs associated with each member listed.
Rogue APs	Displays the number of Rogue APs detected by each member. Use this information to discern whether these radios represent legitimate threats to other members of the redundancy group.
Self Healing Radios	Displays the number of self healing radios on each detected member. These radios can be invaluable if other radios within the redundancy group were to experience problems requiring healing by another radio.

5 Refer to the *Status* field.

The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.

6 Click *Close* to close the dialog without committing updates to the running configuration.

Adding a Redundancy Group Member

Use the *Add* screen as the means to add a new member (by adding their IP address) to an existing redundancy group (cluster).

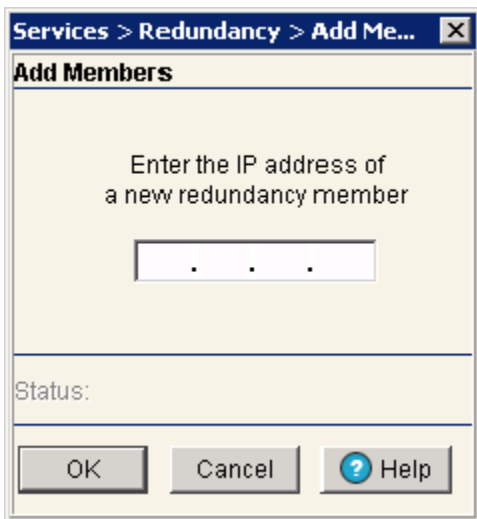
To add a new member to a redundancy group:

1 Select *Services > Redundancy* from the main menu tree.

The *Redundancy* screen displays with the *Configuration* tab selected.

2 Select the *Member* tab.

- 3 Select the *Add* button.



- 4 Enter the IP Address of a new member.
- 5 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 6 Refer to the *Status* field.

The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Redundancy Group License Aggregation Rules

The following are rules governing license usage among members of a redundancy group:

- A redundancy group license is determined by adding individual controller licenses.
- Do not allow different port speed/duplex settings on members. Each members should have the settings.
- In a redundancy group of three controllers (S1, S2 and S3), if S1 has X licenses, S2 has Y licenses and S3 has Z licenses, the license count is X+Y+Z (the aggregation of each controller).
- A cluster license is re-calculated whenever a new controller brings existing licenses to a group or an existing controller’s license value changes (increases or decreases).
- A simple controller reboot will not initiate a new cluster license calculation, provided the re-booted controller does not come up with different installed license.
- A change to an installed license during runtime initiates a cluster license calculation.
- If an existing redundancy group member goes down, it will not initiate a cluster license calculation.
- Whenever the cluster protocol is disabled, a member controller forgets the learned cluster license as well as peer information needed to compute license totals.
- If the controller start-up configuration is removed, a member controller forgets the learned cluster license as well as peer information needed to compute license totals.
- If adding a new controller (with zero or non-zero installed license) to a group with at least one license contributing controller down, the new group member will receive a different cluster license value.

For example, for a cluster of three controllers (S1 = 6, S2 = 6 and S3 = 6 licenses), the group license count is 18. If S1 goes down, the license count is still 18, since the license calculation is not initiated if a member controller goes down. If S4 (with zero licenses) is introduced, S4 becomes part of the group (can exchange updates and other packets), but has license count of 12 (NOT 18), even though S2 and S3 still show a license count of 18. This should be an indicator a new member has been introduced during a period when the redundancy group is not operating with all its license contributing members.

Managing Clustering Using the Web UI

Managing clustering in the Web UI is done through the *Cluster GUI* feature. The Cluster GUI feature updates many key screens in the Web UI allowing you to see APs and MUs managed by all active members of a cluster.

To enable the Cluster GUI feature:

- 1 Select *Services > Redundancy* from the main menu tree

The *Redundancy* screen displays with the *Configuration* tab selected

SUMMIT® WM3600 CONTROLLER

Services > Redundancy

Configuration | Status | Member

Enable Redundancy

Redundancy Controller IP: 0 . 0 . 0 . 0 Mode: Primary Standby

Redundancy ID: 1 (1-65535) Discovery Period: 30 (10-60 sec)

Heartbeat Period: 5 (1-255 sec) Hold Time: 15 (10-255 sec)

Critical Resource: 0 . 0 . 0 . 0 Handle STP convergence Enable DHCP Redundancy

Auto Revert

After: 5 min. (1-1800)

Enable Dynamic AP Load Balance

Runtime Schedule Start Date: 06/01/2008 (MM/DD/YYYY)

MU Threshold: 32 Start Time: 00:00 (HH:MM) Enable Cluster GUI

Interval: 1 (1-366 days)

History

State	Time	Trigger	Description
Disabled	Mon May 03 11:28:36 2010 PDT	Disabled	Redundancy Disabled

- 2 Configure redundancy settings using the Command Line Interface or the using the Web UI as described in “[Configuring Redundancy Settings](#)” on page 347.

-
- 3 Add any redundancy group members using the Command Line Interface or using the Web UI as described in [“Configuring Redundancy Group Membership” on page 353](#).
 - 4 On the *Configuration* tab, check the Enable Redundancy checkbox and then check the *Enable Cluster GUI* box.
 - 5 Click the *Apply* button to enable the *Cluster GUI* feature.
 - 6 Once *Cluster GUI* is enabled a *Controller* field will be available in many of the Access Port/Point and mobile unit related screens. The *Controller* field displays which cluster members the APs and MUs are associated with identified by their IP address.



NOTE

When accessing the controller Web UI through a NATed interface the Cluster GUI features will only be accessible if TCP ports 80 and 161 are opened on the router or gateway.

Layer 3 Mobility

Refer to the following sections to configure Layer 3 Mobility:

- [Configuring Layer 3 Mobility on page 359](#)
- [Defining the Layer 3 Peer List on page 362](#)
- [Reviewing Layer 3 Peer List Statistics on page 363](#)
- [Reviewing Layer 3 MU Status on page 365](#)

Configuring Layer 3 Mobility

Layer 3 mobility is a mechanism enabling an MU to maintain the same Layer 3 address while roaming throughout a multi-VLAN network. This enables transparent routing of IP datagrams to MUs during their movement, so data sessions can be maintained while they roam (in for voice applications in particular). Layer 3 mobility maintains TCP/UDP sessions in spite of roaming among different IP subnets.

A mobility domain comprises of a network of controllers among which an MU can roam seamlessly without changing its IP address. Each controller in the mobility domain needs a mobility domain string identifier so MUs roaming between controllers can retain their Layer 3 address and maintain application-layer connectivity.

When an MU enters a mobility domain (by associating with a controller), it is first assigned a home controller. The home controller is responsible for assigning a VLAN for the MU and communicating the MU's mobility-related parameters to the other controllers in the mobility domain. The home controller does not change for the remainder of the MU's presence in the mobility domain. All data packets transmitted/received by the MU including DHCP and ARP are tunneled through the home controller. The IP address for the MU is assigned from the VLAN to which the MU belongs (as determined by the home controller).

The current controller is the controller in the mobility domain an MU is currently associated to. The current controller changes as the MU roams and establishes different associations. The current controller is responsible for delivering data packets from the MU to its home controller and vice-versa.



CAUTION

An AP4600 Series Access Port is required to have a DHCP provided IP address before attempting Layer 3 adoption, otherwise it will not work. Additionally, the Access Port must be able to find the IP addresses of the controllers on the network.

To locate controller IP addresses on the network:

- Configure DHCP option 189 to specify each controller IP address.
 - Configure a DNS Server to resolve an existing name into the IP of the controller. The Access Port has to get DNS server information as part of its DHCP information.
-

Key aspects of Layer 3 Mobility include:

- Seamless MU roaming between controllers on different Layer 3 subnets, while retaining the same IP address.
- Static configuration of mobility peer controllers.
- Layer 3 support does not require any changes to the MU. In comparison, other solutions require special functionality and software on the MU. This creates numerous inter-working problems with working with MUs from different legacy devices which do not support Layer 2 switching.
- Support for a maximum of 20 peers, each handling up to a maximum of 500 MUs.
- A full mesh of GRE tunnels can be established between mobility peers. Each tunnel is between a pair of controllers and can handle data traffic for all MUs (for all VLANs) associated directly or indirectly with the MU.
- Data traffic for roamed MUs is tunneled between controllers by encapsulating the entire Layer 2 packet inside GRE with a proprietary code-point.
- When MUs roam within the same VLAN (Layer 2 Roaming), the behavior is retained by re-homing the MU to the new controller so extra hops are avoided while forwarding data traffic.
- MUs can be assigned IP addresses statically or dynamically.
- Forward and reverse data paths for traffic originating from and destined to MUs that have roamed from one Layer 3 subnet to another are symmetric.



NOTE

When using Layer 3 Mobility ensure that TCP traffic on port 58788 is allowed on the network(s) where mobile units will be roaming from and to.

To configure Layer 3 Mobility for the controller:

- 1 Select *Services > Layer 3 Mobility* from the main menu tree.

The *Layer 3 Mobility* screen appears with the *Configuration* tab displayed.

SUMMIT® WM3600 CONTROLLER

Services > Layer 3 Mobility

Configuration | Peer List | Peer Statistics | MU Status

Use Default Management Interface 10.255.108.36

Use this Local Address Roam Interval (1-300 secs.)

Enable Mobility

<input type="checkbox"/> test-open-1x	<input type="checkbox"/> test-open-hotspot	<input type="checkbox"/> test-4600an-local
<input type="checkbox"/> test-4600bgn-local	<input type="checkbox"/> test-3510a-local	<input type="checkbox"/> test-3510bg-local
<input type="checkbox"/> 107	<input type="checkbox"/> 108	<input type="checkbox"/> 109
<input type="checkbox"/> 110	<input type="checkbox"/> 111	<input type="checkbox"/> 112
<input type="checkbox"/> 113	<input type="checkbox"/> 114	<input type="checkbox"/> 115
<input type="checkbox"/> 116	<input type="checkbox"/> 117	<input type="checkbox"/> 118
<input type="checkbox"/> 119	<input type="checkbox"/> 120	<input type="checkbox"/> 121
<input type="checkbox"/> 122	<input type="checkbox"/> 123	<input type="checkbox"/> 124
<input type="checkbox"/> 125	<input type="checkbox"/> 126	<input type="checkbox"/> 127
<input type="checkbox"/> 128	<input type="checkbox"/> 129	<input type="checkbox"/> 130
<input type="checkbox"/> 131	<input type="checkbox"/> 132	

All WLANs On | All WLANs Off | Apply | Revert | Help

- 2 Select the *Use Default Management Interface* checkbox to use the controller's default management interface IP address for MUs roaming among different Layer 3 subnets. The IP address displayed to the right of the checkbox is used by Layer 3 MU traffic.
- 3 If wanting to use a local IP addresses (non controller management interface) for MUs roaming amongst different Layer 3 subnets, select the *Use this Local Address* checkbox and enter an IP address.
- 4 Use the *Roam Interval* to define maximum length of time MUs within selected WLAN are allowed to roam among different subnets.
- 5 Refer to the table of WLANs and select the checkboxes of those WLANs you wish to enable Layer 3 mobility for.

Once the settings are applied, MUs within these WLANs can roam among different subnets.

- 6 Select the *Enable Mobility* checkbox to enable an MU to maintain the same Layer 3 address while roaming throughout a multi-VLAN network.
- 7 Select the *All WLANs On* button to enable mobility for each WLAN listed.

If unsure if you want to enable mobility for each WLAN, manually select just those you want to enable.

- 8 Select the *All WLANs Off* button to disable mobility for each WLAN listed.
- 9 Click the *Apply* button to save the changes made within this screen. Clicking Apply overwrites the previous configuration.
- 10 Click the *Revert* button to disregard any changes made within this screen and revert back to the last saved configuration.

Defining the Layer 3 Peer List

The Layer 3 Peer List contains the IP addresses MUs are using to roam among various subnets. This screen is helpful in displaying the IP addresses available to those MUs requiring access to different subnet resources.

To define the Layer 3 Peer List:

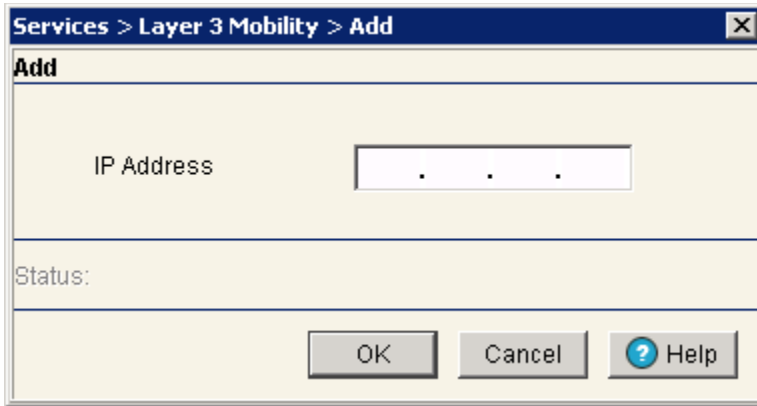
- 1 Select *Services > Layer 3 Mobility* from the main menu tree.
The *Layer 3 Mobility* screen appears with the Configuration tab displayed.
- 2 Select the *Peer List* tab.

The screenshot displays the Summit WM3600 Controller web interface. The left sidebar shows the navigation menu with 'Layer 3 Mobility' selected under the 'Services' category. The main content area is titled 'Services > Layer 3 Mobility' and has tabs for 'Configuration', 'Peer List', 'Peer Statistics', and 'MU Status'. The 'Peer List' tab is active, showing a table with columns for 'IP Address' and 'Session Status'. A 'Show Filtering Options' link is visible above the table. At the bottom of the table area, it says 'Filtering is disabled'. The interface includes a 'Login Details' section with 'Connect To: 10.255.108.36' and 'User: admin', and a 'Message' section. At the bottom, there are buttons for 'Save', 'Logout', 'Refresh', 'Delete', 'Add', and 'Help'.

- 3 Refer to the contents of the Peer List for existing IP addresses and Layer 3 MU session status.

Use this information to determine whether a new IP address needs to be added to the list or an existing address needs to be removed.

- 4 Select an IP address from those displayed and click the *Delete* button to remove the address from the list available for MU Layer 3 roaming among subnets.
- 5 Click the *Add* button to display a screen used for adding the IP address to the list of addresses available for MU Layer 3 roaming.



The screenshot shows a dialog box titled "Services > Layer 3 Mobility > Add". The dialog has a title bar with a close button (X). Below the title bar, the word "Add" is displayed. The main area contains a label "IP Address" followed by a text input field with three dots (.) inside, indicating a dotted decimal IP address format. Below the input field is a "Status:" label. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

Enter the IP addresses in the area provided and click the *OK* button to add the addresses to the list displayed within the *Peer List* screen.

Reviewing Layer 3 Peer List Statistics

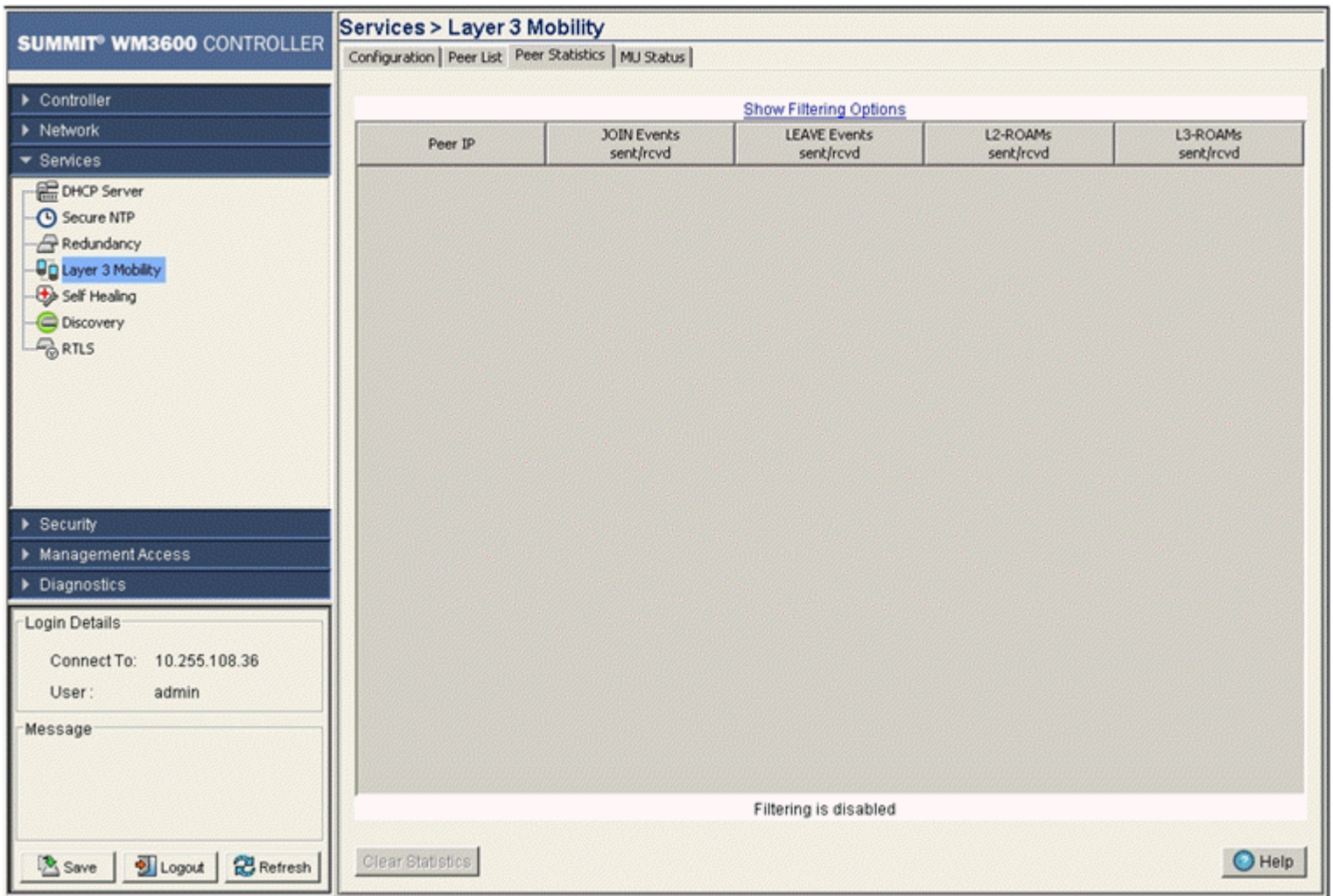
When an MU roams to a current controller on the same Layer 3 network, it sends a L2-ROAM message to the home controller to indicate the MU has roamed within the same VLAN. The old home controller forwards the information to all its peers. The MU is basically re-synchronized to the new current controller, but keeps its old IP address. The same procedure is followed, even if the new current controller is on a different Layer 3 subnet, but uses the same VLAN ID (overlapping VLAN scenario).

Tracking these message counts is important to gauge the behavior within the mobility domain. The Layer 3 Mobility screen contains a tab dedicated to tracking the message sent between the current controller, home controller and MU.

To view Layer 3 peer statistics:

- 1 Select *Services > Layer 3 Mobility* from the main menu tree.
The *Layer 3 Mobility* screen appears with the Configuration tab displayed.

2 Select the *Peer Statistics* tab.



3 Refer to the following information within the Peer Statistics tab:

Peer IP	Displays the IP addresses of the peer controllers within the mobility domain. Each peer can support up to 500 MUs.
JOIN Events sent/rcvd	Displays the number of JOIN messages sent and received. JOIN messages advertise the presence of MUs entering the mobility domain for the first time. When an MU (currently not present in the MU database) associates with a controller, it immediately sends a JOIN message to the host controller with MAC, VLAN and IP information (both current and home controller IP info). The home controller forwards the JOIN to all its peers (except the one from which it received the original message). JOIN messages are always originated by the current controller. JOIN messages are also used during the home controller selection phase to inform a candidate home controller about an MU. The current controller selects the home controller (based on its local selection mechanism) and sends a JOIN message to the home controller that is forwarded to all its peers.

LEAVE Events sent/rcvd	Displays the number of LEAVE messages sent and received. LEAVE messages are sent when the controller decides an MU originally present in the MU database is no longer present in the mobility domain. The criterion to determine the MU has actually left the network is implementation specific. The current controller sends the LEAVE message with the MU's MAC address information to the home controller, which eventually forwards the message to each mobility peer.
L2-ROAMs sent/rcvd	Displays the number of Layer 2 ROAM messages sent and received. When an MU roams to a new controller on a different layer 3 network (MU is mapped to a different VLAN ID), it sends a L3-ROAM message to the home controller with the new IP information for the current controller it is associated with. The L3-ROAM message is then forwarded by the home controller to each peer.
L3-ROAMs sent/rcvd	Displays the number of Layer 3 ROAM messages sent and received. When an MU roams to a new current controller (on the same layer 3 subnet as the old current controller), it sends a L2-ROAM message to the old home controller with the new home controller-IP and current controller-IP information. This L2-ROAM message is then forwarded by the old home controller to each peer.

- 4 Click the *Clear Statistics* button to remove the data displayed for the selected peer IP address.

Reviewing Layer 3 MU Status

The Layer 3 Mobility *MU Status* tab displays a set of MU stats for associated MUs within the mobility domain. Use the MU status information to familiarize yourself with these MUs and their mobility-related parameters to distinguish new MUs entering the network from existing MUs roaming within the mobility domain.

To view Layer 3 mobility MU statistics:

- 1 Select *Services > Layer 3 Mobility* from the main menu tree.

The *Layer 3 Mobility* screen appears with the Configuration tab displayed.

- 2 Select the *MU Status* tab.

The screenshot displays the Summit WM3600 Controller web interface. The left sidebar shows a navigation menu with categories: Controller, Network, Services, Security, Management Access, and Diagnostics. Under Services, options include DHCP Server, Secure NTP, Redundancy, Layer 3 Mobility (highlighted), Self Healing, Discovery, and RTLS. The main content area is titled 'Services > Layer 3 Mobility' and contains tabs for Configuration, Peer List, Peer Statistics, and MU Status (selected). Below the tabs is a 'Show Filtering Options' link and a table with columns: MU MAC, MU IP Addr, Home Ctr IP, Home Ctr VLAN, Curr Ctr IP, and Room. The table is currently empty. At the bottom of the table area, it says 'Filtering is disabled'. The interface also includes a 'Login Details' section with 'Connect To: 10.255.108.36' and 'User: admin', a 'Message' field, and buttons for Save, Logout, Refresh, and Help.

Configuring Self Healing

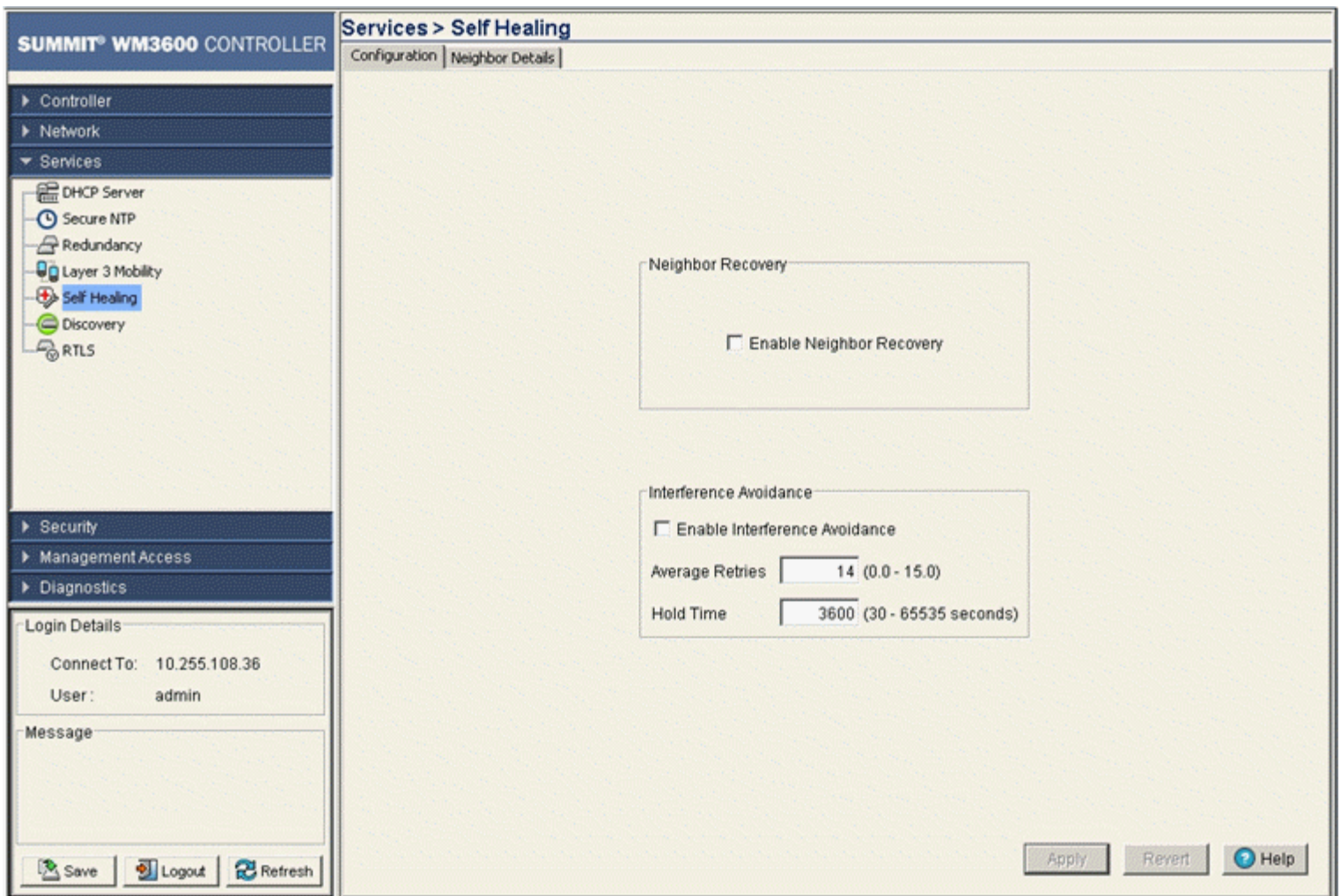
The controller supports a feature called *Self Healing* that enables radios to take corrective action when one or more radios fail. To enable the feature the user must specify radio neighbors that would self heal if either one goes down. The neighbor radios do not have to be of the same type. Therefore, an 11bg radio can be the neighbor of an 11a radio and either of them can self heal when one of them fails.

The controller initiates self healing when it loses communication with the Access Port or when another radio (configured in detector mode) informs the controller a particular radio is not transmitting beacons.

To configure self-healing on the controller:

- 1 Select *Services > Self Healing* from the main menu tree.

The Self Healing page launches with the *Configuration* tab displayed.



- 2 Select the *Enable Neighbor Recovery* checkbox.

Enabling Neighbor Recovery is required to conduct manual neighbor detection.

- 3 Refer to the Interference Avoidance field to define the following settings:

Enable Interference Avoidance	When enabled, the controller is capable of controlling channels on an Access Port (<i>Automatic Channel Selection</i>) if interference is observed on the current operating channel.
Average Retries	Displays the average number of retries for an MU to communicate with a neighbor radio. Define a retry value between 0.0 and 15.0 retry attempts. Average Retries is a threshold value, when exceeded ACS is initiated.
Hold Time	Set the interval (in seconds) that disables interference avoidance after detection. The hold time prevents the radio from re-running ACS continuously.

- 4 Click the *Apply* button to save the changes made within this screen. Clicking Apply overwrites the previous configuration.

- Click the *Revert* button to disregard any changes made within this screen and revert back to the last saved configuration.

Configuring Self Healing Neighbor Details

The Neighbor Details page displays all the radios configured on the controller and their neighbor designations.

To configure self-healing on the controller:

- Select *Services > Self Healing* from the main menu tree.
The Self Healing page launches with the *Configuration* tab displayed.
- Select the *Neighbor Details* tab.

SUMMIT® WM3600 CONTROLLER

Services > Self Healing

Configuration Neighbor Details

Neighbor recovery is currently **disabled**.
Enable Neighbor recovery and then click on 'Detect Neighbors' to perform automatic 'Neighbor Detection'.

Show Filtering Options

Radio	Description	Type	AP Mac Address	Action	Neighbor Radio Indices
1	RADIO1	802.11bgn	00-04-96-44-51-8C	Both	None
2	RADIO2	802.11an	00-04-96-44-51-8C	Both	None
3	RADIO3	802.11bg	00-04-96-43-50-70	Both	None
4	RADIO4	802.11a	00-04-96-43-50-70	Both	None

Filtering is disabled

Edit Remove Neighbors Detect Neighbors Help

The top right-hand corner displays whether neighbor recovery is currently enabled or disabled. To change the state, click the *Enable Neighbor Recovery* checkbox within the Configuration tab.

- Refer to the following information as displayed within the Neighbor Recovery screen.

Radio Index Displays a numerical identifier used (in conjunction with the radio's name) to differentiate the radio from its peers.

Description	Displays a text description used (in conjunction with the radio's index) to differentiate the radio from its peers.
Type	Displays the radio as either a 802.11a or 802.11bg or 802.11an and 802.11bgn radio.
AP Mac Address	Displays the Ethernet MAC address of the Access Port. Use the Access Port MAC Address for the addition or deletion of the radio.
Action	Displays the self healing action configured for the radio. Options include: <ul style="list-style-type: none"> • <i>Raise Power</i>—The transmit power of the radio is increased when a neighbor radio is not functioning as expected. • <i>Open Rates</i>—Radio rates are decreased to support all rates when a neighbor radio is not functioning as expected. • <i>Both</i>—Increases power and increases rates when a neighbor radio is not functioning as expected. • <i>None</i>—No action is taken when a neighbor radio is not functioning as expected.
Neighbor Radio Index	Displays the indexes of the radio's neighbors.

- 4 Highlight an existing neighbor and click the *Edit* button to launch a screen designed to modify the self healing action and/or neighbors for the radio. For more information, see [“Editing the Properties of a Neighbor” on page 369](#).
- 5 Select the *Remove Neighbors* button to remove all neighbors from the selected radio's neighbor list.
- 6 Click the *Detect Neighbors* button to auto-determine neighbors for the radios.



NOTE

The Detect Neighbors button is enabled only when the Enable Neighbor Recovery checkbox is selected from within the Configuration tab. Ensure this option has been enabled before trying to detect neighbors.

Enabling this feature automatically makes each radio disassociate with their attached MUs, clear the current neighbor list and move into detection mode to detect neighboring radios.

Neighbor detection works best if all radios are configured and adopted. Starting the automatic neighbor detection feature disassociates MUs and clears the current neighbor configuration.

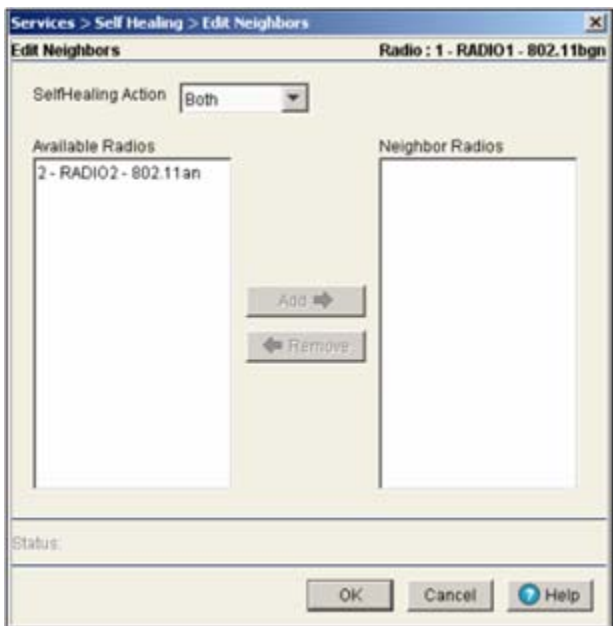
Editing the Properties of a Neighbor

Use the *Edit* screen to specify the neighbor of a selected radio and the action the radio performs in the event its neighbor radio fails.

To edit the properties of a neighbor:

- 1 Select *Services > Self Healing* from the main menu tree.
- 2 Select the *Neighbor Details* tab.

- 3 Select an existing neighbor and click the *Edit* button.



The radio index and description display in the upper right corner of the screen. The *Available Radios* value represents the radios that can be added as a neighbor for the target radio. *Neighbor Radios* are existing radios (neighbors).

- 4 Select one of the following four actions from the Self Healing Action drop-down menu:
 - *None*—The radio takes no action at all when its neighbor radio fails.
 - *Open Rates*—The radio will default to factory-default rates when its neighbor radio fails.
 - *Raise Power*—The radio raises its transmit power to the maximum provided its power is lower than the maximum permissible value.
 - *Both*—The radio will open its rates as well as raise its power.
- 5 Click the *Add* -> button to move a radio from the Available Radios list to the Neighbor Radios list. This dedicates neighbors for this radio.
- 6 Select a radio and click <- *Remove* to move the radio from the Neighbor Radios list to the Available Radios list.
- 7 Refer to the *Status* field for an update of the edit process.

The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to save the changes to the running configuration and close the dialog.
- 9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Controller Discovery

Controller discovery enables the SNMP discovery (location) of devices. To discover devices in the specified range of IP addresses, the controller Web UI sends SNMP GET requests (using the user specified SNMP v2 or v3 version) to all IP addresses on the specified network. The results of the

discovery are helpful for isolating devices compatible for operation with the locating controller, thus extending the potential coverage area and MU support base within the controller managed network.

Use the *Discovery Profiles* tab to view existing SNMP search profiles using a user defined range of IP addresses. Existing profiles can be modified or deleted and new profiles can be added as needed. Refer to the *Recently Found Devices* tab to view a table of devices discovered by the current discovery process. Each discovered device compatible with the locating controller is displayed in a shaded color to distinguish it from non-compatible devices.



CAUTION

Controller discovery can be a time consuming operation. However, the controller discovery operation is a standalone process. This allows users to perform other configuration operations when discovery is running in the background.

Configuring Discovery Profiles

To configure controller discovery:

- 1 Select *Services > Discovery* from the main menu tree.

The *Discovery* page launches with the *Discovery Profiles* tab displayed.

The screenshot shows the Summit WM3600 Controller web interface. The left-hand navigation menu includes sections for Controller, Network, Services, Security, Management Access, and Diagnostics. Under Services, the following options are listed: DHCP Server, Secure NTP, Redundancy, Layer 3 Mobility, Self Healing, Discovery (highlighted), and RTLS. Below the navigation menu is a 'Login Details' section with 'Connect To: 10.255.108.36' and 'User: admin'. A 'Message' section is also present. The main content area is titled 'Services > Discovery' and has two tabs: 'Discovery Profiles' (selected) and 'Recently Found Devices'. The 'Discovery Profiles' tab displays a table with the following columns: Index, Profile Name, Start IP Address, End IP Address, and SNMP Version. The table is currently empty. Below the table are buttons for 'Edit', 'Delete', 'Add', and 'Start Discovery'. A 'Help' icon is located in the bottom right corner of the main content area.

- 2 Refer to the following information within the Discovery Profiles tab to discern whether an existing profile can be used as is, requires modification (or deletion) or if a new discovery profile is required.

Index	Displays the numerical identifier used to differentiate this profile from others with similar configurations. The index is supplied to new profiles sequentially.
Profile Name	Displays the user-assigned name for the profile. The profile name should associate the profile with the group of devices or area where the discovered devices are anticipated to be located.
Start IP Address	Displays the starting numeric (non DNS) IP address from where the search for available network devices is conducted.
End IP Address	Displays the ending numeric (non DNS) IP address from where the search for available network devices is conducted.
SNMP Version	Displays the version of the SNMP (either SNMP v2 or v3) used for discovering available network devices.

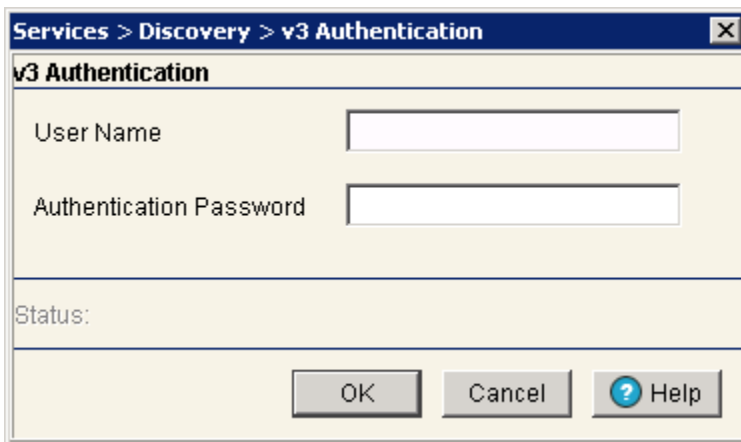
- 3 Select an existing profile and click the *Edit* button to modify the profile name starting and ending IP address and SNMP version. Extreme Networks recommends editing a profile only if some of its attributes are still valid, if the profile is obsolete, delete it and create a new one.
- 4 Select an existing profile and click the *Delete* button to remove this profile from the list of available profiles.
- 5 Click the *Add* button to display a screen used to define a new controller discovery profile. For more information, see [“Adding a New Discovery Profile” on page 374](#).
- 6 Click the *Start Discovery* button to display a *Read Community String* (SNMP v2) or *V3 Authentication* (SNMP v3) screen.

When Start Discovery is selected, the controller prompts the user to verify their SNMP credentials against the SNMP credentials of discovered devices. SNMP v2 and v3 credentials must be verified before the controller displays discovered devices within the Recently Found Devices table.

If SNMP v2 is used with a discovering profile, a *Read Community String* screen displays. The Community String entered is required to match the name used by the remote network management software of the discovered controller.



If SNMP v3 is used with a discovering profile, a *V3 Authentication* screen displays. The User Name and Password are required to match the name used by the remote network management software of the discovered controller.



When the credentials of the V2 Read Community or V3 Authentication screens are satisfied, the controller discovery process begins.

- 7 If necessary, click the *Stop Discovery* button (enabled only during the discovery operation) to stop the discovery operation.

Adding a New Discovery Profile

If the contents of an existing profile are no longer relevant to warrant modification using the Edit function, then a new controller discovery profile should be created

To create a new controller discovery profile:

- 1 Select *Services > Discovery* from the main menu tree.
- 2 Click the *Add* button at the bottom of the screen.

- 3 Define the following parameters for the new controller discovery profile:

Profile Name	Define a user-assigned name used to title the profile. The profile name should associate the profile with the group of devices or area where the discovered devices should be located.
Start IP Address	Enter the starting numeric (non DNS) IP address from where the search for available network devices is conducted.
End IP Address	Enter the ending numeric (non DNS) IP address from where the search for available network devices is conducted
SNMP Version	Use the drop-down menu to define the SNMP version (either v2 or v3) used for discovering available network devices.

- 4 Refer to the *Status* field for an update of the edit process.

The Status is the current state of the requests made from the applet. Requests are any “SET/GET” operation from the applet. The Status field displays error messages if something goes wrong in the transaction between the applet and the controller.

- 5 Click *OK* to save the changes to the running configuration and close the dialog.
- 6 Click *Cancel* to close the dialog without committing updates to the running configuration.

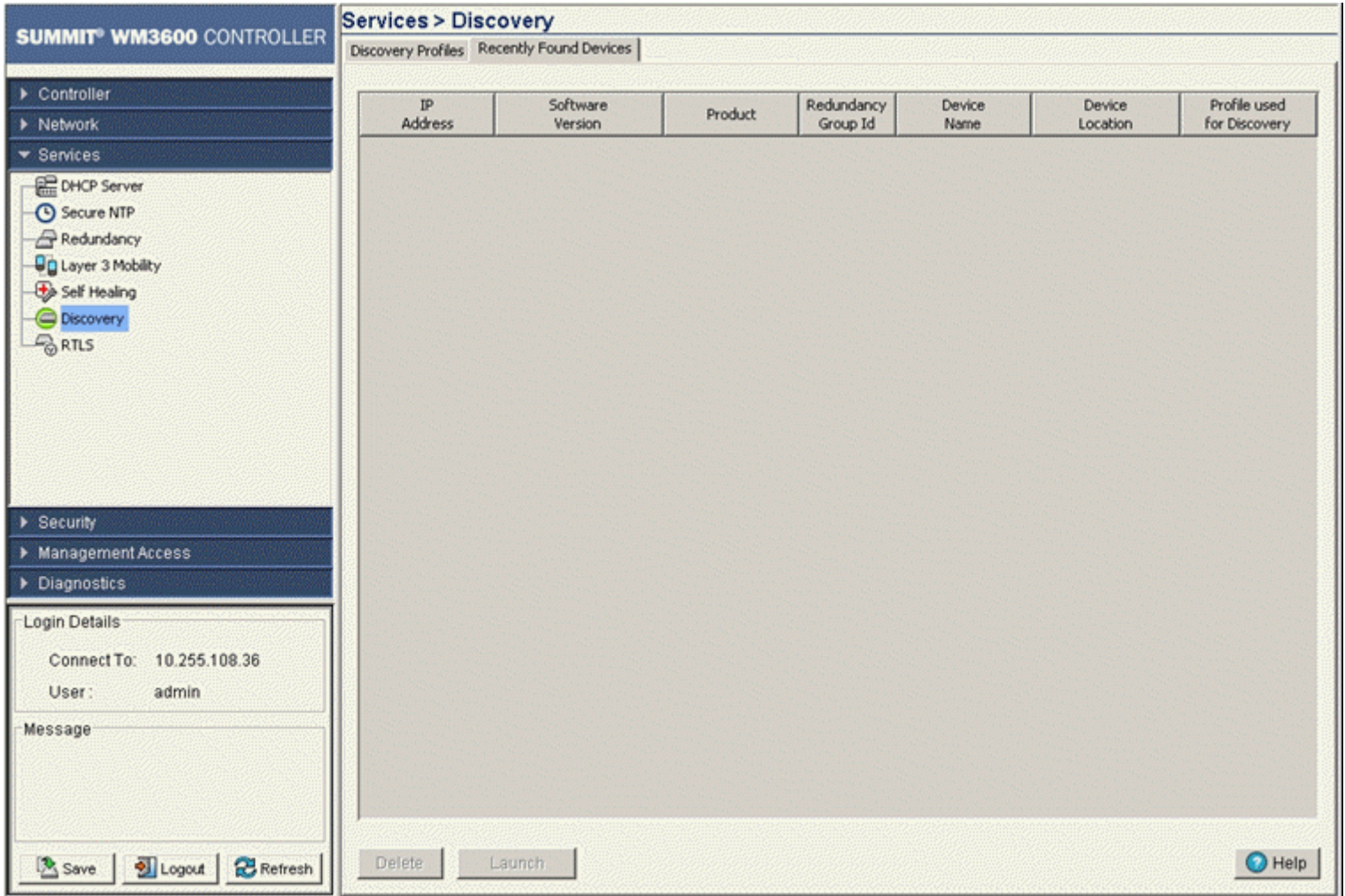
Viewing Discovered Controllers

Refer to the *Recently Found Devices* tab to view a table of devices found by the discovery process. Each discovered device compatible with the locating controller is displayed in a shaded color to distinguish it

from non-compatible devices. The controller Web UI enables users display the Web UI of the discovered device in a separate browser window.

To view the devices located by the controller:

- 1 Select *Services > Discovery* from the main menu tree.
- 2 Select the *Recently Found Devices* tab.



- 3 Refer to the following within the Recently Found Devices screen to discern whether a located device should be deleted from the list or selected to have its Web UI launched and its current configuration modified.

IP Address	Displays the IP address of the discovered controller. This IP address obviously falls within the range of IP addresses specified for the discovery profile used for the device search. If the IP addresses displayed do not meet your search expectations, consider creating a new discovery profile and launching a new search.
Software Version	Displays the software version running on the discovered device.
Product	Displays the name of the device discovered by the device search. If the list of devices discovered is unsatisfactory, consider configuring a new discovery policy and launching a new search.

Redundancy Group ID	If the discovered device is part of a redundancy group, its cluster ID displays within this column. The Redundancy ID would have been assigned using the Controller > Redundancy screen.
Device Name	Displays the device name assigned to the discovered device. This name would have been assigned using the Controller > Configuration screen.
Device Location	Displays the device location defined to the discovered device. The location would have been assigned using the Controller > Configuration screen.
Profile used for Discovery	Displays the profile selected from within the Discovery Profiles tab and used with the Start Discovery function to discover devices within the controller managed network. If the group of devices discovered and displayed within the Recently Found Devices tab does not represent the device demographic needed, consider going back to the Discovery Profiles tab and selected a different profile for the controller discovery process.

- 4 If a discovered controller is of no interest, select it from among the discovered devices displayed and click the *Delete* button.

Once removed, the located device cannot be selected and its Web UI displayed.

- 5 Select a discovered device from among those located and displayed within the Recently Found Devices screen and click the *Launch* button to display the Web UI for that controller.



CAUTION

When launching the Web UI of a discovered device, take care not to make configuration changes rendering the device ineffective in respect to its current configuration.

Locationing

The Summit WM Geofencing Architecture provides a very comprehensive and elegant solution for physical security to wireless without impacting the mobility. The Summit WM Wireless ACLs allow protection based on the MAC address and location of clients within user defined boundaries. This solution provides protection within user defined boundaries, allowing access to clients located within the zone and denying and mitigating access to clients outside the zone.

The Extreme Networks Geofencing architecture provides a dynamic solution by locating all clients and enforcing ACLs for each client based on it's current location. This capability is no easy feat and is only made possible with the following three core components of the Summit WM architecture which closely interact to provide physical security without compromising mobility.

The core components of the Summit WM Geofencing solution are:

- Industry's only Native RTLS Engine
- Wireless ACLs
- Controller Management (CLI, SNMP and Applet)

RTLS Engine. The native RTLS engine is a software module on the Summit WM architecture based wireless controllers. The RTLS engine locates thousands of clients in real time and provides the current location for each client

Wireless ACLs. The Wireless ACL in Summit WM uses location as a credential and as such is designed to enforce admission policies based on the current location of the client. By default all clients are allowed admission in all zones and the Wireless ACLs can be configured to deny admission to a single MAC address (client) or a group of clients for each defined zone.

Controller Management (CLI, SNMP or Applet). Controller Management plays a key role in defining and configuring the multiple Geofencing zones. This includes configuration of site parameters including site dimensions, zones and Access Point locations.

Each zones perimeter must include a minimum of 3 points and must not exceed 16 points. Additionally the zones perimeter must not overlap another defined zone. Each Zone is assigned a ZoneID which is in turn used in creating the ACLs which will deny admission within that specific zone.

RTLS Overview

Locationing (also called Real Time Location-based Services and Real Time Location Application Services) delivers end-user applications based on:

- The location of mobile devices (devices with location enabling technology, such as a WiFi supported handheld, Wi-Fi laptop or cell phone)
- The location of an attached tag (a location enabled mobile device in miniaturized form, for example a WiFi tag, UWB tag or RFID tag that is attached to a person, vehicles or a package)

An Extreme Networks wireless LAN controllers (such as a Summit WM3700) can facilitate true RF technology-agnostic mobility, allowing customers to view, manage and troubleshoot their RF network (Wi-Fi, RFID, UWB, mesh etc.) and provide accurate asset locationing information across multiple networks in real-time. This solution can also be packaged as a locationing appliance.

SOLE—Smart Opportunistic Location Engine

SOLE is an on-board location engine using a combination of innovative algorithms to determine location based on asset type. SOLE fuses the location information reported by several technologies into one seamless environment to get more meaningful results.

SOLE helps locate assets (including rogues) including passive tags, semi-passive tags, active tags (UWB,802.11, RFID etc) and MUs. SOLE returns the location of passive tags as seen by mobile RFID readers (like a MC9090) by combining the 802.11 reader's location with RFID antenna direction/location data.

Applications (users) inform SOLE (Summit WM3000 Series Controller) about a facility map, location of infrastructure and zones. A zone is an area of specific interest with respect to whenever an asset becomes visible or invisible in that area.

SOLE uses the following input variables as needed for the specific tag type calculating location:

- User configurations
- RSSI propagation based on facility layout and RF barriers as specified by the user
- Smart surroundings (fixed wireless devices such as printers, price verifiers, near me tags as installed in the facility)
- Runtime RF environment
- The previous position of the tag
- TDoA

- AoA

SOLE is capable of receiving input of location from external 3rd party location engines such as Aer Scout and Ekahau. SOLE also has a self learning process that adapts with a changing environment. SOLE also provides an open platform for supporting new architectures, future algorithms or newer asset types.

Defining Site Parameters

In order for the locationing engine to function properly the site parameters must first be defined. Sites are defined on an X,Y axis with the upper left corner of the site being assigned a value of 0,0. When locations of tags are displayed they are displayed in the same X,Y format relative to the origin value of 0,0.

To configure your site parameters:

- 1 Select *Services > RTLS* from the main menu tree.

The screenshot shows the Summit WM3600 Controller web interface. The left-hand navigation menu includes sections for Controller, Network, Services (with sub-items like DHCP Server, Secure NTP, Redundancy, Layer 3 Mobility, Self Healing, Discovery, and RTLS), Security, Management Access, and Diagnostics. The main content area is titled 'Services > RTLS' and has tabs for 'Site', 'SOLE', 'Aer Scout', and 'Ekahau'. The 'Site' tab is active, showing 'Site Information' with fields for Name, Description, and Dimension (X, Y, Z, and Unit). The 'AP Information' section contains a table with columns for AP Mac, Location (X, Y, Z), Status, Controller IP, 11a Radio (Index, Mac, Power, Chan), and 11bg Radio (Index, Mac, Power, Chan). At the bottom of the page are buttons for Save, Logout, Refresh, Apply, Revert, and Help.

- 2 Select the *Site* tab.

3 Enter a *Name* and optionally a *Description* for the site:

Name	Enter a name for the site where locationing is deployed. This is for identification purposes only.
Description	Provide a description of the site where locationing is deployed. This is an optional field.

4 When mapping out a site for locationing an origin point must be selected in one of the corners of the site. That origin will become the upper left corner of the site map with coordinates of 0,0. The length and width of the site is then mapped out on the X and Y axes. Those length and width along with the height are entered into the field below.

Define the Dimensions and *Unit* of measure used to define the site size:

Length	Enter the length of the site. This is the X axis of your site map based on the origin point of 0,0. The size is either in feet or meters depending on which unit of measure is selected below. The valid range for length is 1-1000m or 1-3000ft.
Width	Enter the width of the site. This is the Y axis of your site map based on the origin point of 0,0. The size is either in feet or meters depending on which unit of measure is selected below. The valid range for width is 1-1000m or 1-3000ft.
Height	Enter the height of the site. The size is either in feet or meters depending on which unit of measure is selected below. The acceptable range for height is 0-20m or 0-60ft. Height is an optional parameter and is not taken into account by the locationing algorithm.
Unit	Use the pulldown menu to select the unit of measure used for dimensions. The options are feet or meters.

5 The AP Information section displays the following information about APs:

AP MAC	Lists the MAC Addresses of all APs which have been configured for RTLS.
Location: X Coordinate	Displays the value of the X Coordinate for each AP. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map. This value is user configured and not detected by the controller. For information on how to configure AP location information, see “Adding AP Location Information” on page 380 .
Location: Y Coordinate	Displays the value of the Y Coordinate for each AP. The Y coordinate is relative to the origin point of 0,0 in the upper left corner of the site map. This value is user configured and not detected by the controller. For information on how to configure AP location information, see “Adding AP Location Information” on page 380 .
Location: Z Coordinate	Displays the value of the Z Coordinate for each AP. The Z coordinate is the height of the AP relative to the lowest point of the site. This value is user configured and not detected by the controller. For information on how to configure AP location information, see “Adding AP Location Information” on page 380 .
Status	Displays the status value for each AP.
Controller IP	Displays the IP address of controller associated with each AP configured for RTLS.
11a Radio	Displays the Index, MAC Address, Power and Channel information for the 802.11a radio on each AP.
11b Radio	Displays the Index, MAC Address, Power and Channel information for the 802.11b radio on each AP.

- 6 Click the *Apply* button to save the changes made within this screen. Clicking *Apply* overwrites the previous configuration.
- 7 Click the *Revert* button to disregard any changes made within this screen and revert back to the last saved configuration.

Adding AP Location Information

To add AP Location information for your site: Select *Services > RTLS* from the main menu tree.

- 1 Select the *Site* tab.
- 2 Click the *Add* button.

The screenshot shows a dialog box titled "Services > RTLS > Add AP". The dialog has a title bar with a close button (X). The main area is titled "Add AP" and contains four input fields: "AP MAC" with a placeholder "- - - - -", "X Coordinate" with a range "(1 - 80)", "Y Coordinate" with a range "(1 - 50)", and "Z Coordinate" with a range "(0 - 5)". Below these fields is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

Configuring SOLE Parameters

To configure the controller's internal SOLE locationing engine:

- 1 *Services* > *RTLS* from the main menu tree.
- 2 Select the *SOLE* tab.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a menu tree with the following items: Controller, Network, Services (expanded), Security, Management Access, and Diagnostics. Under Services, the following sub-items are listed: DHCP Server, Secure NTP, Redundancy, Layer 3 Mobility, Self Healing, Discovery, and RTLS (highlighted). The main content area is titled "Services > RTLS" and has tabs for "SOLE", "Aeroscout", and "Ekahau". The "SOLE" tab is selected. The page contains a checkbox labeled "Locate All Mobile-Units" which is unchecked. Below this is a text input field for "MU Locate Interval" with the value "30" and a note "(5 - 3600 sec)". At the bottom of this section are "Apply", "Revert", and "Help" buttons. To the right is a table titled "MU MAC" which is currently empty. Below the table are "Delete" and "Add" buttons. At the bottom of the main content area is a section titled "Located MUs" containing a table with columns: MAC, Location (subdivided into X Coordinate and Y Coordinate), Timestamp, and Zone. The table is currently empty. At the bottom left of the interface are "Save", "Logout", and "Refresh" buttons. A "Login Details" section shows "Connect To: 10.255.108.36" and "User: admin". A "Message" section is also present.

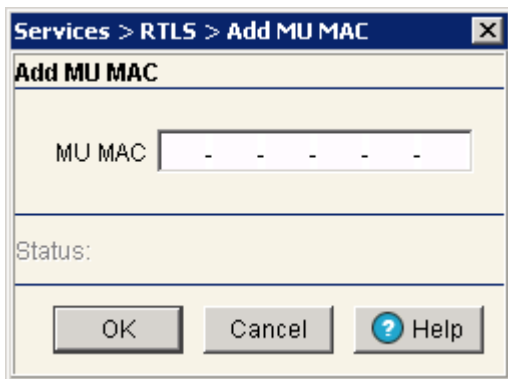
- 3 Check the *Locate All Mobile-Units* checkbox to locate all MUs known to the controller across all WLANs. This will also disable manual entry of MU MAC addresses in the field below. This takes effect immediately when the box is checked.
- 4 Enter a value for the *MU Locate Interval* in seconds. The *MU Locate Interval* determines how often the locationing of MUs is updated. The valid range for this is between 5 to 3600 seconds.
- 5 Click the *Apply* button to save the MU Locate Interval value.
- 6 Click the *Revert* button to cancel any changes made within MU Locate Interval value and revert back to the last saved configuration.



NOTE

AP coordinates can only be configured in the Command Line Interface. For more information on configuring AP coordinates please consult the Summit WM3000 Series Controller CLI Reference Guide.

- 7 The *MU MAC* table allows you to manually add or remove MAC Addresses which can be located by the SOLE engine. This supports a maximum of 512 MUs. This table is disabled when the *Locate All MUs* checkbox is selected.
 - a To add MUs to the *MU MAC* table click the *Add* button to open a dialogue box allowing you to add a MAC Address to the *MU MAC* table allowing it to be located by the controller's SOLE engine.



- b To remove a MAC Address from the *MU MAC* table select a MAC Address from the table and click the *Delete* button to remove that MU. This table is disabled when the *Locate All MUs* checkbox is selected.

Once SOLE has been enabled MUs found by the locationing engine will be displayed in the *Located MUs* table at the bottom of the page. For each located MU the following information is displayed:

MAC	Lists the MAC Addresses of all MUs which have been located by the controller.
Location: X Coordinate	Displays the value of the X Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Location: Y Coordinate	Displays the value of the Y Coordinate for each located MU. The Y coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Timestamp	Displays the last time for each MU that its location was computed by the controller.
Zone	Lists the last known zone for each located MU. Zone configuration can be defined using the CLI interface only. When no zones are configured, the controller defaults the entire site to Zone 0.



NOTE

Zone configuration can be defined using the CLI interface only. For information on Zone Configuration, please see the Summit WM3000 Series Controller CLI Reference Guide.

Configuring Aeroscout Parameters

To configure the controller to work with an external Aeroscout RTLS engine:

- 1 *Services* > *RTLS* from the main menu tree.
- 2 Select the *Aeroscout* tab.

SUMMIT® WM3600 CONTROLLER

Services > RTLS

Site | SOLE | **Aeroscout** | Ekahau

Enable Multicast MAC 00 - 00 - 00 - 00 - 00 - 00

External

IP Address	0.0.0.0		
Port	0		
No. of RX Msgs	0	Last Msg RX Time	N/A
No. of TX Msgs	0	Last Msg TX Time	N/A
No. of Tag Reports	0		

Onboard using SOLE

Enable

Locate Interval 20 (5 - 3600 seconds)

MAC	Location		Timestamp	Zone
	X Coordinate	Y Coordinate		

Save Logout Refresh Apply Revert Help

- 3 Check the *Enable* checkbox to globally enable Aeroscout RTLS support on the controller. This takes effect immediately when the box is checked.
- 4 Enter the *Multicast MAC Address* used for all Aeroscout tags to send updates via multicast to the MAC address specified. Typically the MAC address will start with 01-0C-CC-XX-XX-XX.



NOTE

To use the onboard SOLE engine to locate Aeroscout tags, site parameters, AP location (Command Line Interface only) and Zone configuration (optional, Command Line Interface only) must be configured.

- 5 Click the *Apply* button to save the *Multicast MAC Address* value.
- 6 Click the *Revert* button to cancel any changes made within *Multicast MAC Address* value and revert back to the last saved configuration.

7 If the *Multicast MAC Address* is configured and Aeroscout support is enabled, the following information will be displayed

IP Address	Displays the IP address of the external Aeroscout RTLS engine.
Port	Displays the port number which the controller uses to connect to the external Aeroscout RTLS engine.
No. of RX Msgs	Displays the number of messages received by the controller from the external Aeroscout RTLS engine.
Last Msg RX Time	Displays the Date and Time that the last message was received from the external Aeroscout RTLS engine.
No. of TX Msgs	Displays the number of messages transmitted by the controller to the external Aeroscout RTLS engine.
Last Msg TX Time	Displays the Date and Time that the last message was sent to the external Aeroscout RTLS engine.
No. of Tag Reports	Displays the number of Tag Reports received from the external Aeroscout RTLS engine.

8 To use the onboard SOLE engine to locate Aeroscout tags, check the *Enable* checkbox. This is enabled immediately after checking the box.

9 If the onboard SOLE engine is enabled to locate Aeroscout tags, enter a *Locate Interval* in seconds to specify how often the known tags are located by the SOLE engine.

10 Click the *Apply* button to save the *Locate Interval* value.

11 Click the *Revert* button to cancel any changes made within *Locate Interval* value and revert back to the last saved configuration.

If the onboard SOLE engine is enabled to locate Aeroscout tags, the following information will be displayed for each located MU:

MAC	Lists the MAC Addresses of all MUs which have been located by the controller.
Location: X Coordinate	Displays the value of the X Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Location: Y Coordinate	Displays the value of the Y Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Timestamp	Displays the last time for each MU that its location was computed by the controller.
Zone	Lists the last known zone for each located MU. Zone configuration can be defined using the CLI interface only. When no zones are configured, the controller defaults the entire site to Zone 0.



NOTE

Zone configuration can be defined using the CLI interface only. For information on Zone Configuration, please see the Summit WM3000 Series Controller CLI Reference Guide.

Configuring Ekahau Parameters

To configure the controller to work with an external Ekahau RTLS engine:

- 1 *Services* > *RTLS* from the main menu tree.

The screenshot shows the 'Services > RTLS' configuration page for a Summit WM3700 Controller. The page is divided into several sections:

- Navigation Menu:** Located on the left, it includes sections for Controller, Network, Services, Security, Management Access, and Diagnostics. The 'Services' section is expanded to show options like DHCP Server, Secure NTP, Redundancy, Layer 3 Mobility, Self Healing, Discovery, and RTLS (which is highlighted).
- Site Selection:** At the top, 'Site | SOLE | Aeroscout | Ekahau' is displayed.
- Enable:** A checkbox labeled 'Enable' is checked.
- Multicast MAC:** A text field contains '00 - 00 - 00 - 00 - 00 - 00'.
- External:** This section includes:
 - IP Address:** A text field with '0 - 0 - 0 - 0'.
 - Port:** A text field with '1000 (1000 - 9000)'.
 - Statistics:** 'No. of RX Msgs', 'No. of TX Msgs', and 'No. of Tag Reports' are all set to '0'. 'Last Msg RX Time' and 'Last Msg TX Time' are both 'N/A'.
- Onboard using SOLE:** A checkbox labeled 'Enable' is unchecked.
- Locate Interval:** A text field contains '20 (5 - 3600 seconds)'.
- Table:** A table with columns for MAC, Location (subdivided into X Coordinate and Y Coordinate), Timestamp, and Zone. The table is currently empty.
- Buttons:** At the bottom right, there are 'Apply', 'Revert', and 'Help' buttons.

- 2 Select the *Ekahau* tab.
- 3 Check the *Enable* checkbox to globally enable Ekahau support on the controller. This takes effect immediately when the box is checked.
- 4 Enter the *Multicast MAC Address* used for all Ekahau tags to send updates via multicast to the MAC address specified. Typically the MAC address will start with 01-0C-CC-XX-XX-XX.



NOTE

To use the onboard SOLE engine to locate Ekahau tags, site parameters, AP location (Command Line Interface only) and Zone configuration (optional, Command Line Interface only) must be configured.

- 5 Specify the *IP Address* of the Ekahau RTLS engine server.
- 6 Enter the *Port* number used to communicate with the Ekahau RTLS engine. The port range must be between 1000 and 9000.
- 7 Click the *Apply* button to save the *Multicast MAC Address*, *IP Address* and *Port* information.
- 8 Click the *Revert* button to cancel any changes made within *Multicast MAC Address*, *IP Address* and *Port* settings and revert back to the last saved configuration.

9 If the *Multicast MAC Address*, *IP Address* and *Port* values are configured and Ekahau RTLS support is enabled the following information will be displayed:

No. of RX Msgs	Displays the number of messages received by the controller from the external Ekahau RTLS engine.
Last Msg RX Time	Displays the Date and Time that the last message was received from the external Ekahau RTLS engine.
No. of TX Msgs	Displays the number of messages transmitted by the controller to the external Ekahau RTLS engine.
Last Msg TX Time	Displays the Date and Time that the last message was sent to the external Ekahau RTLS engine.
No. of Tag Reports	Displays the number of Tag Reports received from the external Ekahau RTLS engine.

10 To use the onboard SOLE engine to locate Ekahau tags check the *Enable* checkbox. This is enabled immediately after checking the box.

11 If the onboard SOLE engine is enabled to locate Ekahau tags, enter a *Locate Interval* in seconds to specify how often the known tags are located by the SOLE engine.

12 Click the *Apply* button to save the *Locate Interval* value.

13 Click the *Revert* button to cancel any changes made within *Locate Interval* value and revert back to the last saved configuration.

If the onboard SOLE engine is enabled to locate Ekahau tags the following information will be displayed for each located MU:

MAC	Lists the MAC Addresses of all MUs which have been located by the controller.
Location: X Coordinate	Displays the value of the X Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Location: Y Coordinate	Displays the value of the Y Coordinate for each located MU. The X coordinate is relative to the origin point of 0,0 in the upper left corner of the site map.
Timestamp	Displays the last time for each MU that its location was computed by the controller.
Zone	Lists the last known zone for each located MU. Zone configuration can be defined using the CLI interface only. When no zones are configured, the controller defaults the entire site to Zone 0.



NOTE

Zone configuration can be defined using the CLI interface only. For information on Zone Configuration, please see the Summit WM3000 Series Controller CLI Reference Guide.

7 Controller Security

CHAPTER

This chapter describes the security mechanisms available to the controller. This chapter describes the following security configuration activities:

- [Displaying the Main Security Interface on page 387](#)
- [Access Point Detection on page 389](#)
- [Wireless IDS/IPS on page 399](#)
- [Configuring Firewalls and Access Control Lists on page 403](#)
- [Configuring NAT Information on page 445](#)
- [Configuring IKE Settings on page 457](#)
- [Configuring IPSec VPN on page 465](#)
- [Configuring the RADIUS Server on page 489](#)
- [Creating Server Certificates on page 509](#)
- [Configuring Enhanced Beacons and Probes on page 523](#)

Displaying the Main Security Interface

Refer to main *Security* interface for a high level overview of device intrusion and controller access permission options.

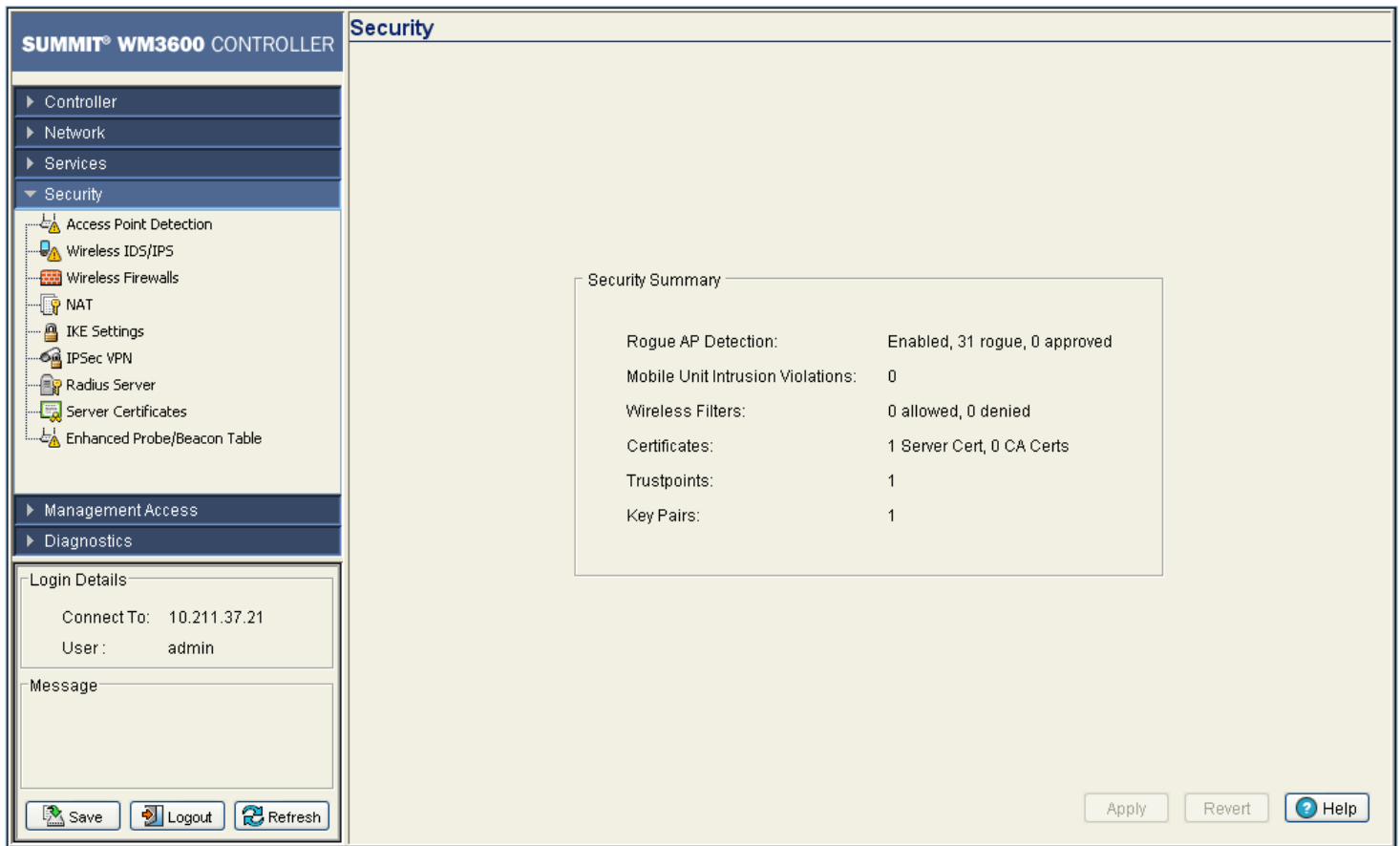


NOTE

When the controller's configuration is successfully updated (using the Web UI), the affected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the affected screen's Status field remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To view main menu security information:

- 1 Select *Security* from the main menu tree.



- 2 Refer to the following information to discern if configuration changes are warranted:

Rogue AP Detection	Displays the Enabled or Disabled state of the controller to detect potentially hostile Access Ports/Points (the definition of which defined by you). Once detected, these devices can be added to a list of devices either approved or denied from interoperating within the controller managed network. For more information, see “Access Point Detection” on page 389 .
Mobile Unit Intrusion Violations	Displays the state of the controller protecting against threats from MUs trying to find network vulnerabilities. For more information, see “Wireless IDS/IPS” on page 399 .
Wireless Filters	Displays the state of the filters used to either allow or deny a MAC address (or groups of MAC addresses) from associating with the controller. For more information, see “Configuring Firewalls and Access Control Lists” on page 403 .
Certificates	Displays the number of Server and CA certificates currently used by the controller. For more information, see “Creating Server Certificates” on page 509 .
Trustpoints	Displays the number of trustpoints currently in use by this controller. The trustpoint signing the certificate can be a certificate authority, corporation or an individual. A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. For more information, see “Using Trustpoints to Configure Certificates” on page 509 .

Key Pairs

Displays the number of Key Pairs currently used by the controller. For more information, see [“Certificate Authority Root Certificates” on page 520](#).

The *Apply* and *Revert* buttons are greyed out within this screen, as there is no data to be configured or saved.

Access Point Detection

Use the *Access Point Detection* menu options to view and configure the detection of other Access Points. The Access Point Detection screen consists of the following tabs:

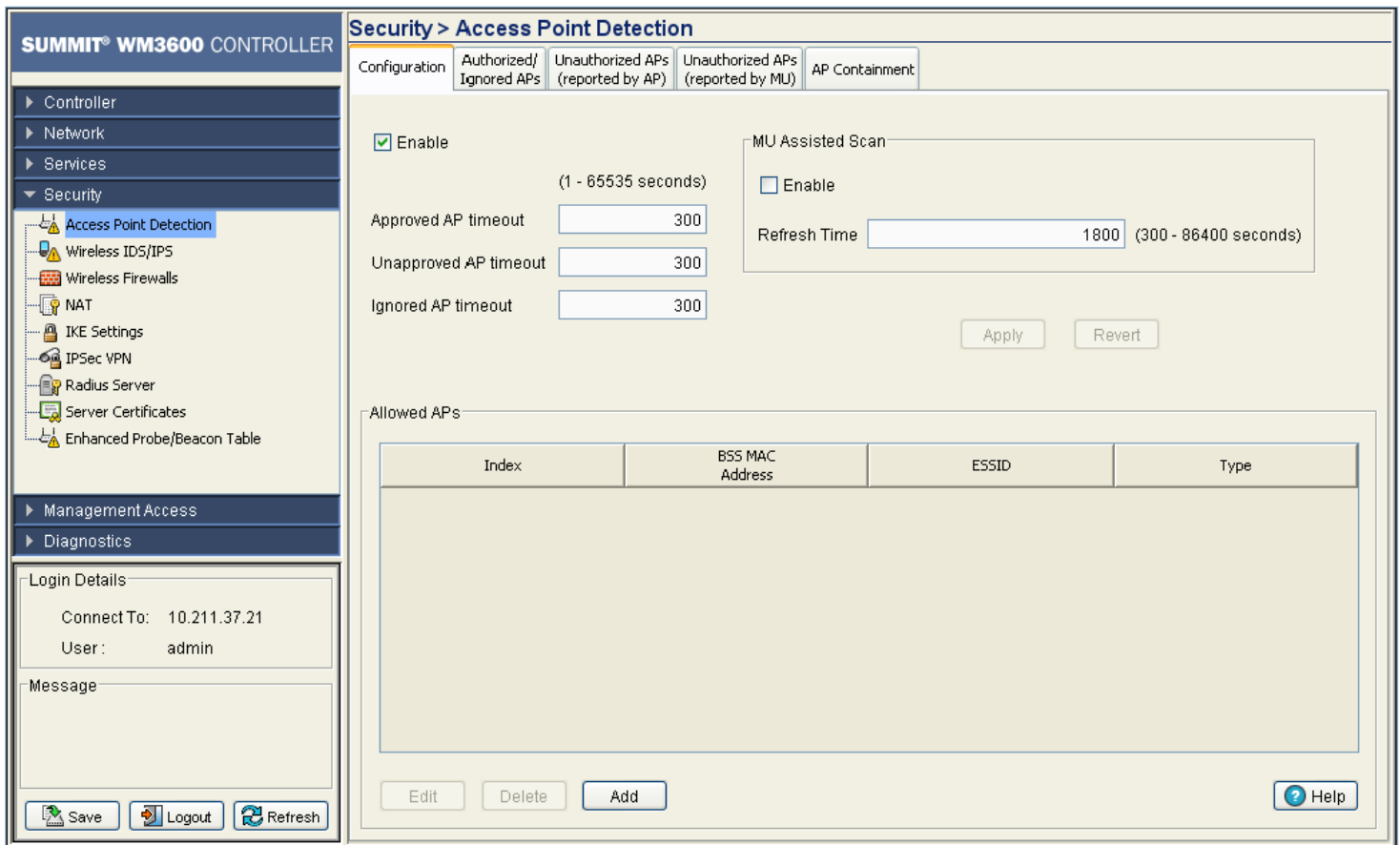
- [Enabling and Configuring AP Detection on page 389](#)
- [Authorized / Ignored APs on page 393](#)
- [Unauthorized APs \(AP Reported\) on page 395](#)
- [Unauthorized APs \(MU Reported\) on page 396](#)
- [AP Containment on page 398](#)

Enabling and Configuring AP Detection

Use the *Configuration* screen to allow the controller to detect potentially hostile Access Points, set the number of detected APs allowed and define the timeout and threshold values used for detection. The controller can enable both AP4600 Series Access Points and certain Motorola made MUs to scan and detect Access Points within the controller managed network. Continually re-validating the credentials of associated devices reduces the possibility of an Access Point hacking into the controller managed network.

To configure AP Detection:

- 1 Select *Security > Access Point Detection* from the main menu.
- 2 Select the *Configuration* tab.



- 3 Enable AP assisted scanning and timeout intervals as required.

Enable	Select the <i>Enable</i> checkbox to enable associated Access Ports to detect potentially hostile Access Points (the definition of which defined by you). Once detected, the Access Points can be added to a list of APs either approved or denied from interoperating within the controller managed network.
Approved AP timeout	Define a value (in seconds) the controller uses to timeout (previously approved) Access Points that have not communicated with the controller. The range is from 1-65535 seconds, with a default of 300 seconds. This value is helpful for continually re-validating Access Points that interoperate within the controller managed network.
Unapproved AP timeout	Define a value (in seconds) the controller uses to remove Access Points that have not communicated with the controller. The range is from 1-65535 seconds, with a default of 300 seconds.
Ignored AP timeout	Define a value (in seconds) the controller uses to remove ignored APs that have not communicated with the controller. The range is from 1 to 65335 seconds, with a default of 300 seconds.

4 Refer to the *MU Assisted Scan* field to enable associated MUs to assist in the detection of Access Points.

Enable	Select the <i>Enable</i> checkbox to enable associated MUs to detect potentially hostile Access Points (the definition of which defined by you). Once detected, these devices can be added to a list of Access Points either approved or denied from interoperating within the controller managed network.
Refresh Time	Define a value (in seconds) associated MUs use to scan for Access Points. The range is from 300–86400 seconds, with a default of 1800 seconds.



NOTE

Extreme Networks Summit WM3000 Series WLAN controller supports certain Motorola made MUs for MU assisted scan. Contact Extreme Networks Support for details of these special MU devices.



NOTE

When using MU Assisted Scans with an AP4600 Series Access Port, the MU Assisted scan will begin as soon as the Enable checkbox is selected. Subsequent scans will take place based on the time defined in the Refresh Time field.



NOTE

When using MU Assisted Scans with an AP35xx the MU Assisted scan will not begin immediately. The first scan will begin after the current Refresh Time cycle has expired.

- 5 Click the *Apply* button to save the changes made.
- 6 Click the *Revert* button to cancel any changes and revert back to the last saved configuration.
- 7 Refer to the *Allowed APs* field to view the policies used for interpreting Access Points as allowed.

Index	Displays the numerical identifier (index value) assigned to this particular set of Allowed APs. Assign this value by clicking <i>Add</i> for a new set of Access Point address information or click the <i>Edit</i> button to revise the index. The Index can be used as reference to group specific devices numerically to a specific range of MAC or ESSID addresses. This user cannot modify the index from this screen.
BSS MAC Address	Displays the MAC address of the Allowed AP(s). The MAC addresses displayed are defined by clicking the <i>Add</i> button and entering a specific MAC address or by allowing all MAC addresses to be allowed. The list of MAC addresses allowed can be modified by highlighting an existing entry, clicking the <i>Edit</i> button and revising the properties of the MAC address.
ESSID	Displays the ESSIDs of the Allowed AP(s). The addresses displayed are defined by clicking the <i>Add</i> button and entering a specific MAC address or by allowing all MAC addresses to be allowed. The list of MAC addresses allowed can be modified by highlighting an existing entry, clicking the <i>Edit</i> button and revising the properties of the MAC address.
Type	Displays the radio type of the allowed APs. Available types are: 802.11a, 802.11an, 802.11bg, and 802.11bgn.

- 8 Select an Allowed AP and click the *Edit* button to launch a screen used to modify the index and SSID of the AP. For more information, see [“Adding or Editing an Allowed AP” on page 392](#).
- 9 Select an Allowed AP and click the *Delete* button to remove the AP from list of Allowed APs.
- 10 Click the *Add* button to display a screen used to enter device information for a new AP added to the Allowed AP list. For more information, see [“Adding or Editing an Allowed AP” on page 392](#).

Adding or Editing an Allowed AP

To add a new address range or modify the address range used to designate devices as allowed:

- 1 Select *Security > Access Point Detection* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Select an existing Allowed AP and click the *Edit* button to modify the properties of an existing Allowed AP or click the *Add* button to define the attributes of a new Allowed AP.

- 4 If adding a new Allowed AP, use the *Index* parameter to assign a numerical index value to this particular Access Point. The index range is from 1-200. If editing an existing Allowed AP, this is a read only field and cannot be modified.
- 5 Refer to the *BSS MAC Address* field to define the following:

Any MAC Address/ Specific MAC Address	Click the <i>Any MAC Address</i> radio button to allow any MAC address detected on the network as an Allowed AP. This is not necessary if a specific MAC address is used with this index.
	Click the second radio button to enter a specific MAC address as an Allowed AP. Use this option if (for network security) you want to restrict the number of MAC Addresses to a single MAC address.

6 Refer to the *ESSID* field to configure Access Point ESSID permissions.

Any ESSID/Specific ESSID Click the *Any ESSID* radio button to allow any ESSID located on the network as an Allowed AP. This may not be necessary if a specific ESSID was used with this particular index.

Click the second radio button to enter a specific ESSID as an Allowed AP. Use this option if (for network security) you want to restrict the number of device ESSIDs saved for this index to a single Access Point ESSID.

7 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

8 Click *OK* to use the changes to the running configuration and close the dialog.

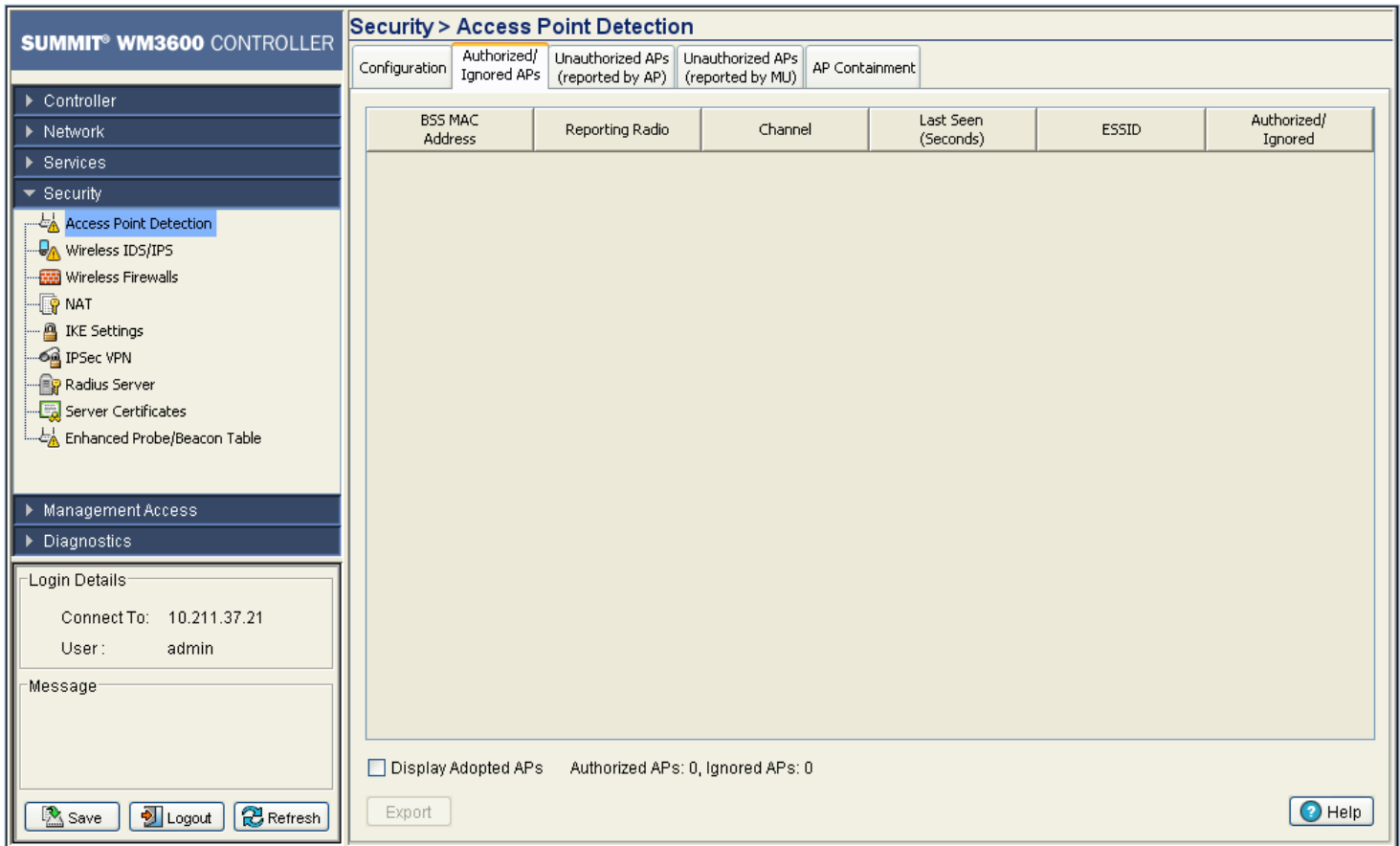
9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Authorized / Ignored APs

Those Access Points detected and approved for operation within the controller managed network can be separately displayed to assess the reporting (detecting) AP, the channel of operation, the last time the AP was observed on the network and the ESSID. Use this information to assess if an approved Access Point was incorrectly defined as approved and requires categorization as an unapproved and disallowed AP.

To review the attributes of allowed APs:

- 1 Select *Security > Access Point Detection* from the main menu.
- 2 Select the *Authorized/Ignored APs* tab.



3 The *Approved APs* table displays the following information:

BSS MAC Address	Displays the MAC Address of each approved AP. These MAC addresses are Access Points observed on the network meeting the criteria (MAC and ESSIDs) of allowed APs.
Reporting AP	Displays the numerical value assigned to the radio used with the specific device MAC Address and SSID listed for this approved AP.
Channel	Displays the channel the approved AP is currently transmitting on. If this device is operating on a channel not frequently used within your network segment, perhaps the device is correctly defined as an approved AP.
Last Seen (In Seconds)	Displays the time (in seconds) the approved AP was last seen on the network.
ESSID	Displays the SSID of each approved AP.
Authorized/Ignored APs	Displays authorized APs.

4 The *Number of Approved APs* is simply the sum of all of approved Access Point MAC Addresses detected.

5 Select the *Display Adopted APs* check box.

6 Click the *Export* button to export the contents of the table to a Comma Separated Values file (CSV).

Unauthorized APs (AP Reported)

Use the *Unapproved APs (AP Reported)* tab to review Access Points detected by associated controller Access Port radios and are restricted from operation within the controller managed network. The criteria for restriction was defined using the *Security > Access Point Detection > Configuration* screen.

To view Access Port detected unapproved Access Points:

- 1 Select *Security > Access Point Detection* from the main menu tree.
- 2 Click the *Unauthorized APs (AP Reported)* tab.

Security > Access Point Detection

Configuration	Authorized/ Ignored APs	Unauthorized APs (reported by AP)	Unauthorized APs (reported by MU)	AP Containment				
		BSS MAC Address	Reporting Radio	Channel	Signal Strength (dBm)	Last Seen (Seconds)	ESSID	Detected on Wire
		00-03-7F-BE-F1-1D	8	2	-87	16	Spider-bg	
		00-04-96-42-33-30	8	1	-97	16	101	
		00-04-96-42-34-30	8	8	-87	15		
		00-04-96-42-34-31	8	6	-82	15	multiple_vlans	
		00-04-96-42-34-32	8	7	-88	15	guestwireless	
		00-04-96-42-76-C0	8	2	-85	16	ENSL	
		00-04-96-42-76-C1	8	2	-85	16	SKO2011	
		00-16-01-D6-00-82	8	8	-75	15	CorpSE-DDWRT	
		00-23-68-11-ED-F0	8	2	-75	16	test-101-my	
		00-23-68-11-ED-F1	8	5	-83	15	test-102	
		00-23-68-11-ED-F2	8	3	-66	16	103	
		00-23-68-2E-73-B8	8	2	-74	2	jy-v5-650	
		00-23-68-2E-F4-E0	8	1	-97	69	Extreme-wpa	
		00-23-68-2E-F4-E1	8	1	-97	118	Extreme_Guest	
		00-23-68-2F-0C-A0	8	3	-82	9	Extreme-wpa	
		00-23-68-2F-0C-A1	8	2	-84	16	Extreme_Guest	
		00-23-68-2F-8B-20	8	6	-88	1	Extreme-wpa	
		00-23-68-2F-8B-21	8	7	-86	1	Extreme_Guest	
		00-23-68-2F-E0-10	8	2	-65	2	Extreme-wpa	
		00-23-68-2F-E0-11	8	2	-65	2	Extreme_Guest	
		00-23-68-2F-EC-40	8	12	-66	17	Extreme-wpa	
		00-23-68-2F-EC-41	8	12	-65	17	Extreme_Guest	
		00-23-68-2F-F4-40	8	2	-88	5	Extreme-wpa	
		00-23-68-2F-F4-41	8	2	-87	20	Extreme_Guest	
		00-23-68-30-09-D0	8	13	-86	17	Extreme-wpa	
		00-23-68-30-09-D1	8	13	-87	0	Extreme_Guest	
		00-23-68-30-22-F0	8	6	-96	22	Extreme-wpa	

Display Adopted APs Authorized APs: 0, Ignored APs: 0

Export Allow Contain Help

3 The *Unauthorized APs (AP Reported)* table displays the following information:

- | | |
|---------------------------------|---|
| BSS MAC Address | Displays the MAC Address of each Unapproved AP. These MAC addresses are Access Points observed on the network, but have yet to be added to the list of Approved APs, and are therefore interpreted as a threat on the network.

If a MAC Address displays on the list incorrectly, click the <i>Allow</i> button and add the MAC Address of a newly Allowed AP index. |
| Reporting Radio | Displays the numerical value for the radio used with the detecting AP. |
| Channel | Displays the channel the Unapproved AP is currently transmitting on. |
| Signal Strength (in dBm) | Displays the <i>Relative Signal Strength Indicator</i> (RSSI) for the detected (and unapproved) AP. APs with a strong signal may pose a more significant risk within the controller managed network. |
| Last Seen (in Seconds) | Displays the time (in seconds) the Unapproved AP was last seen on the network by the detecting AP. |

ESSID	Displays the ESSID of each Unapproved AP. These ESSIDs are device ESSIDs observed on the network, but have yet to be added to the list of Approved APs and are therefore interpreted as a threat. If an ESSID displays on the list incorrectly, click the <i>Allow</i> button and add the ESSID to a new Allowed AP index.
Detected on Wire	When enabled, the controller identifies if a detected unauthorized AP has been connected to the wired network.

- 4 The *Number of Unauthorized APs* is simply the sum of all of Unapproved Radio MAC Addresses detected.
- 5 Select the Display Adopted APs check box.
- 6 If a radio's MAC address is listed incorrectly, highlight the MAC Address and click the *Allow* button. Assign an Index and define the required device address information to move the device into the list of approved Access Point MAC addresses. The number of Unapproved APs updates accordingly as devices are added and removed.
- 7 Click the *Export* button to export the contents of the table to a *Comma Separated Values* file (CSV).

Unauthorized APs (MU Reported)

Use the *Unauthorized APs (MU Reported)* tab to review unapproved Access Points detected by associated MUs. The criteria for Access Point approval was defined using the *Security > Access Point >*

Configuration screen, using the values defined within the *MU Assisted Scan* field. To view unapproved Access Points detected by controller radio associated MUs:

- 1 Select *Security > Access Point Detection* from the main menu tree.
- 2 Click the *Unauthorized APs (MU Reported)* tab.

SUMMIT® WM3600 CONTROLLER

Security > Access Point Detection

Configuration | Authorized/ Ignored APs | **Unauthorized APs (reported by MU)** | Unauthorized APs (reported by AP) | AP Containment

BSS MAC Address	Reporting MU	Last Seen (Seconds)	ESSID	Detected on Wire
Number of Unauthorized APs : 0				

Number of Unauthorized APs : 0

Export Help

Save Logout Refresh

3 The *Unauthorized APs (MU Reported)* table displays the following information:

BSS MAC Address	Displays the MAC Address of each Unapproved AP. These MAC addresses are Access Points observed on the network (by associated MUs), but have yet to be added to the list of approved APs, and are therefore interpreted as a threat on the network.
Reporting MU	Displays the numerical value for the detecting MU.
Last Seen (In Seconds)	Displays the time (in seconds) the Unapproved AP was last seen on the network by the detecting MU. Use this interval to determine whether the detected MU is still a viable threat.
ESSID	Displays the ESSID of each Unapproved AP. These ESSIDs are device ESSIDs observed on the network, but have yet to be added to the list of Approved APs and are therefore interpreted as a threat.
Detected on Wire	When enabled, the controller identifies if a detected unauthorized AP has been connected to the wired network.

4 The *Number of Unauthorized APs* is simply the sum of all of Unapproved Radio MAC Addresses detected.

5 Click the *Export* button to export the contents of the table to a Comma Separated Values file (CSV).

AP Containment

Use the rogue *AP Containment* feature to provide protection from rogue Access Points by disrupting traffic to mobile units associated with the Rogue AP and prevents new mobile units from getting associated to the Rogue AP.

To configure Access Point Containment and view rogue APs:

- 1 Select *Security > Access Point Detection* from the main menu tree.
- 2 Click the *AP Containment* tab.

The *AP Containment* screen is divided into two sections, configuration and rogue AP information.

- 3 To enable the AP containment feature, check the *Enable Containment* checkbox and specify a *Containment Interval* between 20 and 5000 milliseconds. The *Containment Interval* field determines the interval after which broadcast 802.11 de-authentication messages will be sent.
- 4 When the containment feature has been enabled and a *Containment Interval* has been set, click the *Apply* button to enable the feature and save the interval value.
- 5 The rogue AP table displays the following information about known rogue APs:

Index	A unique numerical ID assigned by the controller for each of the known rogue APs.
Rogue BSS Mac	Display a list of all know Rogue BSS MAC Addresses known to the controller.

Number of Finders	Displays the number of detector APs that have found each of the specified Rogue APs.
Channel	Displays the channels that each of the known Rogue APs are broadcasting on.

- 6 To manually add a rogue AP to the table, click the *Add* button and enter the MAC address of the known rogue AP.
- 7 To remove an AP from the rogue AP table, select that AP and click the *Delete* button.

Wireless IDS/IPS

Unauthorized attempts to access the controller managed LAN by MUs / APs / other Rogue devices are a significant threat to the network, and one that is very pervasive currently. The controller has several means to protect against threats from intruding devices, trying to find network vulnerabilities.

Use the controller's *Wireless IDS/IPS* facility to view and configure wireless intrusion related information. The *Wireless IDS/IPS* screen provides the following functionalities:

- [Configuring Wireless IDS/IPS on page 400](#)
- [Viewing Filtered MUs on page 402](#)

Configuring Wireless IDS/IPS

To configure Wireless IDS/IPS:

- 1 Select *Security > Wireless IDS/IPS* from the main tree menu.
- 2 Click the *Configuration* tab.

Security > Wireless IDS/IPS

Configuration | Filtered MUs

Enable WIDS

Collection Settings

Detection Window: (5 - 300 seconds)

Violation Parameters

Violation Type	Trigger against			Threshold Values for		Time to Filter
	Auth	Unauth	Ignore	Mobile Unit	Radio	
AP Default Configuration	✓	✗	✗			
Ad-Hoc Advertising Authorized SSID	✓	✓				0
Ad-Hoc Network Violation Authorized Device	✓					0
Beacon with broadcast ESSID	✗	✗	✗			
De-auth from broadcast smac	✓	✗	✗			0
Detect Adhoc Networks		✗				0
EAP Flood	✓	✗		30	100	0
Excessive 802.11 replays	✗			10	25	0
Excessive Auth or Association	✗	✓		25	120	0
Excessive Authentication failure	✗			5	20	0
Excessive Crypto replays	✗	✗		10	25	0
Excessive Decryption failures	✗			25	75	0
Excessive Disassociation	✓	✗		25	45	0
Excessive EAP Start Frames	✗	✗		10	30	0
Excessive EAP-NAKS	✗	✗		10	20	0
Excessive Probes	✗	✗		30	200	0
Excessive Unassociated Frames		✓		2		0
Fake AP Flood		✓	✓			
Frames with known bad ESSIDs	✓	✓				0
Frames with non-changing WEP IV	✓	✗	✗			0
Impersonation Attack Detected	✓					0
Invalid 802.1x frames	✗	✗				0
Invalid Frame Length	✓	✗	✗			0

Bad ESSID Configuration | Reset to defaults | Apply | Revert | Help

The MU Intrusion Detection tab consists of the following two fields:

- Collection Settings
- Violation Parameters

- 3 Within the *Collection Settings* field, set the *Detection Window* interval (in seconds) the controller uses to scan for MU violations. The available range is from 5–300 seconds.
- 4 Refer to the *Violation Parameters* field to define threshold values that trigger an alarm:

Violation Type	Displays the name of the violation for which threshold values are set in the MU, radio and controller columns.
Trigger Against (Auth, Unauth, Ignore)	Displays what conditions will trigger the violation parameter against Authorized APs, Unauthorized APs and Ignored APs. If a violation is triggered by an AP type it will display with a green check box. If it is not triggered on an AP type it will display with a red X.
Threshold Values for Mobile Unit	Set the MU threshold value for each violation type. If exceeded, the MU will be filtered and displayed within the Filtered MUs screen.
Threshold Values for Radio	Set the radio threshold value for each violation type. If exceeded, the radio will be filtered and displayed within the Filtered Radios screen.

Time to Filter Set the Time to Filter interval (in seconds) the controller uses to filter out MUs defined as committing a violation. Refer to [“Viewing Filtered MUs” on page 402](#) to review the contents of the MUs that have been filtered thus far.



CAUTION

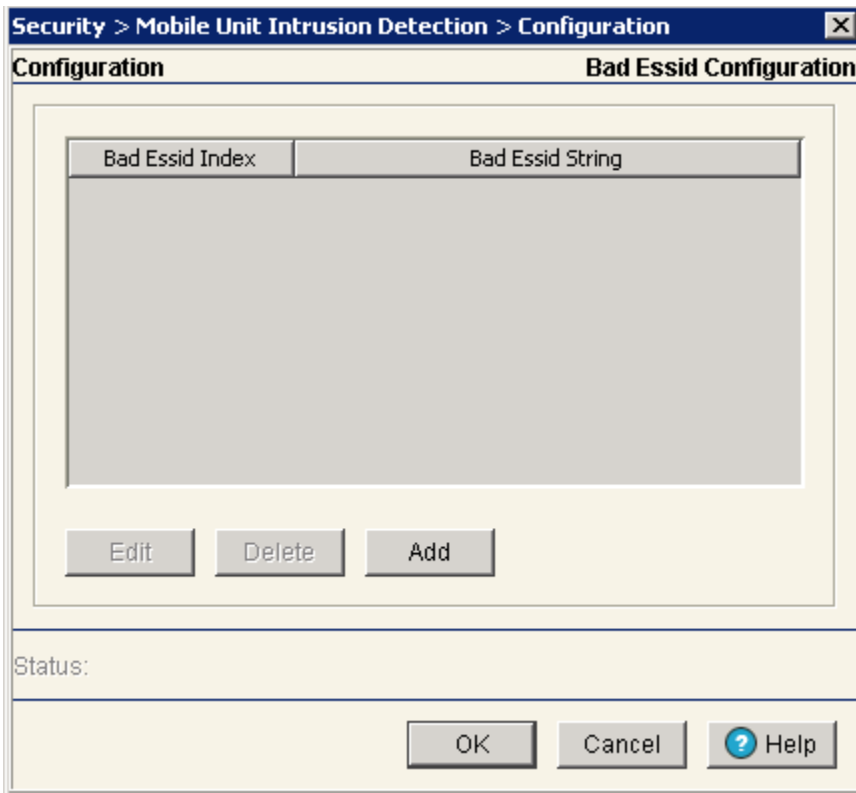
Setting MU threshold values too low can jeopardize MU performance or break the MU's connection.



NOTE

Setting a violation parameter to 0 will disable that option.

- 5 When using the *Frames with known bad ESSIDs* violation parameter, it is necessary to enter a list of known bad ESSIDs for the violation parameter. To enter this information, select *Frames with known bad ESSIDs* and then click the *Bad Essid Config* button to launch a dialogue box where bad ESSIDs can be added and removed.



NOTE

If using the *Frames with known bad ESSIDs* violation parameter, the parameter will not function if no ESSIDs are entered in the *Bad Essid Config* dialog.

- 6 Click *Apply* to save the configuration.

- Click *Revert* to rollback to the previous configuration.

Viewing Filtered MUs

Periodically check the *Filtered MUs* tab to review MUs filtered by the controller for incurring a violation based on the settings defined within the *Configuration* tab. Each MU listed can be deleted from the list or its attributes exported to a user defined location.

To view status of those MUs filtered using the settings defined within the *Configuration* tab:

- Select *Security > Wireless IDS/IPS* from the main tree menu.
- Click the *Filtered MUs* tab.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation tree with 'Security > Wireless IDS/IPS' selected. The main content area displays the 'Filtered MUs' tab, which contains a table with the following columns: MAC Address, Radio Index, Violation Type, and Time Remaining. The table is currently empty. Below the table are 'Delete' and 'Export' buttons. At the bottom right is a 'Help' button. The bottom left of the interface shows 'Login Details' (Connect To: 10.211.37.21, User: admin) and a 'Message' field. At the very bottom are 'Save', 'Logout', and 'Refresh' buttons.

The Filtered MUs tab displays the following read-only information for detected MUs:

- | | |
|-------------|--|
| MAC Address | Displays the MU's MAC address. Defer to this address as the potentially hostile MU's identifier. |
| Radio Index | The radio index displays the index of the detected MU. Use this information to discern whether the detected MU is known and whether it truly constitutes a threat. |

Violation Type Displays the reason the violation occurred for each detected MU. Use the Violation Type to discern whether the detected MU is truly a threat on the controller managed network (and must be removed) or can be interpreted as a non threat. The following violation types are possible:

- Excessive Probes
- Excessive Association
- Excessive Disassociation
- Excessive Authentication failure
- Excessive Crypto replays
- Excessive 802.11 replays
- Excessive Decryption failures
- Excessive Unassociated Frames
- Excessive EAP Start Frames
- Null destination
- Same source/destination MAC
- Source multicast MAC
- Weak WEP IV
- TKIP Countermeasures
- Invalid Frame Length
- Excessive EAP-NAKS
- Invalid 802.1x frames
- Invalid Frame Type
- Beacon with broadcast ESSID
- Frames with known bad ESSIDs
- Unencrypted traffic
- Frames with non-changing WEP IV
- Detect Adhoc Networks
- De-auth from broadcast smac
- Invalid Sequence Number

The following violation types require the Access Port be in scan mode:

- Beacon with broadcast ESSID
- Frames with known bad ESSIDs

Time Remaining Displays the time remaining before the next filter activity. Detected MUs are removed from the filtered list when they no longer violate the thresholds defined within the Configuration tab.

- 3 Select a detected MU and click the *Delete* button to remove it from the list of MUs you are tracking as potential threats within the controller managed network.
- 4 Click the Export button to export the contents of the table to a Comma Separated Values file (CSV).

Configuring Firewalls and Access Control Lists

An *Access Control List* (ACL) is a sequential collection of permit and deny conditions that apply to controller packets. When a packet is received on an interface, the controller compares the fields in the

packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists.

**NOTE**

If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.

Use the *Wireless Firewall* screen to view, add and configure access control configurations. Typically, an ACL consists of series of entries called an Access Control Entry (ACE). Each ACE defines the rule which defines whether the packets needs to be controlled/routed or needs to be dropped. The ACL screen displays three tabs:

- Security Policy
- Configuration
- Statistics

Each of these tabs has sub tabs which provide configuration options for creating and attaching the ACLs.

**NOTE**

For an overview of how the controller uses an ACL to filter permissions to the controller managed network, go to [“ACL Overview” on page 404](#).

ACL Overview

An ACL contains an ordered list of *Access Control Entries (ACEs)*. Each ACE specifies an action and a set of conditions that a packet must satisfy in order to match the ACE. The order of conditions in the list is critical because the controller stops testing conditions after the first match.

The controller supports the following ACLs to filter traffic:

- *Router ACLs*—Applied to VLAN (Layer 3) interfaces. These ACLs filter traffic based on Layer 3 parameters like *source IP, destination IP, protocol types* and *port numbers*. They are applied on packets routed through the controller. Router ACLs can be applied to inbound traffic only, not both directions.
- *Port ACLs*—Applied to traffic entering a Layer 2 interface. Only controlled packets are subjected to these kind of ACLs. Traffic filtering is based on Layer 2 parameters like—*source MAC, destination MAC, Ethertype, VLAN-ID, 802.1p bits* (OR) Layer 3 parameters like—*source IP, destination IP, protocol, port number*.

**NOTE**

Port and router ACLs can be applied only in an inbound direction. WLAN ACLs support applying ACLs in the inbound and outbound direction.

- *Wireless LAN ACLs*—A Wireless LAN ACL is designed to filter/mark packets based on the wireless LAN from which they arrived rather than filtering the packets arrived on Layer 2 ports.

For more information, see

- [Router ACLs on page 405](#)
- [Port ACLs on page 406](#)
- [Wireless LAN ACLs on page 407](#)
- [ACL Actions on page 407](#)
- [Precedence Order on page 407](#)

Router ACLs

Router ACLs are applied to Layer 3 or VLAN interfaces. If an ACL is already applied in a particular direction on an interface, applying a new one will replace the existing ACL. Router ACLs are applicable only if the controller acts as a gateway, and traffic is inbound only.

The controller supports two types of Router ACLs:

- *Standard IP ACL*—Uses the source IP address as matching criteria.
- *Extended IP ACL*—Uses the source IP address, destination IP address and IP protocol type as basic matching criteria. It can also include other parameters specific to a protocol type (like source and destination port for TCP/UDP protocols).

Router ACLs are stateful and are not applied on every packet routed through the controller. Whenever a packet is received from a Layer 3 interface, it is examined against existing sessions to determine if it belongs to an established session. ACLs are applied on the packet in the following manner.

- 1 If the packet matches an existing session, it is not matched against ACL rules and the session decides where to send the packet.
- 2 If no existing sessions match the packet, it is matched against ACL rules to determine whether to accept or reject it. If ACL rules accept the packet, a new session is created and all further packets belonging to that session are allowed. If ACL rules reject the packet, no session is established.

A session is computed based on:

- Source IP address
- Destination IP address
- Source Port
- Destination Port
- ICMP identifier
- Incoming interface index
- IP Protocol



NOTE

Port and router ACLs can be applied only in an inbound direction. WLAN ACLs support applying ACLs in the inbound and outbound direction.

Each session has a default idle time-out interval. If no packets are received within this interval, the session is terminated and a new session must be initiated. These intervals are fixed and cannot be configured by the user.

The default idle time-out intervals for different sessions are:

- *ICMP and UDP sessions*—30 seconds
- *TCP sessions*—2 hours

Port ACLs

The controller supports Port ACLs on physical interfaces and inbound traffic only. The following Port ACLs are supported:

- *Standard IP ACL*—Uses a source IP address as matching criteria.
- *Extended IP ACL*—Uses a source IP address, destination IP address and IP protocol type as basic matching criteria. It can also include other parameters specific to a protocol type, like the source and destination ports for TCP/UDP protocols.
- *MAC Extended ACL*—Uses source and destination MAC addresses and VLAN ID. Optionally, it also uses Ethertype information.

Port ACLs are also stateful and are not applied on every packet controlled through the controller. Whenever a packet is received inbound, it is examined against existing sessions to determine if it belongs to an established session. ACLs are applied on the packet in the following manner:

- 1 If the packet matches an existing session, it is not matched against ACL rules and the session decides where to send the packet.
- 2 If no existing sessions match the packet, it is matched against ACL rules to determine whether to accept or reject it. If ACL rules accept the packet, a new session is created and all further packets belonging to that session are allowed. If ACL rules reject the packet, no session is established.

A session is based on:

- Source IP address
- Destination IP address
- Source Port
- Destination Port
- ICMP identifier
- Incoming interface index
- IP Protocol
- Source MAC
- Destination MAC
- Ethertype
- VLAN-ID
- 802.1p bits

When a Port ACL is applied to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. With Port ACLs, you can filter:

- IP traffic by using IP ACL
- Non-IP traffic by using MAC addresses.

Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

You cannot apply more than one IP ACL and one MAC ACL to a Layer 2 interface. If an IP ACL or MAC ACL is already configured on a Layer 2 interface and a new IP ACL or MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

Wireless LAN ACLs

Wireless LAN ACLs filter/mark packets based on the wireless LAN from which they arrive rather than filtering packets on Layer 2 ports.

In general, a Wireless-LAN ACL can be used to filter wireless to wireless, wireless to wired and wired to wireless traffic. Typical wired to wired traffic can be filtered using a Layer 2 port based ACL rather than a WLAN ACL.

Each WLAN is assumed to be a virtual Layer 2 port. Configure one IP and one MAC ACL on the virtual WLAN port. In contrast to Layer 2 ACLs, a WLAN ACL can be enforced on both the Inbound and Outbound direction.

ACL Actions

Every ACE within an ACL is made up of an action and matching criteria. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:

- *deny*—Instructs the ACL not to allow a packet to proceed to its destination.
- *permit*—Instructs the ACL to allow a packet to proceed to its destination.
- *mark*—Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.
 - VLAN 802.1p priority.
 - TOS/DSCP bits in the IP header.



NOTE

A Permit All ACL is not supported when using NTP. If a Permit All ACL is used with NTP, the client will not be able to synchronize with the NTP server.



NOTE

Only a Port ACL supports a mark action. With Router ACLs, a mark is treated as a permit and the packet is allowed without modifications.

Precedence Order

The rules within an ACL are applied to packets based on their precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence value.

Consider the following when adding rules:

- Every ACL entry in an ACL is associated with a precedence value unique for every entry. You cannot enter two different entries in an ACL with the same precedence value. This value can be

between 1 and 5000. An ACE in an ACL is associated with a unique precedence value. No two ACEs can have the same precedence value.

- Specifying a precedence value with each ACL entry is not mandatory. If you do not want to specify one, the system automatically generates a precedence value starting with 10. Subsequent entries are added with precedence values of 20, 30 and so on. 10 is the default offset between any two rules in an ACL. However, if the user specifies a precedence value with an entry, that value overrides the default value. The user can also add an entry in between two subsequent entries (for example, in between 10 and 20).
- If an entry with a max precedence value of 5000 exists, you cannot add a new entry with a higher precedence value. In such a case, the system displays an error stating “Rule with max precedence value exists”. Either delete the entry or add new entries with precedence values less than 5000. A user can add a maximum of 500 ACEs in an ACL.
- Rules within an ACL are displayed in an ascending order of precedence.



NOTE

ACEs with lower precedence are always applied first to packets. Therefore, it is advised to add more specific entries in the ACL first then the general ones. While displaying the ACL, the entries are displayed in an ascending order of precedence.

Attaching an ACL on a WLAN Interface/Port

Use the *Attach-WLAN* tab to view and assign an ACL to a WLAN on the controller. If a MAC ACL is being attached, create a ACL entry to allow arp with least precedence.



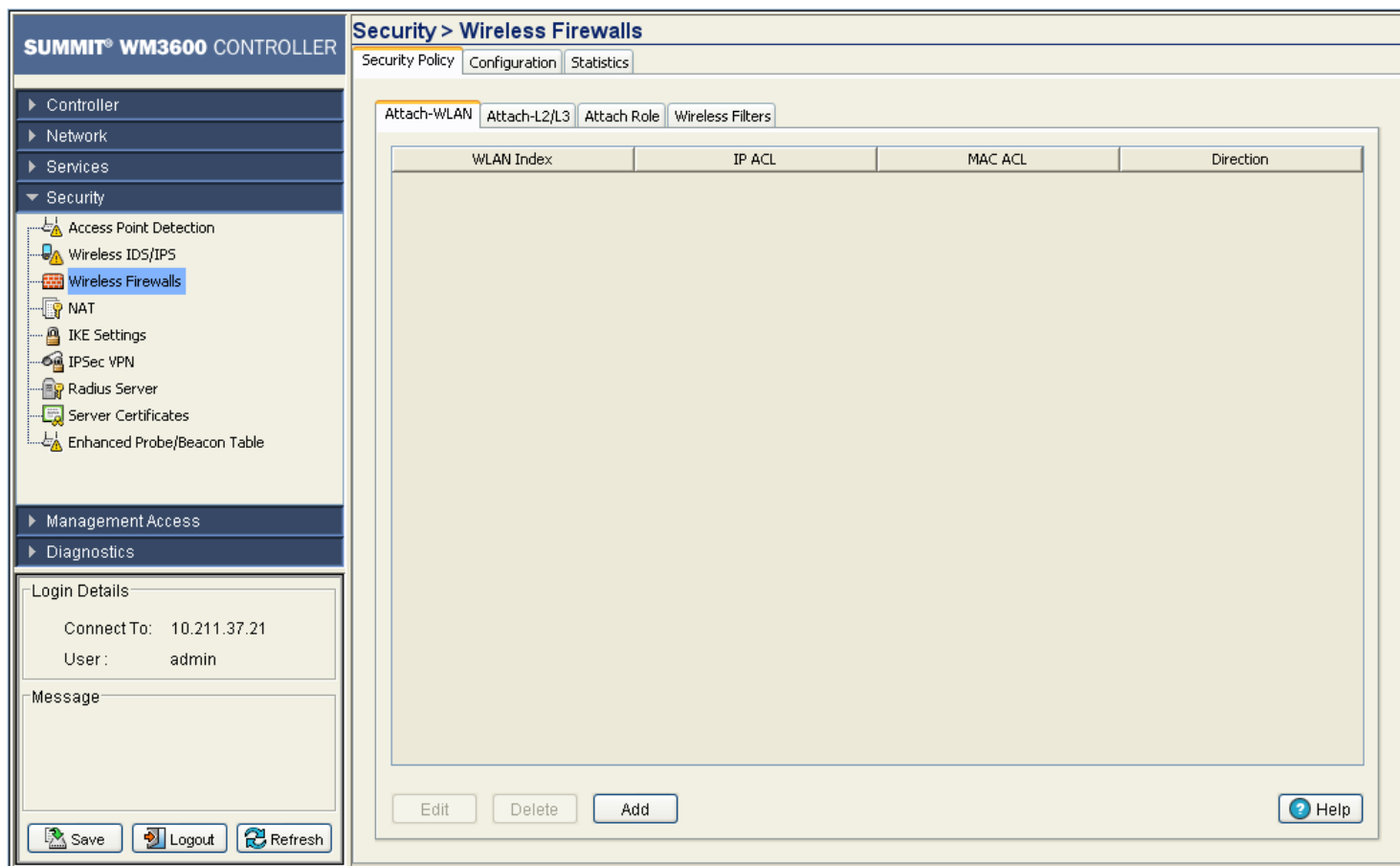
NOTE

WLAN based ACLs allow users to enforce rules/ACLs on both the inbound and outbound direction, as opposed to Layer 2 ACLs, which just support the inbound direction.
The ACL rules per AAP is <0-24>

To configure a WLAN ACL:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.

3 Click the *Attach-WLAN* tab.



4 Refer to the following information as displayed within the *Attach-WLAN* tab:

WLAN Index	Displays the list of WLANs attached with ACLs.
IP ACL	Displays the IP ACL configured.
MAC ACL	Displays the MAC ACL configured.
Direction	Displays whether the WLAN ACL is configured to work in an inbound or outbound direction.

5 Select a WLAN (by row) and click Edit to modify the WLAN Index, IP ACL and MAC ACL values.

6 Select a row and click the *Delete* button to delete the ACL from the list available (but not from the controller).

7 Click the *Add* button to add an ACL to a WLAN interface. For more information, see [“Adding or Editing a New ACL WLAN Configuration”](#) on page 409.

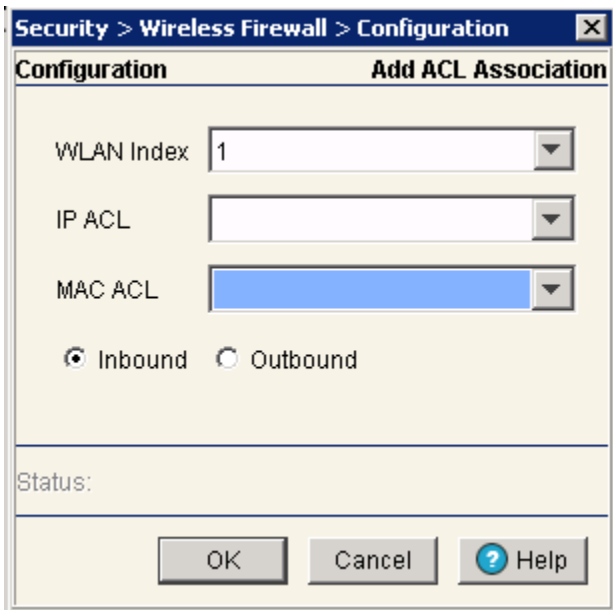
Adding or Editing a New ACL WLAN Configuration

After creating an ACL, it can be applied to one or more WLANs on the controller. To attach an ACL to a WLAN:

1 Select *Security > Wireless Firewall* from the main menu tree.

2 Click the *Security Policy* tab.

- 3 Click the *Attach-WLAN* tab.
- 4 Click the *Add* button to create a new ACL WLAN association or highlight an existing association and click the *Edit* button.



- 5 Define a *WLAN Index* between 1 and 32.
- 6 Use the *IP ACL* drop-down menu to select an IP ACL for the WLAN.
- 7 Use the *MAC ACL* drop-down menu to select the MAC ACL for the WLAN interface.
- 8 Select either the *Inbound* or *Outbound* radio button to define which direction the ACL applies.
- 9 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to use the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

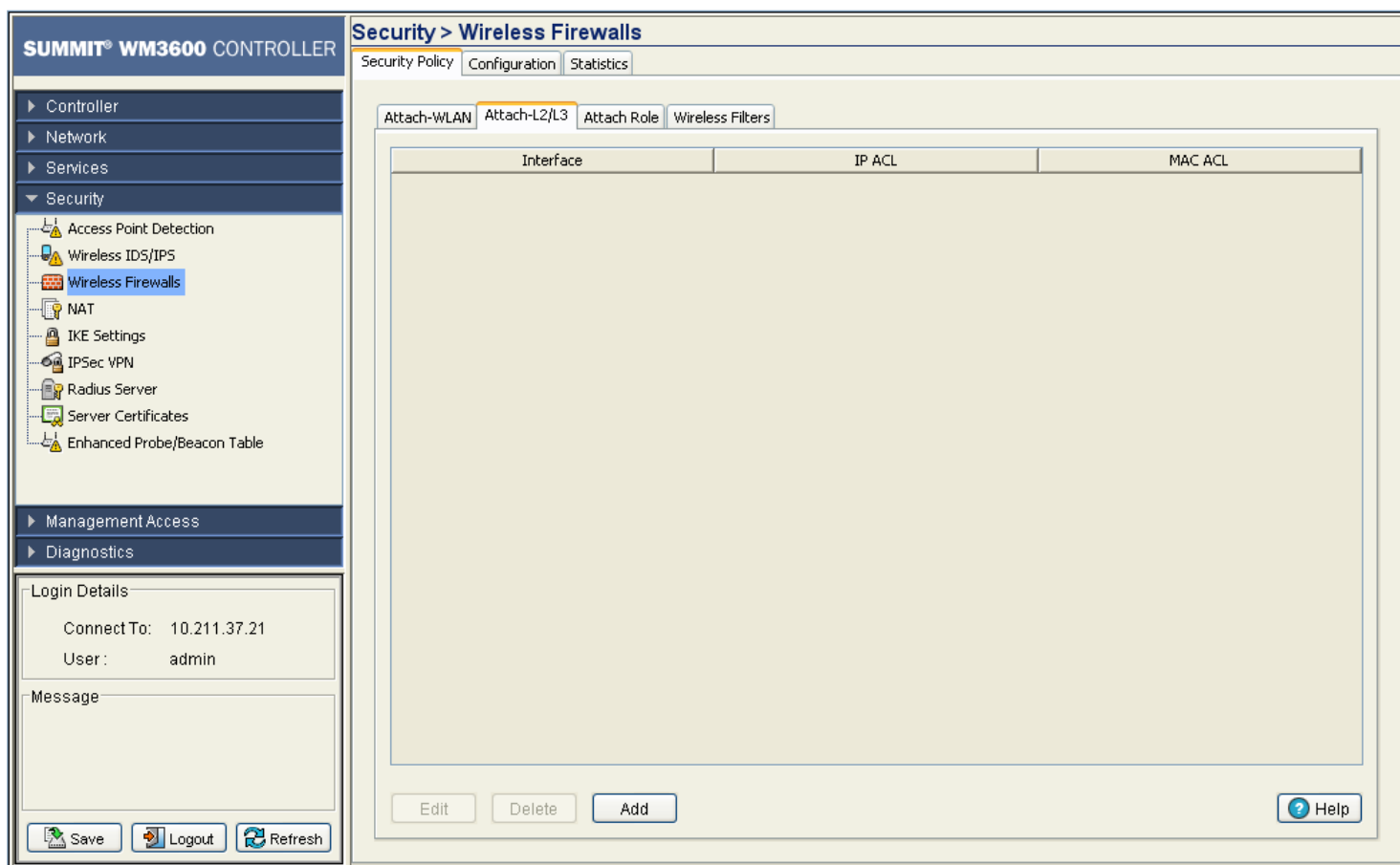
Attaching an ACL Layer 2/Layer 3 Configuration

Use the *Attach-L2/L3* screen to view and assign the ACL to a physical interface or VLAN.

To attach an interface:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.

3 Click the *Attach-L2/L3* tab.



4 Refer to the following information as displayed within the Attach tab:

Interface	The interface to which the controller is configured. It can be one of the following: <ul style="list-style-type: none">• ge 1-5 for Summit WM3400, ge 1-8 for Summit WM3600 and ge 1-4 for Summit WM3700• up 1• <i>vlan1</i> (or any additional VLANs that have been created)
IP ACL	Displays the IP ACL configured as the inbound IP for the Layer 2 or Layer 3 interface.
MAC ACL	Displays the MAC ACL to be configured as the MAC IP for the Layer 2 interface.

5 Select an interface and click *Edit* to modify the ACL interface, IP ACL and MAC ACL values.

6 Select an interface and click the *Delete* button to delete the interface configuration from the controller.

7 Click *Add* button to add an physical or VLAN interface to the controller. For more information, see [“Adding a New ACL Layer 2/Layer 3 Configuration”](#) on page 412.

Adding a New ACL Layer 2/Layer 3 Configuration

After creating an ACL, it can be applied to one or more interfaces. On a Layer 3 interface or Layer 2 interface, ACLs can be applied only in an inbound direction. To add an ACL interface to the controller:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.
- 3 Click the *Attach-L2/L3* tab.
- 4 Click the *Add* button.

- 5 Use the *Interface* drop-down menu to select the interface to configure on the controller. Available options include—ge 1-8, up 1, VLAN 1 (plus those VLANs created thus far) and Tunnel *n* (where *n* equals the name(s) of those tunnels created thus far).
- 6 Use the *IP ACL* drop-down menu to select an IP ACL used as the inbound IP for the layer 2 or layer 3 interface.
- 7 Use the *MAC ACL* drop-down menu to select an MAC ACL used as the MAC IP for the layer 2 interface.
- 8 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 9 Click *OK* to use the changes to the running configuration and close the dialog.
- 10 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring the Role Based Firewall

Use the *Attach Role* screen to view and assign an ACL to a role.



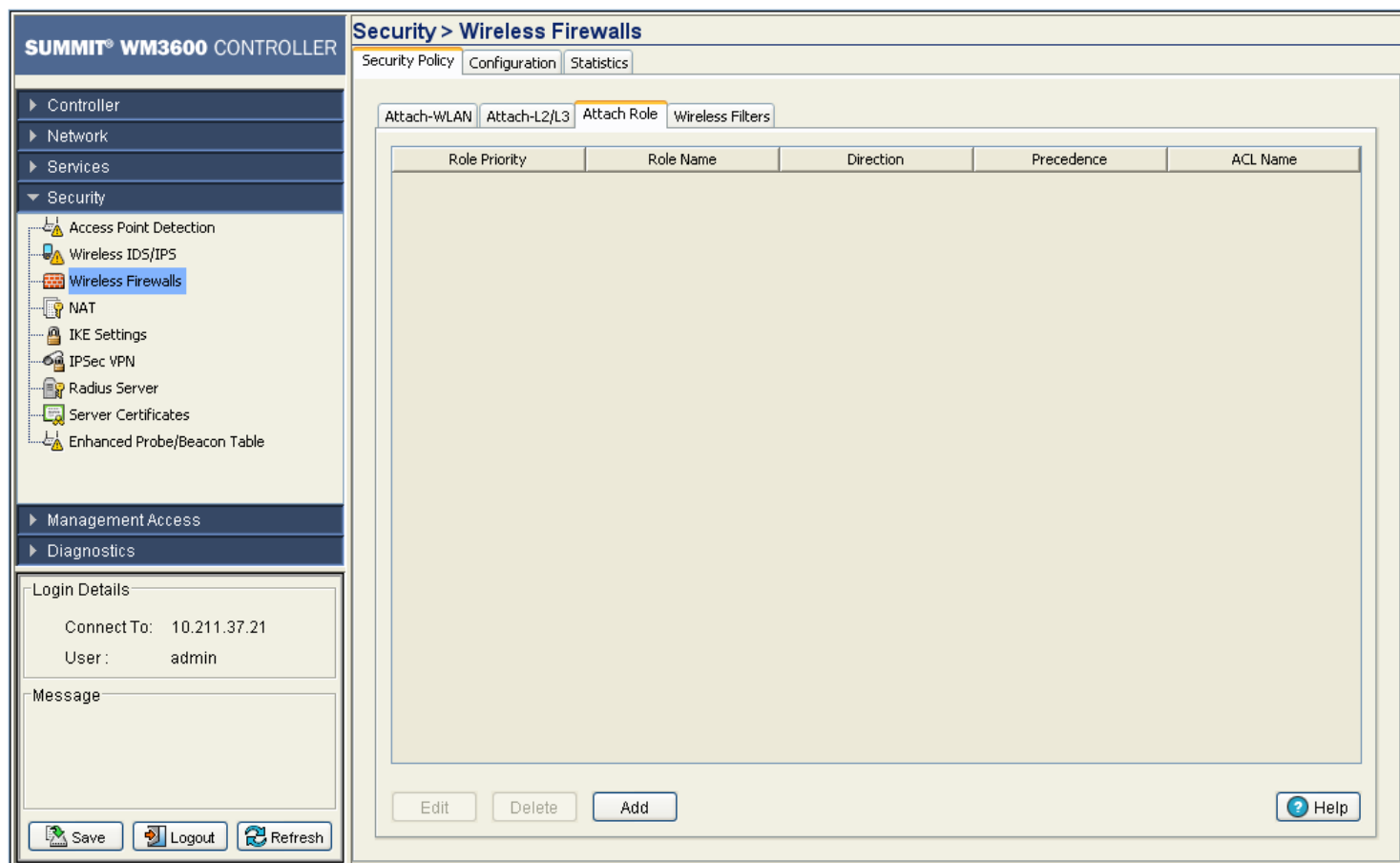
NOTE

Advanced Security License is required to activate the Role Based Firewall feature.

To attach a role:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.

3 Click the *Attach Role* tab.



4 Refer to the following information as displayed within the *Attach Role* tab:

Role Priority	Displays the priority assigned to the role as determined by the <i>Sequence Number</i> associated with the role.
Role Name	Displays the role name assigned to each role. Role names are assigned when they are added from the <i>Security > Wireless Firewall > Configuration > Role</i> tab.
Direction	Displays the direction which the role is associated with. The role can be associated in either the <i>Inbound</i> or <i>Outbound</i> direction.
Precedence	Displays the <i>ACL Precedence</i> . The ACL precedence range is 1-100.
ACL Name	Displays the name of the ACL associated with each role. ACLs can be configured on the ACL tab.

5 Click *Add* button to add a new role. For more information, see [“Configuring the Role Based Firewall” on page 414.](#)

6 Select an interface and click the *Delete* button to delete the interface configuration from the controller.

Configuring the Role Based Firewall

After creating an ACL, it can be applied to one or more Roles. On a role, ACLs can be applied in either an inbound or outbound direction. To add an ACL interface to the controller:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.
- 3 Click the *Attach Role* tab.
- 4 Click the *Add* button.

- 5 Select a *Role Name* from the drop-down menu. *Role Names* can be added in the *Configuration > Role* tab.
- 6 Use the *ACL* drop-down menu to select an ACL to associate with the *Role Name*.
- 7 Select *Inbound* or *Outbound* to apply the new role to the appropriate interface.
- 8 Set a *Precedence* level for the ACL. The valid range is between 1 and 100 with the lower the precedence numbers getting higher priority.
- 9 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 10 Click *OK* to use the changes to the running configuration and close the dialog.
- 11 Click *Cancel* to close the dialog without committing updates to the running configuration.

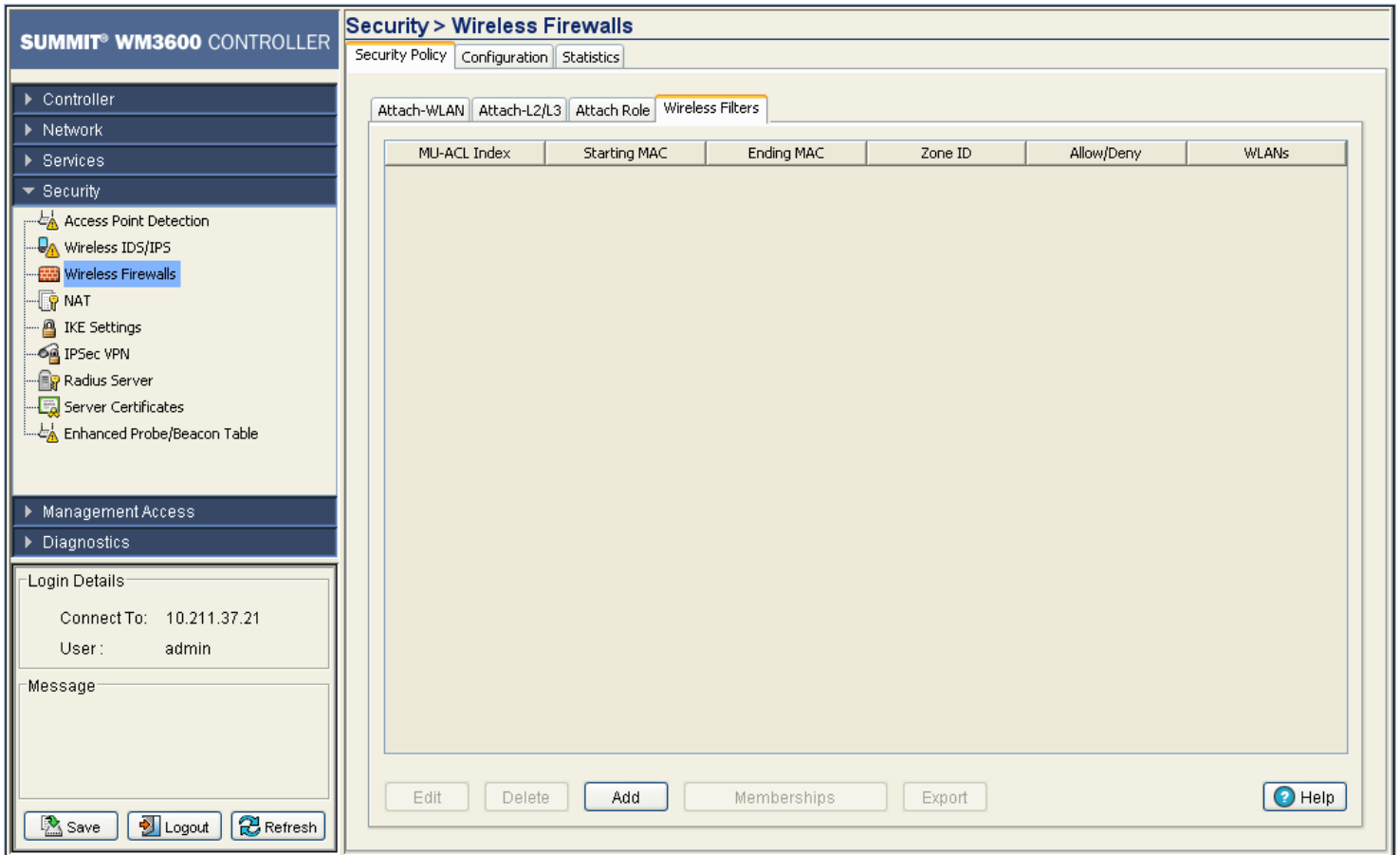
Configuring Wireless Filters

Use filters to either allow or deny a MAC address (or groups of MAC addresses) from associating with the controller. Refer to the *Wireless Filters* screen to review the properties of existing controller filters. A filter can be selected from those available and edited or deleted. Additionally, a new filter can be added if an existing filter does not adequately express the MU's address range required.

To display the Wireless Filters main page:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.

- 3 Click the *Wireless Filters* tab.
- 4 The *Wireless Filters* tab contains the following read-only information:



MU-ACL Index	Displays a numerical identifier used to associate a particular ACL to a range of MAC addresses (or a single MAC address) that are either allowed or denied access to the controller managed network.
Starting MAC	Displays the beginning MAC Address (for this specific Index) either allowed or denied access to the controller managed network.
Ending MAC	Displays the ending MAC Address (for this specific Index) either allowed or denied access to the controller managed network.
Zone ID	Displays a Zone ID associated with each Wireless Filter. Zone ID can be between 1 and 48. Zones allows you to associate firewall policies to each zone. All members of the same zone will have the same firewall policies applied to them.
Allow/Deny	States whether this particular ACL Index and MAC address range has been allowed or denied access to the controller managed network.
WLANs	Displays the WLANs associated with each Wireless Filter.

- 5 If the properties of an existing filter fulfill to your needs but still require modification to better filter devices, select the *Edit* button. For more information see, [“Editing an Existing Wireless Filter” on page 416.](#)
- 6 If an existing filter is now obsolete, select it from those listed and click the *Delete* button.

- 7 Click the *Add* button to create a new filter. For more information, see [“Adding a new Wireless Filter” on page 417](#).
- 8 Click the *Memberships* button to display a screen wherein a selected index can be added to one or more existing WLANs. For more information see, [“Associating an ACL with WLAN” on page 419](#)
- 9 Click the *Export* button to export the contents of the table to a *Comma Separated Values* file (CSV).

Editing an Existing Wireless Filter

Use the *Edit* screen to modify the properties of an existing filter. This is recommended if an existing filter contains adequate device address information, but the allow/deny permissions need to be changed or if only minor changes are required to the starting and ending MAC addresses. If significant changes are required to a usable filter, consider creating a new one.

To edit an existing filter:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.
- 3 Click the *Wireless Filters* tab.
- 4 Select one of the existing ACLs from the filters list.
- 5 Click the *Edit* button at the bottom of the screen to launch a screen for editing an ACL.

The user can modify an ACL Index (numerical identifier) for the ACL, and edit the starting an ending MAC address range for the devices allowed or denied access to the controller managed network.

- 6 The *MU-ACL Index* is used as an identifier for a MAC Address range and allow/deny ACL designation. The available index range is 1–1000. However, the index is not editable, only its starting/ending MAC range and allow/deny designation. If a new index is needed, create a new filter.

-
- 7 Modify the existing *Starting MAC* for the target Index or leave the *Starting MAC* value as is and just modify the *Ending MAC* Address or *Allow/Deny* designation.
 - 8 Modify the existing *Ending MAC* for the target Index. Enter the same *Starting MAC* address within the *Ending MAC* field to use only the *Starting MAC* address as either allowed or denied access to the controller managed network.
 - 9 To associate a zone with the ACL select a *Zone ID* from the pulldown menu. Zone numbers range from 1 to 48. Creating zones allows you to associate firewall policies to each zone. All members of the same zone will have the same firewall policies applied to them.
 - 10 Use the drop-down menu to select *Allow* or *Deny*.
This rule applies to MUs within the specified *Starting* and *Ending MAC* Address range. For example, if the adoption rule is to *Allow*, access is granted for all MUs within the specified range.
 - 11 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
 - 12 Click *OK* to use the changes to the running configuration and close the dialog.
 - 13 Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding a new Wireless Filter

Use the *Add* screen to create a new index and define a new address permission range. Once created, an allow or deny designation can be applied to the new filter ACL.

To create a new filter ACL:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.
- 3 Click the *Wireless Filters* tab.
- 4 Click the *Add* button at the bottom of the screen to launch a new dialogue used for creating an ACL.

Define an Index (numerical identifier) for the ACL and the starting and ending MAC address range for devices allowed/denied access to the controller managed network.

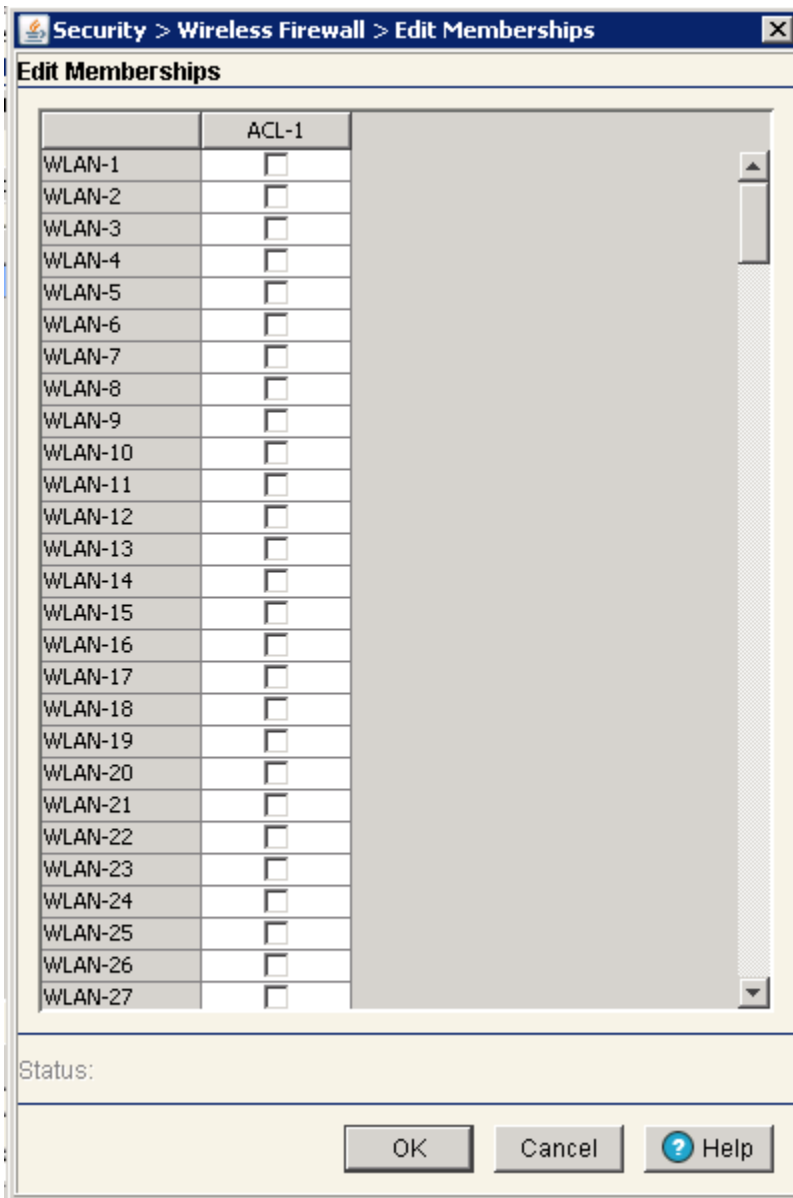
- 5 Enter an Index numerical value (1 -1000) in the *MU-ACL Index* field.
The MU-ACL Index is a numerical identifier used to associate a particular ACL to a range of MAC addresses (or a single MAC address) either allowed or denied access to the controller managed network. Enter a new Index to define a new MAC Address range and allow/deny ACL Index designation.
- 6 Enter a hex value for the *Starting MAC* address.
This is the beginning MAC address either allowed or denied access to the controller managed network.
- 7 Enter a hex value for the *Ending MAC* address. Enter the same Starting MAC address within the *Ending MAC* field to use only the *Starting MAC* address as either allowed or denied access to the controller managed network.
- 8 To modify the zone associated with the ACL select a *Zone ID* from the pulldown menu. Zone numbers range from 1 to 48. Creating zones allows you to associate firewall policies to each zone. All members of the same zone will have the same firewall policies applied to them.
- 9 Use the drop-down menu to select *Allow* or *Deny*.
This rule applies to MUs within the specified Starting and Ending MAC Address range. For example, if the adoption rule is to Allow, access is granted for all MUs within the specified range.
- 10 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 11 Click *OK* to use the changes to the running configuration and close the dialog.
- 12 Click *Cancel* to close the dialog without committing updates to the running configuration.

Associating an ACL with WLAN

Use the *Membership* screen to define a name for the ACL index and map the index to WLANs (1-32) requiring membership permission restrictions.

To associate a filter ACL index with a WLAN:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Security Policy* tab.
- 3 Click the *Wireless Filters* tab.
- 4 Select one or more of the existing ACLs from the filters list.
- 5 Click the *Memberships* button.



- 6 Select the box to the right of each WLAN you want associated with the ACL. Selecting a WLAN maps it the MAC address range and allow or deny designation assigned to it. Consequently, be sure

you are not restricting MU traffic for a WLAN that requires those MAC addresses to interact with the controller.

- 7 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to use the changes to the running configuration and close the dialog.
- 9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring the Firewall

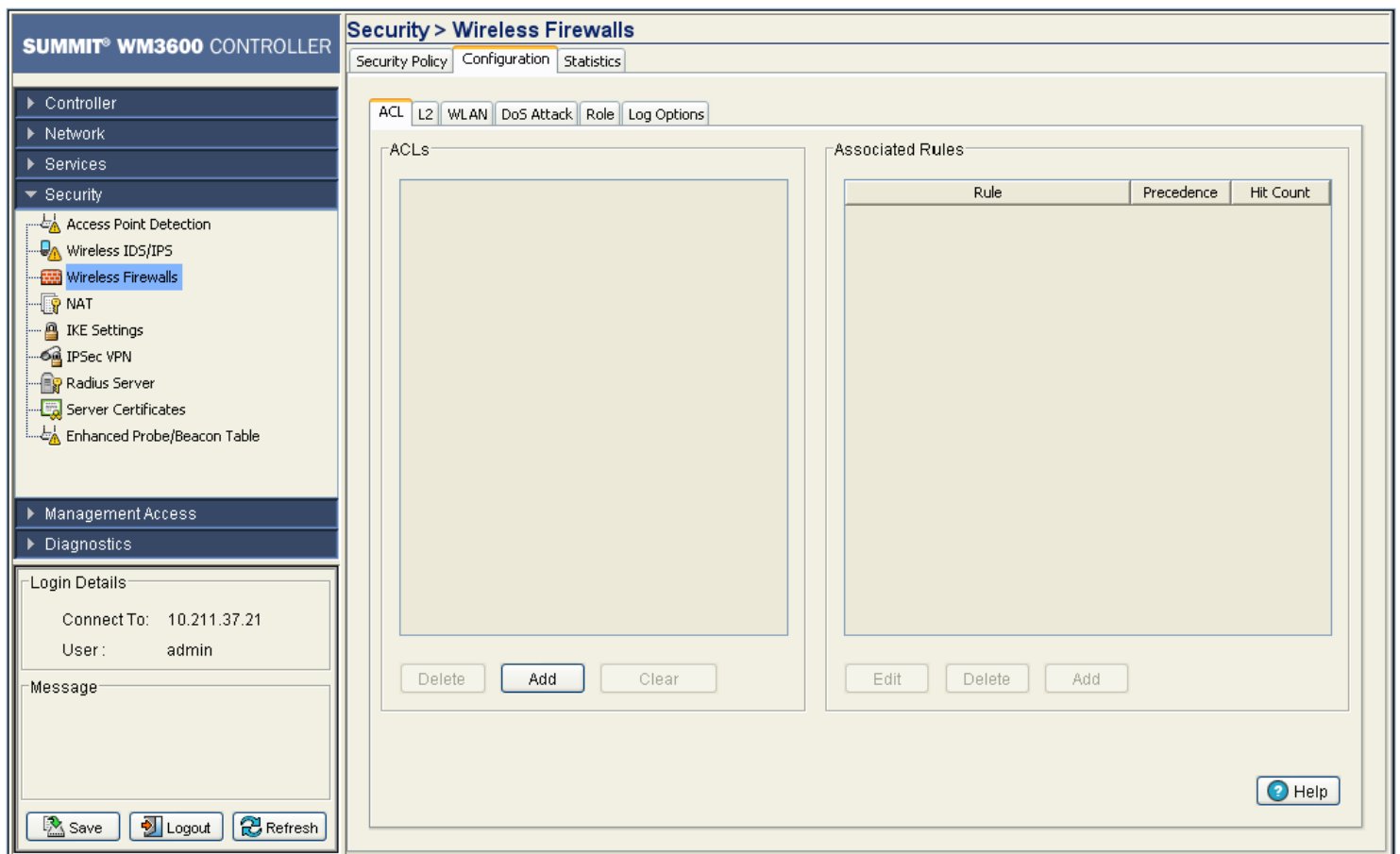
Configure the Firewall to create either standard/extended ip or extended MAC access control lists.

To configure the Firewall:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *ACL* tab.
- 4 Add a new ACL entry as explained in [“Adding a New ACL” on page 421](#).

5 The Configuration tab consists of the following two fields:

- *ACLs*—existing access lists
- *Associated Rules*—allow/deny rules



The *ACLs* field displays the list of ACLs currently associated with the controller. An ACL contains an ordered list of ACEs. Each ACE specifies a permit or deny designation and a set of conditions the packet must satisfy to match the ACE. Because the controller stops testing conditions after the first match, the order of conditions in the list is critical.

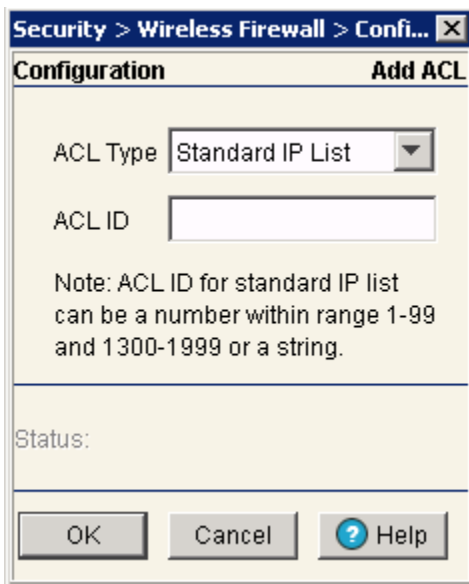
- 6 If an existing ACL no longer satisfies controller access control requirements, select it from among the existing ACLs and click the *Delete* button.
- 7 Use the *Add* button (within the *ACLs* field) to add an additional ACL. For more information, see [“Adding a New ACL” on page 421](#).
- 8 To reset the *Hit Count* number, click the *Clear Counters* button.
- 9 Refer to the *Associated Rules* field to assess the rules and precedence associated with each ACL. If necessary, rules and can be added or existing rules modified. For more information, see [“Adding a New ACL Rule” on page 422](#).

Adding a New ACL

When a packet is received by the controller, the controller compares the packet against the ACL to verify the packet has the required permissions to be forwarded. Often, ACLs need to be added as client permission changes during controller operation.

To create a new ACL:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *ACL* tab to view the list of ACLs currently associated with the controller.
- 4 Click the *Add* button.



- 5 Select an *ACL Type* from the drop-down menu. The following options are available:
 - *Standard IP List*—Uses source IP addresses for matching operations.
 - *Extended IP List*—Uses source and destination IP addresses and optional protocol information for matching operations.
 - *MAC Extended List*—Uses source and destination MAC addresses, VLAN ID and optional protocol information.
- 6 Enter a numeric index name for the ACL in the *ACL ID* field.
- 7 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to use the changes to the running configuration and close the dialog.
- 9 Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding a New ACL Rule

To add a new rule:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *ACL* tab.

- Click the *Add* button within the Associated Rules field.

The screenshot shows a dialog box titled "Add Rule" with a close button (X) in the top right corner. The dialog is for an "ACL Type : Standard IP". It contains the following fields and controls:

- Precedence(1 - 5000)**: A text input field.
- Operation**: A dropdown menu currently set to "deny".
- Logging**: A checkbox that is unchecked.
- Attribute to mark**: A section containing three checkboxes and text input fields:
 - 802.1p(0 - 7)
 - TOS(0 - 255)
 - DSCP(0 - 63)
- Filters**: A section containing:
 - Source Address**: A text input field.
 - Source Wildcard/Mask**: A dropdown menu currently set to "any".
- Status**: A text input field.
- Buttons: **OK**, **Cancel**, and **Help** (with a question mark icon).

- Use the *Precedence* field to enter a precedence (priority) value between 1 and 5000.
The rules within an ACL will be applied to packets based on their precedence value. Rules with lower precedence are always applied first.



NOTE

If adding an access control entry to an ACL using the controller SNMP interface, Precedence is a required parameter.

- Use the *Operation* drop-down menu to define a permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority.
- Select the *Logging* checkbox to generate log messages when a packet has been forwarded, denied or marked based on the criteria specified in the access lists.
- If *mark* is selected from within the *Operations* drop-down menu, the *Attribute to mark* field is enabled. Select the 802.1p (0–7) or TOS(0–255) or DSCP(0–63) checkbox and define the attribute receiving priority with this ACL mark designation.
- From within the *Filters* field, select a *Source Mask Length* from the drop-down menu.
The *Source Mask Length* is the size of the network or host (in mask format). The mask length defines a match based on the Network / Host.

- 10 Use the *Source Address* field to enter the IP address where the packets are sourced.
- 11 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 12 Click *OK* to use the changes to the running configuration and close the dialog.
- 13 Click *Cancel* to close the dialog without committing updates to the running configuration.

Editing an Existing Rule

As network and access permission requirements change, existing ACL rules need to be modified to be relevant with new client access requests.

To modify an existing ACL rule:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *ACL* tab.
- 4 Select an ACL from the *ACLs* field.
The rules associated with the selected ACL display in the *Associated Rules* section.
- 5 Click the *Edit* button within the *Associated Rules* field.

Edit Rule ACL Type : Standard IP

Precedence(1 - 5000)

Operation

Logging

Attribute to mark

802.1p(0 - 7)

TOS(0 - 255)

DSCP(0 - 63)

Filters

Source Address

Source Wildcard/Mask

Status:

- 6 Use the *Precedence* field to modify the precedence (priority) between 1 and 5000.

The rules within an ACL are applied to packets based on their precedence value. Rules with lower precedence are always applied first.



NOTE

If adding an access control entry to an ACL using the controller SNMP interface, Precedence is a required parameter.

- 7 Use the *Operation* drop-down menu (if necessary) to modify the permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority.
- 8 Select the *Logging* checkbox to generate log messages when a packet has been forwarded, denied or marked based on the criteria specified in the access lists.
- 9 If *mark* is selected from within the *Operations* drop-down menu, the *Attribute to mark* field becomes enabled. If necessary, select the *802.1p (0–7)* or *TOS(0–255)* checkbox and define the attribute receiving priority with this ACL mark designation.
- 10 From within the *Filters* field, modify (if necessary) the *Source Mask Length* from the drop-down menu. The source is the source address of the network or host in dotted decimal format. The Source-mask is the network mask.
- 11 Use the *Source Address* field to revise (if necessary) the IP address where the packets are sourced.



NOTE

If an Extended IP ACL is used, a Destination Wildcard/Mask and Destination Address are required.

- 12 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 13 Click *OK* to use the changes to the running configuration and close the dialog.
- 14 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Layer 2 Firewall

To review Layer 2 firewall rules:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *L2* tab.

4 The L2 tab contains the following information:

SUMMIT® WM3600 CONTROLLER Security > Wireless Firewalls

Security Policy Configuration Statistics

ACL L2 WLAN DoS Attack Role Log Options

Interface Name	ARP Rate	DHCP Trust	ARP Trust	Broadcast Storm Threshold	Multicast Storm Threshold	Unknown Unicast Storm
ge1	0	✓	✗	0	0	0
ge2	0	✓	✗	0	0	0
ge3	0	✓	✗	0	0	0
ge4	0	✓	✗	0	0	0
ge5	0	✓	✗	0	0	0
ge6	0	✓	✗	0	0	0
ge7	0	✓	✗	0	0	0
ge8	0	✓	✗	0	0	0
up1	0	✓	✗	0	0	0
tunnel1	0	✓	✗	0	0	0

Edit Delete Add Help

- Interface Name Displays the interface associated with the Layer 2 firewall. Available Layer 2 interfaces are: in WM3400 ge1-5 and up1; in WM3600 ge 1-8 and up1; and in WM3700 ge 1-4.
- ARP Rate Displays the Address Resolution Protocol (ARP) rate. Rates can be between 1 and 1000000
- DHCP Trust Displays the DHCP trust status for the selected L2 interface. Any DHCP packets from a DHCP server connected to the selected interface is considered trusted. These DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. By default all physical interfaces are DHCP trusted. Onboard DHCP server is also trusted as the controller's local port is always trusted. When DHCP trust is enabled, a green checkmark is displayed. when disabled, a red 'X' is displayed.
- ARP Trust Displays the ARP trust status for the selected L2 interface. Trusted ARP packets are also used to update the DHCP Snoop Table to prevent IP spoof and arp-cache-poisoning attacks. By default, none of the physical or aggregate interfaces are ARP trusted.
- Broadcast Storm Threshold Displays the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

Multicast Storm Threshold	Displays the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.
Unknown Unicast Storm	Displays the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

Adding Layer 2 Firewall Configurations

To configure new Layer 2 firewall rules:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *L2* tab.
- 4 Click the *Add* button.

- 5 Configure the following values for each new Layer 2 configuration:

Interface Name	Assign the interface to be associated with the Layer 2 firewall. Available Layer 2 interfaces are: in WM3400 ge1-5 and up1; in WM3600 ge 1-8 and up1; and in WM3700 ge 1-4.
ARP Rate	Specify the Address Resolution Protocol (ARP) rate. Rates can be between 1 and 1000000.
DHCP Trust	Select to enable DHCP trust on this interface. A DHCP server must always be connected to an interface that has its DHCP trust enabled.

ARP Trust	Select to enable ARP trust on this interface. ARP packets received on this interface are considered trusted and information from these packets is used to identify rogue devices.
Broadcast Storm Threshold	Configure the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.
Multicast Storm Threshold	Configure the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.
Unknown Unicast Storm	Configure the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 1-1000000 packets per second.

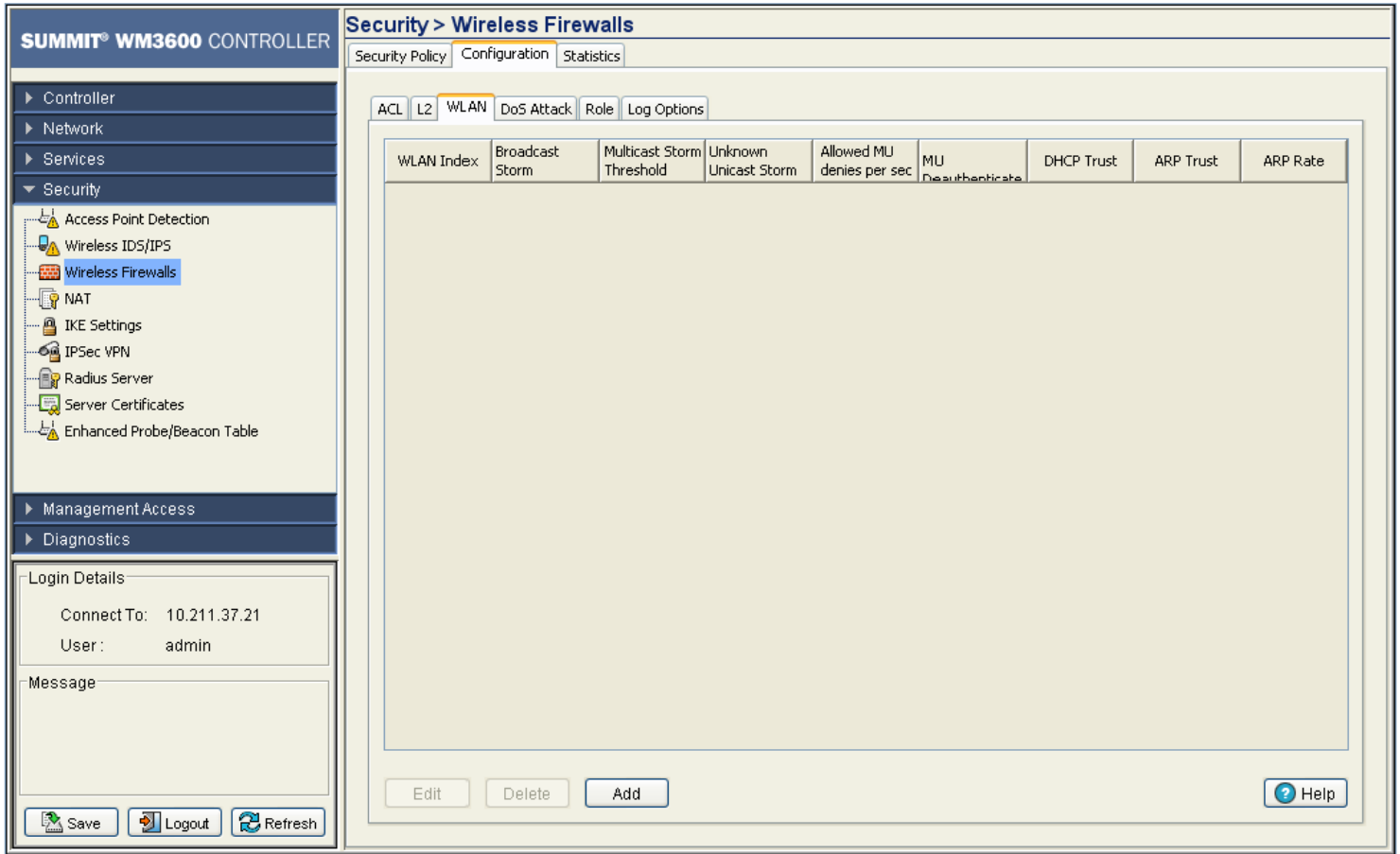
- 6 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to use the changes to the running configuration and close the dialog.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring WLAN Firewall rules

To review WLAN firewall rules:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *WLAN* tab.

4 The WLAN tab contains the following information:



WLAN Index	Displays the WLAN index number. This number is configured on the wireless LAN configuration page.
Broadcast Storm Threshold	Displays the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.
Multicast Storm Threshold	Displays the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.
Unknown Unicast Storm	Displays the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.
Allowed MU denies per sec	Displays the permissible number of denied packets per second that a mobile unit on this WLAN may send before it is deauthenticated. The threshold range is 0-1000000 packets per second.

MU Deauthenticate	Displays whether or not mobile unit deauthentication is enabled for each WLAN. If <i>MU Deauthenticate</i> is enabled any associated mobile unit which hit the thresholds configured for Allowed MU denies per second will be deauthenticated. If MU Deauthenticate is enabled a green checkmark will be displayed. When it is disabled a red “X” will be displayed.
DHCP Trust	Displays the DHCP trust status for the selected WLAN. These DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. Any DHCP packets from a DHCP server connected to the selected WLAN is considered trusted. By default all WLANs are not DHCP trusted. When DHCP trust is enabled, a green checkmark is displayed. when disabled, a red 'X' is displayed.
ARP Trust	Displays the ARP trust status for the selected WLAN. Trusted ARP packets are also used to update the DHCP Snoop Table to prevent IP spoof and arp-cache-poisoning attacks. By default, none of the WLANs are ARP trusted.
ARP Rate	Displays the Address Resolution Protocol (ARP) rate threshold. The ARP threshold determines the number of ARP packets permissible per second. Rates can be between 0 and 1000000

- 5 If the properties of an existing WLAN firewall setting fulfill to your needs but still require modification to better filter traffic, select the WLAN and click the *Edit* button.
- 6 If an existing WLAN firewall rule is now obsolete, select it from those listed and click the *Delete* button.
- 7 Click the *Add* button to create a new WLAN firewall rule. For more information, see [“Adding a new WLAN Firewall Rule” on page 430](#).

Adding a new WLAN Firewall Rule

To add new WLAN firewall rules:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *WLAN* tab.

4 Click the *Add* button.

5 To create a new WLAN Firewall rule configure the following information:

WLAN Index	Select a WLAN index number from the pulldown menu. This number is configured on the wireless LAN configuration page.
Broadcast Storm Threshold	Enter the Broadcast Storm Threshold for each interface. When the rate of broadcast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The valid threshold range is 0-1000000 packets per second.
Multicast Storm Threshold	Enter the Multicast Storm Threshold for each interface. When the rate of multicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The valid threshold range is 0-1000000 packets per second.
Unknown Unicast Storm	Enter the Unknown Unicast Storm Threshold for each interface. When the rate of unknown unicast packets exceeds the high threshold configured for an interface, packets are throttled till the rate falls below the configured rate. Thresholds are configured in terms of packets per second. The threshold range is 0-1000000 packets per second.
Allowed MU denies per sec	Configure the permissible number of denied packets per second that a mobile unit on this WLAN may send before it is deauthenticated. The threshold range is 0-1000000 packets per second.
MU Deauthenticate	Configure whether or not mobile unit deauthentication is enabled for each WLAN. If <i>MU Deauthenticate</i> is enabled, any associated mobile unit which hit the thresholds configured for storm traffic will be deauthenticated. To enable deauthentication, check the box.

DHCP Trust	Select to enable DHCP trust on this WLAN. When disabled, any DHCP packets received on the interface is dropped.
ARP Trust	Select to enable ARP trust on this WLAN. ARP packets received on this interface are considered trusted and information from these packets is used to identify rogue devices.
ARP Rate	Enter the Address Resolution Protocol (ARP) threshold. The ARP threshold determines the number of ARP packets permissible per second. Rates can be between 0 and 1000000

- 6 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to use the changes to the running configuration and close the dialog.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Denial of Service (DoS) Attack Firewall Rules

To review Denial of Service Attack firewall rules:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *DoS Attack* tab.

4 The DoS Attack tab contains the following information:

The screenshot shows the configuration page for the DoS Attack tab in the Summit WM3600 Controller. The page is titled "Security > Wireless Firewalls" and has tabs for "Security Policy", "Configuration", and "Statistics". The "Configuration" tab is active, and the "DoS Attack" sub-tab is selected. Below the sub-tabs, there is a table with columns: Type, Check Enabled, Logging Level, Attack Count, and Last Occurrence. The table lists 28 different DoS attack types, all of which are currently enabled (indicated by a green checkmark) and set to a "Warning" logging level. The attack count for all types is 0, and the last occurrence is 0:00:00.00. Below the table, there is a note: "Click on Log Level to edit, press TAB and Apply when done or ESCAPE to abort". At the bottom of the page, there are buttons for "Enable", "Disable", "Enable All", "Disable All", "Clear", "Apply", "Revert", and "Help".

Type	Check Enabled	Logging Level	Attack Count	Last Occurrence
Smurf	✓	Warning	0	0:00:00.00
Twinge	✓	Warning	0	0:00:00.00
Invalid IP Protocol	✓	Warning	0	0:00:00.00
Ascend	✓	Warning	0	0:00:00.00
Chargen	✓	Warning	0	0:00:00.00
Fraggle	✓	Warning	0	0:00:00.00
ICMP Router Solicit	✓	Warning	0	0:00:00.00
ICMP Router Advt	✓	Warning	0	0:00:00.00
IP Route Opt	✓	Warning	0	0:00:00.00
Snork	✓	Warning	0	0:00:00.00
FTP Bounce	✓	Warning	0	0:00:00.00
TCP Intercept	✓	Warning	0	0:00:00.00
Bcast/Mcast ICMP	✓	Warning	0	0:00:00.00
TCP Header Fragmented	✓	Warning	0	0:00:00.00
WinNuke	✓	Warning	0	0:00:00.00
Land	✓	Warning	0	0:00:00.00
UDP Short Header	✓	Warning	0	0:00:00.00
TCP Bad Sequence	✓	Warning	0	0:00:00.00
TCP Fin Scan	✓	Warning	0	0:00:00.00
TCP Null Scan	✓	Warning	0	0:00:00.00
TCP Xmas Scan	✓	Warning	0	0:00:00.00
TCP Post Syn	✓	Warning	0	0:00:00.00
IP TTL Zero	✓	Warning	0	0:00:00.00
IP Spoof	✓	Warning	0	0:00:00.00

- Type** Displays the Denial of Service attack type. The controller currently supports enabling or disabling 28 types of DoS attack filters.
- Check Enabled** This field will show a green checkmark next to the Denial of Service Attack filters that are enabled on the controller firewall. When a DoS Attack filter is disabled a red "X" will be shown in this column.
- Logging Level** The Logging Level field displays the level of Syslog logging enabled for each DoS Attack filter. The logging level uses standard Syslog levels of:
- Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Info
 - Debug
 - None
- To change the logging level, click on the specific field and choose the logging level from the pull-down menu.

Attack Count	Displays the number of times that each DoS attack have been observed by the controller firewall. Clicking the <i>Clear Stats</i> button on this page will reset all <i>Attack Counts</i> to 0.
Last Occurrence	Displays the amount of time since each DoS attack has been observed by the controller firewall. Clicking the <i>Clear Stats</i> button on this page will reset all <i>Last Occurrence</i> timers to 0:00:00.00.

- 5 To enable a Denial of Service Attack filter, select a disabled rule from the table and click the *Enable* button. The *Check Enabled* field will show a green checkmark next to the Denial of Service Attack filters that are enabled on the controller firewall.
- 6 To disable a Denial of Service Attack filter, select an enabled rule from the table and click the *Disable* button. When a DoS Attack filter is disabled a red "X" will be shown in the *Check Enabled* column.

**NOTE**

Of the 28 DoS Attack filters supported by the controller, 10 can be disabled individually. Those filters are:

- Smurf
 - Twinge
 - Invalid IP protocol
 - ICMP router advertisement
 - Src ip route
 - Echo ports
 - Snork
 - FTP bounce
 - TCP intercept
 - Bcast Mcast ICMP
-

- 7 To enable all Denial of Service Attack filters, click the *Enable All* button. The *Check Enabled* field will show a green checkmark next to the Denial of Service Attack filters that are enabled on the controller firewall.
- 8 To disable all Denial of Service Attack filters, click the *Disable All* button. When a DoS Attack filter is disabled a red "X" will be shown in the *Check Enabled* column.
- 9 To clear statistics for Denial of Service Attacks, click the *Clear Stats* button. This will reset all *Attack Counts* to 0 and all *Last Occurrence* times to 0:00:00.00.
- 10 Click the *Apply* button to save the changes made within the DoS Attach screen.
- 11 Click the *Revert* button to cancel any changes made within the DoS Attach screen and revert back to the last saved configuration.

Configuring the Role

To view configured roles:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.

3 Click the *Role* tab.

The screenshot shows the configuration page for Wireless Firewalls Roles. The left sidebar contains a navigation tree with 'Security > Wireless Firewalls' selected. The main content area has tabs for 'ACL', 'L2', 'WLAN', 'DoS Attack', 'Role', and 'Log Options'. The 'Role' tab is active, showing a checkbox for 'Role Assignment Immediate' and 'Apply' and 'Revert' buttons. Below is a table with the following data:

Sequence Number	Role Name	AP Location	ESSID	MU MAC Address	Group Name
10001	default-role			00-00-00-00-00-00	

At the bottom of the table are 'Edit', 'Delete', and 'Add' buttons, and a 'Help' button in the bottom right corner.

4 Select the checkbox Role Assignment Immediate and click Apply to assign the role immediately.

5 Role configuration screen displays the following information:

- Sequence Number** Displays the sequence number associated with each role. Sequence numbers determine the order in which roles are applied. Roles with lower sequence numbers are applied before those with higher sequence numbers. Sequence numbers are assigned when a role is created and cannot be edited.
- Role Name** Displays the name of each role. The role name is configured when the role is created and cannot be edited.
- AP Location** Displays the AP Location filters, if any, applied to each role. The AP location filters can be set when the role is created or may be edited by selecting a role and clicking the *Edit* button.
- ESSID** Displays the ESSID filters, if any, applied to each role. The ESSID location filters can be set when the role is created or may be edited by selecting a role and clicking the *Edit* button.
- MU MAC Address** Displays the MU MAC Address filters, if any, applied to each role. The MU MAC Address filters can be set when the role is created or may be edited by selecting a role and clicking the *Edit* button.
- Group Name** Displays the RADIUS Group name, if any, that is associated with each role. The Group Name filters can be set when the role is created or may be edited by selecting a role and clicking the *Edit* button.

- 6 To create a new role, click the *Add* button. For more information see [“Creating a new Role” on page 436](#).
- 7 To edit an existing role, click the *Edit* button and modify the filter settings.
- 8 To remove a role, select that rule from the table and click the *Delete* button. A confirmation will be displayed before the rule is deleted from the controller.

Creating a new Role

To add new role:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *Role* tab.

4 Click the *Add* button.

Security > Wireless Firewall > ADD

Configuration

Sequence No. (1 - 10000) Role Name

AP Location Any

ESSID Any

Group Name Any

MU MAC Any

MU MAC

MU MAC Mask

Authentication

Any

No Authentication

802.1X EAP

Kerberos

Hotspot

MAC Authentication

Encryption

Any

No Encryption

WEP 64

WEP 128

TKIP

CCMP

TKIP-CCMP

KeyGuard

WEP 128 KeyGuard

Status:

5 To create a new role configure the following information:

- | | |
|-----------------|--|
| Sequence Number | Enter a sequence number to be associated with each role. Sequence numbers determine the order that role are applied. Roles with lower sequence numbers are applied before those with higher sequence numbers. Sequence numbers are assigned when a role is created and cannot be edited. |
| Role Name | Enter a name for each role. The role name is configured when the role is created and cannot be edited. |

AP Location	<p>Select an AP Location filter, if any, to apply to the role.</p> <p>Available AP Location filters are:</p> <ul style="list-style-type: none"> • <i>Exact</i>: The role will only be applied to APs with the exact location string specified in the role. • <i>Contains</i>: The role will be applied to APs whose location contains the location string specified in the role. • <i>Not Contains</i>: The role will be applied to APs whose location does not contain the location string specified in the role. • <i>Any</i>: The role will be applied to any AP Locations.
ESSID	<p>Select an ESSID filter, if any, to apply to the role.</p> <p>Available ESSID filters are:</p> <ul style="list-style-type: none"> • <i>Exact</i>: The role will only be applied when the exact ESSID string specified in the role. • <i>Contains</i>: The role will be applied when the ESSID contains the string specified in the role. • <i>Not Contains</i>: The role will be applied when the ESSID does not contain the string specified in the role. • <i>Any</i>: The role will be applied to any ESSIDs.
Group Name	<p>Select a Group Name filter, if any, to apply to the role.</p> <p>Available Group Name filters are:</p> <ul style="list-style-type: none"> • <i>Exact</i>: The role will only be applied when the exact RADIUS Group Name string specified in the role. • <i>Contains</i>: The role will be applied when the RADIUS Group Name contains the string specified in the role. • <i>Not Contains</i>: The role will be applied to when the RADIUS Group Name does not contain the string specified in the role. • <i>Any</i>: The role will be applied to any RADIUS Group Name.
MU MAC Address	<p>Configure the MU MAC Address filters, if any, applied to each role. The MU MAC Address filter can be set to apply the role to any MU MAC Address or a specific MU MAC Address or a MU MAC Mask.</p>
Authentication	<p>Select an Authentication filter, if any, to apply to the role.</p> <p>Available Authentication filters are:</p> <ul style="list-style-type: none"> • <i>Equals</i>: The role will only be applied when the Authentication type matches the exact Authentication method specified in the role. • <i>Not Equals</i>: The role will only be applied when the Authentication type does not match the exact Authentication method specified in the role. • <i>Any</i>: The role will be applied to any Authentication type.
Encryption	<p>Select an Encryption filter, if any, to apply to the role.</p> <p>Available Encryption filters are:</p> <ul style="list-style-type: none"> • <i>Equals</i>: The role will only be applied when the Encryption type matches the exact Encryption method specified in the role. • <i>Not Equals</i>: The role will only be applied when the Encryption type does not match the exact Encryption method specified in the role. • <i>Any</i>: The role will be applied to any Encryption type.

6 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

7 Click *OK* to use the changes to the running configuration and close the dialog.

8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Firewall Logging Options

To view firewall logging rules:

- 1 Select *Security > Wireless Firewall* from the main tree menu.
- 2 Click the *Configuration* tab.
- 3 Click the *Log Options* tab.

The screenshot displays the configuration interface for a Summit WM3600 Controller. The left sidebar shows the navigation tree with 'Security > Wireless Firewalls' selected. The main panel is titled 'Security > Wireless Firewalls' and has tabs for 'Security Policy', 'Configuration', and 'Statistics'. Under the 'Configuration' tab, there are sub-tabs for 'ACL', 'L2', 'WLAN', 'DoS Attack', 'Role', and 'Log Options', with 'Log Options' currently active. The 'Log Options' section contains a text box stating: 'Log will be enabled only when threshold set in L2/WLAN config is exceeded.' Below this, there are four log options, each with a 'Disabled' dropdown menu: 'Arp Log', 'Broadcast Log', 'Multicast Log', and 'Unknown Unicast Log'. At the bottom right of the configuration area are 'Apply', 'Revert', and 'Help' buttons. The bottom left of the interface shows a 'Login Details' section with 'Connect To: 10.211.37.21' and 'User: admin', and a 'Message' field. At the very bottom are 'Save', 'Logout', and 'Refresh' buttons.

4 Select the Syslog logging levels for each of the following log types:

ARP Log	<p>The <i>ARP Log</i> field displays the level of Syslog logging enabled for excessive ARP on an interface. The logging level uses standard Syslog levels of:</p> <ul style="list-style-type: none">• Emergency• Alert• Critical• Error• Warning• Notice• Info• Debug• Disabled <p>To change the logging level, click the specific field and choose the logging level from the pulldown menu.</p>
Broadcast Log	<p>The <i>Broadcast Log</i> field displays the level of syslog logging enabled for excessive broadcasts on an interface.</p> <p>The logging level uses standard Syslog levels of:</p> <ul style="list-style-type: none">• Emergency• Alert• Critical• Error• Warning• Notice• Info• Debug• Disabled <p>To change the logging level, click the specific field and choose the logging level from the pulldown menu.</p>
Multicast Log	<p>The <i>Multicast Log</i> field displays the level of syslog logging enabled for excessive multicast on an interface.</p> <p>The logging level uses standard Syslog levels of:</p> <ul style="list-style-type: none">• Emergency• Alert• Critical• Error• Warning• Notice• Info• Debug• Disabled <p>To change the logging level, click the specific field and choose the logging level from the pulldown menu.</p>

Unknown Unicast Log

The *Unknown Unicast Log* field displays the level of syslog logging enabled for excessive unknown unicasts on an interface. The logging level uses standard Syslog levels of:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug
- Disabled

To change the logging level, click the specific field and choose the logging level from the pulldown menu.

- 5 When all logging options have been modified, click the *Apply* button to commit those changes to the controller.
- 6 To undo any changes and go back to the previously saved logging options, click the *Revert* button.

Reviewing Firewall and ACL Statistics

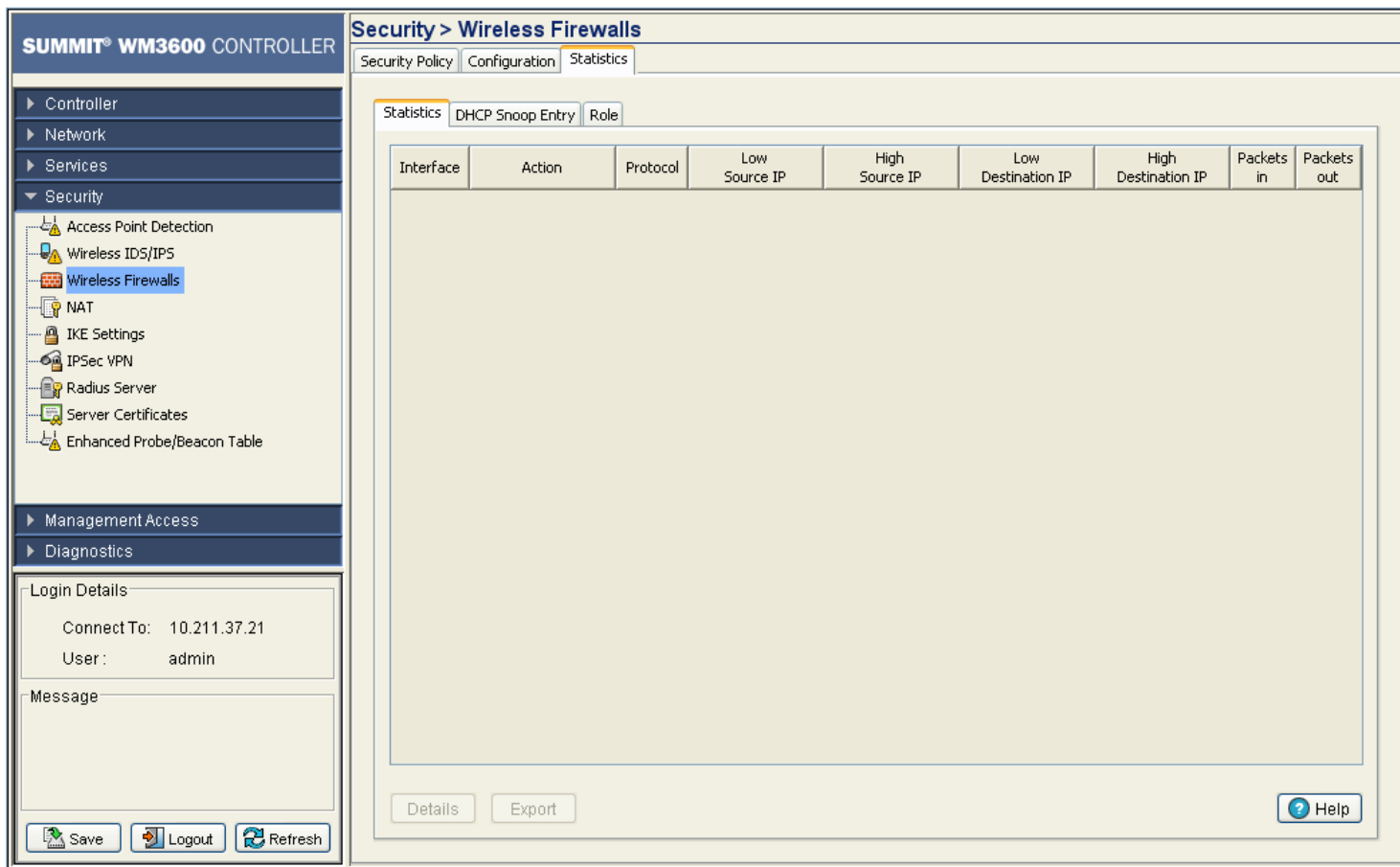
Use the *Statistics* tab to view set of statistics for *ACL*, *DHCP Snoop Entry* and *Role* based firewalls.

Reviewing ACL Statistics

To review ACL statistics:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Statistics* tab.

3 From the *Statistics* section select the *Statistics* tab.



4 Refer to the following information as displayed within the *Statistics* tab:

Interface	Displays the physical/virtual interfaces used to add the ACL association to the controller.
Action	Displays the permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority.
Protocol	Displays the permit, deny or mark designation for the ACL. If the action is to mark, the packet is tagged for priority or "type of service."
Low Source IP	Displays the Low Source IP Address from where the packets are sourced.
High Source IP	Displays the High Source (highest address in available range) IP Address from where the packets are sourced.
Low Destination IP	Displays the Low Destination (lowest address in available range) IP Address.
High Destination IP	Displays the High Destination IP Address.
Packets In	Displays the number of packets (in bytes) transmitted over the ACL.
Packets Out	Displays the number of instances this ACL has been used. Periodically review to determine whether specific ACLs should be deleted or modified to make relevant.

- 5 Select an interface and click the *Details* button to display a more robust set of statistics for the selected interface.

Details			
Index	22444	Rule Precedence	14
Interface	vlan1	Action	permit
Protocol	ip	Times Used	0
Low Source IP	0.0.0.0	High Source IP	255.255.255.255
Low Destination IP	0.0.0.0	High Destination IP	255.255.255.255
Active Flows	0	Total Flows	0
Packets in	0		
Packets out	0		

Status:

- 6 Click the *Export* to export the selected ACL attribute to a user specified location.

Viewing DHCP Snoop Entry Statistics

To review DHCP Snoop Entry statistics:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Statistics* tab.

3 From the *Statistics* section select the *DHCP Snoop Entry* tab.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation menu with categories: Controller, Network, Services, Security, Management Access, and Diagnostics. The Security section is expanded, showing sub-items like Access Point Detection, Wireless IDS/IPS, Wireless Firewalls (highlighted), NAT, IKE Settings, IPSec VPN, Radius Server, Server Certificates, and Enhanced Probe/Beacon Table. The main content area is titled "Security > Wireless Firewalls" and has tabs for Security Policy, Configuration, and Statistics. The Statistics tab is active, and the "DHCP Snoop Entry" sub-tab is selected. The table displays two entries with columns for Client IP Address, VLAN ID, MAC Address, Type, Lease Time, and Ingress Source. The status bar at the bottom indicates "Filtering is disabled" and "Page 1 of 1 loaded." A Help button is visible in the bottom right corner.

Client IP Address	VLAN ID	MAC Address	Type	Lease Time	Ingress Source
10 . 211 . 37 . 1		1 00-04-96-1F-A7-73	Router-DhcpServer		0 ge7
10 . 211 . 37 . 21		1 00-04-96-42-15-6B	DhcpClient	5011200	localport

4 Refer to the following information as displayed within the *DHCP Snoop Entry* tab:

Client IP Address	Displays the DHCP Client IP Address for each entry.
VLAN ID	Displays the VLAN ID number, if any, for each entry in the DHCP Snoop Entry table. The range is <1-4094>. The default value is 1.
MAC Address	Displays the MAC Address of each DHCP Client, DHCP Server or Router in the table.
Type	Displays the type for each DHCP Snoop Entry. Available entry types are: <ul style="list-style-type: none"> • DHCP Client • DHCP Server • Router • DHCP Server Router • DHCP Client Router
Lease Time	Displays the DHCP remaining Lease Time for each entry in the table.
Ingress Source	Displays the MU port number for each entry in the DHCP Snoop Entry table.

Viewing Role Based Firewall Statistics

The Role Based Firewall statistics information displays a list of mobile units associated with each role name.

To review Role Based Firewall statistics:

- 1 Select *Security > Wireless Firewall* from the main menu tree.
- 2 Click the *Statistics* tab.
- 3 From the *Statistics* section select the *Role* tab.

The screenshot displays the Summit WM3600 Controller web interface. The left sidebar shows a navigation tree with 'Security' expanded to 'Wireless Firewalls'. The main content area is titled 'Security > Wireless Firewalls' and has three tabs: 'Security Policy', 'Configuration', and 'Statistics'. The 'Statistics' tab is active, and within it, the 'Role' sub-tab is selected. The main area contains two large empty rectangular boxes labeled 'Role Name' and 'Assigned MUs'. At the bottom right of the main area is a 'Help' button. The bottom of the interface features a 'Login Details' section with 'Connect To: 10.211.37.21' and 'User: admin', a 'Message' field, and buttons for 'Save', 'Logout', and 'Refresh'.

- 4 Refer to the following information as displayed within the *Role* tab:

Role Name	Displays the <i>Role Names</i> for all roles that are active and have mobile units associated with them.
Assigned MUs	Clicking on a <i>Role Name</i> will display all mobile units that are associated with the selected role.

Configuring NAT Information

Network Address Translation NAT provides the translation of an *Internet Protocol* (IP) address within one network to a different, known IP address within another network. One network is designated as the private network, while the other is public. NAT provides a layer of security by translating private (local)

network addresses to one or more public IP addresses. For example, when an administrator wants to allow individuals on the WAN side access to a particular FTP or Web server located on one of the LAN subnets but does not want to permit any other access, NAT is the appropriate solution.

Using NAT, a user can mark one or more interfaces as inside or outside. When a user creates a NAT rule for inside or outside application, it is applied on all the interfaces marked as inside or outside respectively. NAT operates on the controller to connect two networks together. An inside network is assigned addresses requiring conversion into valid addresses before packets can be forwarded to an outside network. The translation process operates in parallel with packet routing.

NAT enables network administrators to move a Web or FTP Server to another host without having to troubleshoot broken links. Change the inbound mapping with the new inside local address to reflect the new host. Configure changes to your internal network seamlessly since the only external IP address either belongs to the controller or from a pool of global addresses.

The controller NAT configuration process is divided into the following configuration activities:

- [Defining Dynamic NAT Translations on page 446](#)
- [Defining Static NAT Translations on page 449](#)
- [Configuring NAT Interfaces on page 453](#)
- [Viewing NAT Status on page 455](#)

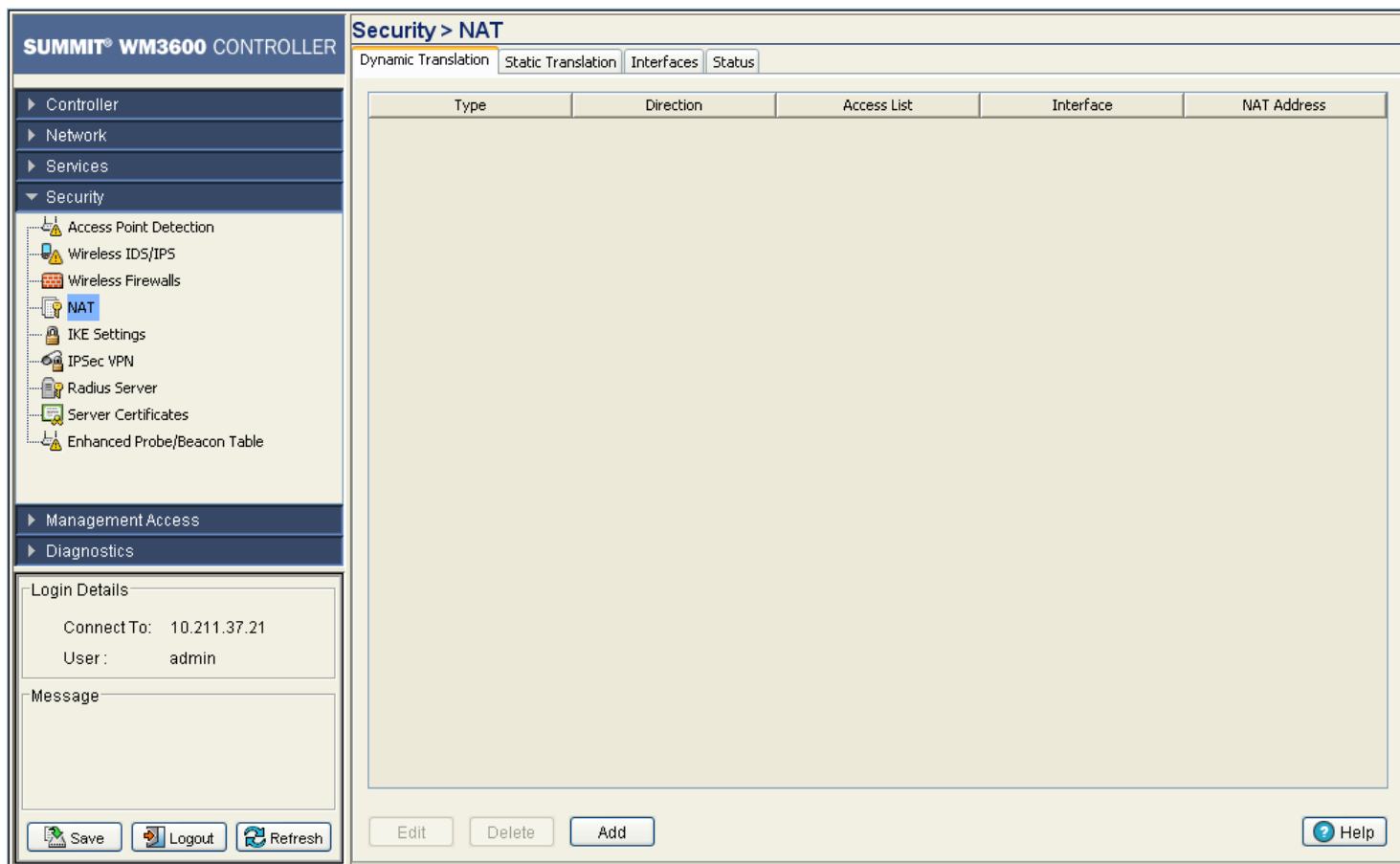
Defining Dynamic NAT Translations

Dynamic NAT translates the IP address of packets going out from one interface to another interface based on the conditions configured in the list. Dynamic NAT requires packets to be controlled through the NAT router to generate translations in the controller translation table.

Refer to the NAT screen's *Dynamic Translation* tab to view existing dynamic NAT configurations available to controller.

To view and add/edit a dynamic NAT configuration:

- 1 Select *Security* > *NAT* from the main menu tree.
- 2 Click the *Dynamic Translation* tab.



3 Refer to the following information as displayed within the *Dynamic Translation* tab.

Type	Displays the NAT type as either: <ul style="list-style-type: none">• <i>Inside</i>—Applies NAT on packets arriving on interfaces marked as inside. These interfaces should be private networks not accessible from outside (public) networks.• <i>Outside</i>—Applies NAT on packets coming in on interfaces marked as outside. These controller interfaces should be public or outside networks accessible from anywhere on the Internet.
Direction	Displays the direction as either: <ul style="list-style-type: none">• <i>Source</i>—The inside network is transmitting data over the network to its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.• <i>Destination</i>—Packets passing through the NAT on the way back to the controller managed LAN are searched against the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the controller managed network.

Access List	Defines the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access-list. Only the Standard IP and Extended IP Access List can be used.
Interface	Defines the interface through which packets are routed. The source IP address and source port number (only if IP protocol is TCP or UDP) of packets is changed to the interface IP address and a random port number.
NAT Address	This is the IP address used during NAT. The users can configure this address.

- 4 Select an existing NAT configuration and click the *Edit* button to modify the settings of this existing NAT configuration. The fields within the Edit screen are similar to those displayed when adding a new NAT configuration.
- 5 Select an existing NAT configuration and click the *Delete* button to remove it from the list of available configurations.
- 6 Click the *Add* button to display a screen to create a new NAT configuration and add it to the list of available configurations. For more information, see [“Adding a New Dynamic NAT Configuration” on page 448](#).

Adding a New Dynamic NAT Configuration

If the existing NAT configurations displayed with the Configuration prove unsuitable for translation, consider creating a new one.

To define a new NAT configuration:

- 1 Select *Security > NAT* from the main menu tree.
- 2 Click the *Dynamic Translation* tab.
- 3 Click the *Add* button.



- 4 Define the NAT *Type* from the drop-down menu. Options include:
 - *Inside*—The set of networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world.
 - *Outside*—All other addresses. Usually these are valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.

-
- 5 Define the NAT *Direction* from the drop-down menu. Options include:
 - *Source*—The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.
 - *Destination*—Packets passing through the NAT on the way back to the controller managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the controller managed network.
 - 6 Use the *Access List* drop-down menu to select the list of addresses used during NAT translation. These addresses (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination
 - 7 Use the *Interface* drop-down menu to select the VLAN used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected represents the intended network traffic within the NAT supported configuration. VLAN1 is available by default.
 - 8 Use the *Enable NAT Address* option to configure an IP address to be used during NAT.
 - 9 Enter the IP address to be used during NAT in the *NAT Address* text field.
 - 10 Refer to the *Status* field for the state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
 - 11 Click *OK* to use the changes to the running configuration and close the dialog.
 - 12 Click *Cancel* to close the dialog without committing updates to the running configuration.

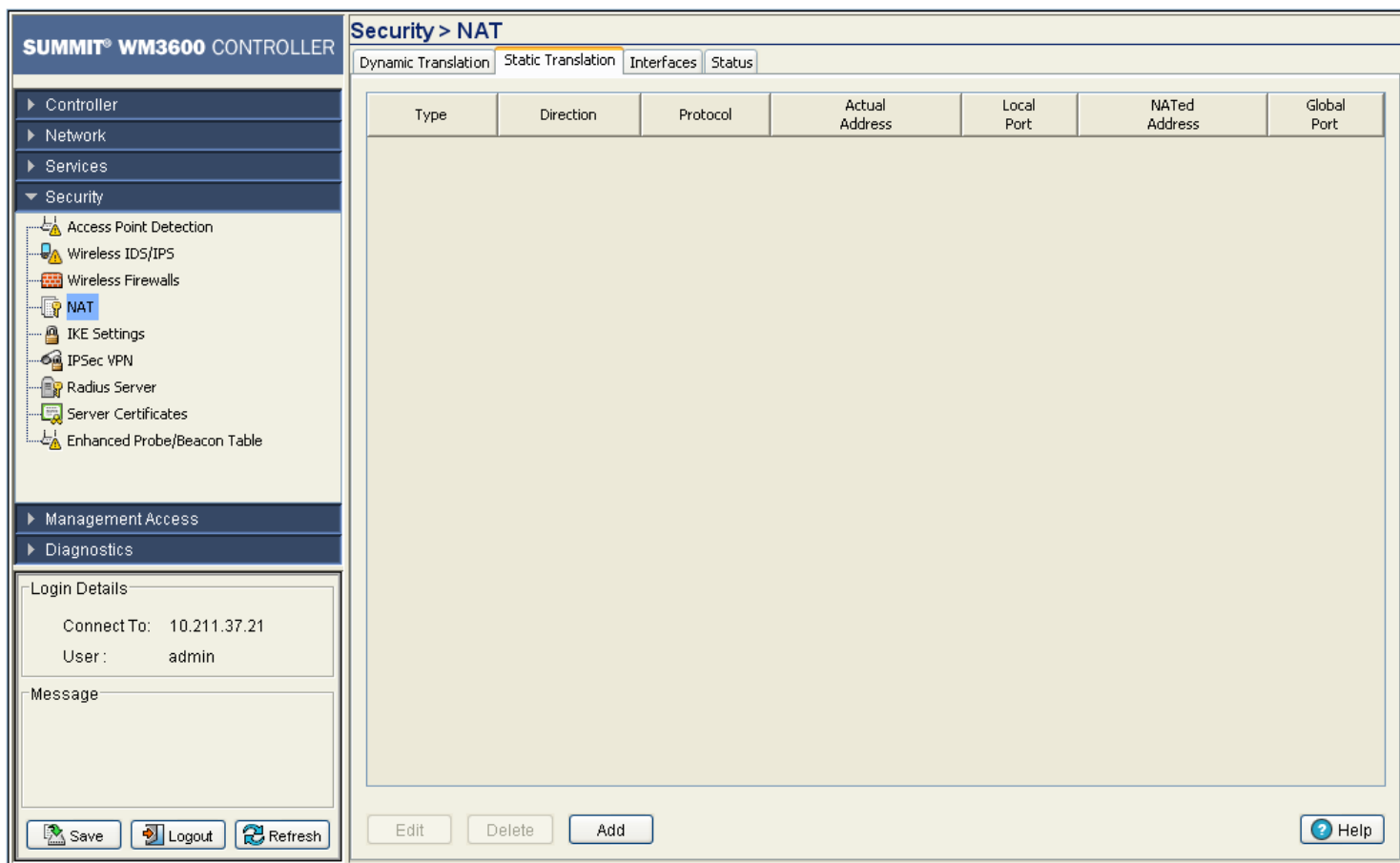
Defining Static NAT Translations

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

Refer to the NAT screen's *Static Translation* tab to view existing static NAT configurations available to controller.

To view and add/edit a dynamic NAT configuration:

- 1 Select *Security* > *NAT* from the main menu tree.
- 2 Click the *Static Translation* tab.



3 Refer to the following information as displayed within the *Static Translation* tab.

- | | |
|-----------|--|
| Type | <p>Displays the NAT type as either:</p> <ul style="list-style-type: none"> • <i>Inside</i>—The set of networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world. • <i>Outside</i>—All other addresses. Usually valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network. |
| Direction | <p>Displays the Direction as either:</p> <ul style="list-style-type: none"> • <i>Source</i>—The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. • <i>Destination</i>—Packets passing through the NAT on the way back to the controller managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address to reach the LAN over the controller managed network. |

Protocol	Displays the tcp or udp option selected for use with the static translation.
Local Address (Actual Address in Summit WM3400)	Displays the Local Address used at the (source) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
Local Port	Applies NAT on packets matching the specified port number. The port number matched can be either source or destination based on the direction specified. This option is valid only if the direction specified is <i>destination</i> .
Global Address (NATed Address in Summit WM3400)	Modifies the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
Global Port	Modifies the port number of the matching packet to the specified value. This option is valid only if the direction specified is <i>destination</i> .

- 4 Select an existing NAT configuration and click the *Edit* button to display screen to modify the settings of this existing NAT configuration. The fields within the Edit screen are similar to those displayed when adding a new NAT configuration.
- 5 Select an existing NAT configuration and click the *Delete* button to remove it from the list of available configurations displayed.
- 6 Click the *Add* button to display screen to create a new NAT configuration and add it to the list of available configurations. For more information, see [“Adding a New Dynamic NAT Configuration” on page 448](#).

Adding a New Static NAT Configuration

If existing NAT configurations prove unsuitable for translation, consider creating a new one.

To define a new NAT configuration:

- 1 Select *Security > NAT* from the main menu tree.
- 2 Click the *Static Translation* tab.

- 3 Click the *Add* button.

- 4 Define the NAT *Type* from the drop-down menu. Options include:
- Inside—The set of networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world.
 - Outside—All other addresses (usually valid addresses located on the Internet). Outside addresses pose no risk if exposed over a publicly accessible network.
- 5 Define the NAT *Direction* from the drop-down menu. Options include:
- Source—The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.
 - Destination—Packets passing through the NAT on the way back to the controller managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address to reach the LAN over the controller managed network.
- 6 Enter the *Local Address (Actual Address in Summit WM3400)* used at the local (source) end of the NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
- 7 Enter the *Local Port (1–65535)* used to for the translation between the controller and its NAT destination.
- 8 Use the *Protocol* drop-down menu to select either *TCP* or *UDP* as the protocol

**NOTE**

After selecting (and saving) a protocol type of TCP or UDP (using the Web UI), the controller CLI will not display the selected protocol type or provide an option to configure it. Ensure both the protocol and port are defined using the Web UI.

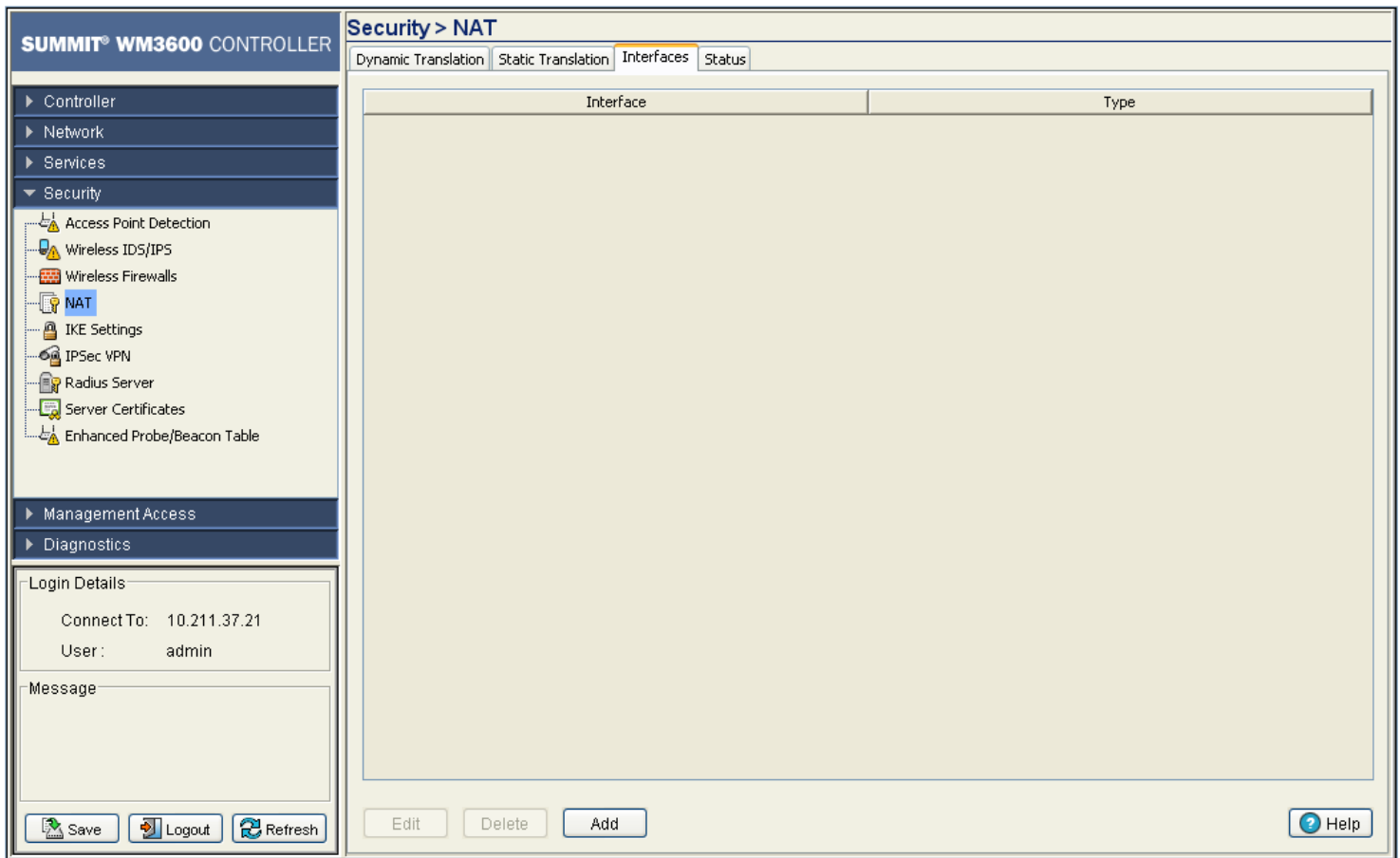
- 9 Enter the *Global Address* (NATed port in Summit WM3400) to assign to a host in the outside network. This should be interpreted as a secure address.
- 10 Displays the *Global Port* used to for the translation between the controller and its NAT destination.
- 11 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something is wrong in the transaction between the applet and the controller.
- 12 Click *OK* to use the changes to the running configuration and close the dialog.
- 13 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring NAT Interfaces

The NAT Interface is the VLAN used to route controller data traffic between the source and destination address locations within the controller-managed network. Any of the default VLANs is available as the NAT interface, in addition to any other VLANs created. In addition to selecting the VLAN, specify the Inside or Outside NAT type.

To view and configure a NAT interface:

- 1 Select *Security* > *NAT* from the main menu tree.
- 2 Click the *Interfaces* tab.

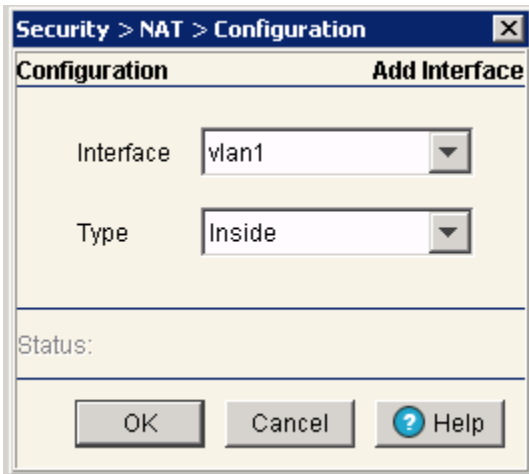


3 Refer to the following information as displayed within the *Interface* tab:

Interface	Displays the VLAN used as the inside or outside NAT type. All defined VLANs are available from the drop-down menu for use as the interface.
Type	<p>Displays the NAT type as either:</p> <ul style="list-style-type: none"> • <i>Inside</i>—The set of controller-managed networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world. • <i>Outside</i>—All other addresses. Usually these are valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.

- 4 To Edit an existing interface, select it from the list of available interfaces and click the *Edit* button. An Edit Interface screen displays allowing the user to modify the VLAN and interface type (inside or outside).
- 5 If an interface is obsolete or of no use to the NAT translation process, select it and click the *Delete* button to remove it from the list of interfaces available.
- 6 If modifying an existing interface is not a valid option, consider configuring a new interface. To define a new NAT interface:

- a Click the *Add* button from within the Interfaces tab.



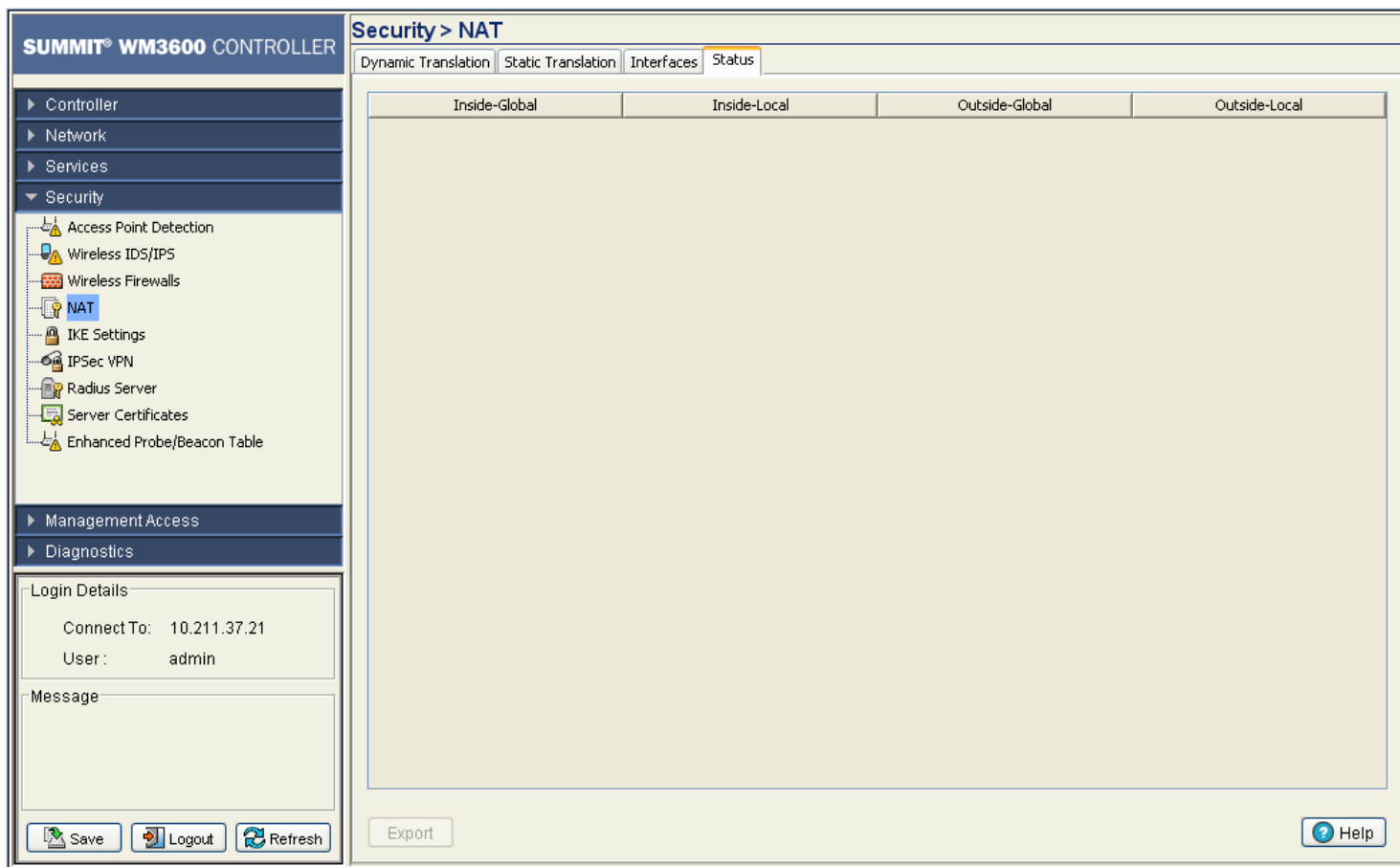
- b Use the *Interface* drop-down menu to select the VLAN used as the communication medium between the controller managed network and its destination (within the insecure outside world).
- c Use the *Type* drop-down menu to specific the Inside or Outside designation as follows:
- *Inside*—The set of controller-managed networks subject to translation. These are the internal addresses you are trying to prevent from being exposed to the outside world.
 - *Outside*—All other addresses. Usually these are valid addresses located on the Internet. Outside addresses pose no risk if exposed over a publicly accessible network.
- d Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- e Click *OK* to use the changes to the running configuration and close the dialog.
- f Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing NAT Status

Use the *Status* tab to review the NAT translations configured thus far for the controller. The Status tab displays the inside and outside local and global IP addresses.

To view and configure a NAT interface:

- 1 Select *Security* > *NAT* from the main menu tree.
- 2 Click the *Status* tab.



- 3 Refer to the following to assess the validity and total NAT translation configurations available to the controller.

Inside-Global	Displays the internal global pool of addresses (allocated out of the controller’s private address space but relevant to the outside) you are trying to prevent from being exposed to the outside world.
Inside Local	Displays the internal local pool of addresses (addresses internal to the controller) you are trying to prevent from being exposed to the outside world.
Outside-Global	The IP address of an outside host as it appears to the inside network.
Outside-Local	The configured IP address assigned to a host in the outside network.

- 4 Click the *Export* button to export the contents of the table to a *Comma Separated Values* file (CSV).

Configuring IKE Settings

IKE (also known as ISAKMP) is the negotiation protocol enabling two hosts to agree on how to build an IPSec security association. To configure the security appliance for virtual private networks, set global IKE parameters that apply system wide and define IKE policies peers negotiate to establish a VPN tunnel.

IKE protocol is an IPSec standard protocol used to ensure security for VPN negotiation, and remote host or network access. IKE provides an automatic means of negotiation and authentication for communication between two or more parties. IKE manages IPSec keys automatically.

The IKE configuration is defined by the following:

- [Defining the IKE Configuration on page 457](#)
- [Setting IKE Policies on page 459](#)
- [Viewing SA Statistics on page 463](#)



NOTE

By default, the IKE feature is enabled. Extreme Networks does not support disabling the IKE server.



NOTE

The default isakmp policy will not be picked up for IKE negotiation if another crypto isakmp policy is created. For the default isakmp policy to be picked up for AAP adoption you must first create the default isakmp policy as a new policy with default parameters. This needs to be done if multiple crypto isakmp policies are needed in the controller configuration.

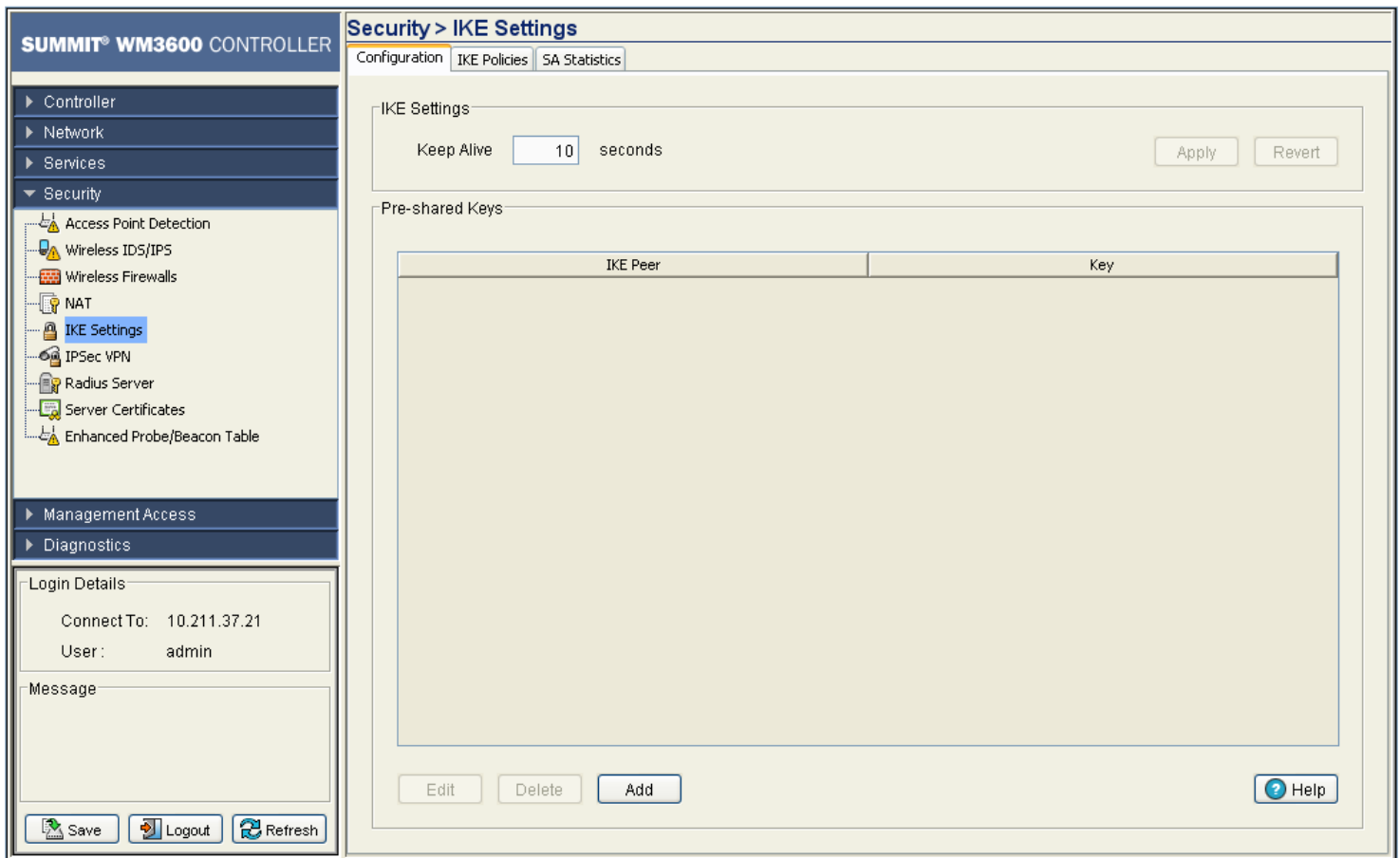
Defining the IKE Configuration

Refer to the *Configuration* tab to enable (or disable) IKE and define the IKE identity (for exchanging identities).

Use IKE to specify IPSec tunnel attributes for an IPSec peer and initiate an IKE negotiation with the tunnel attributes. This feature is best implemented in a crypto hub scenario. This scenario is scalable since the keys are kept at a central repository (the RADIUS server) and more than one controller and application can use the information.

To view the current set of IKE configurations:

- 1 Select *Security > IKE Settings* from the main menu tree.
- 2 Click the *Configurations* tab.



During IKE negotiations, peers must identify themselves to one another. Thus, the configuration you define is the identification medium for device recognition.

- 3 Set a *Keep Alive* interval (in seconds) the controller uses for monitoring the continued presence of a peer and report of the client's continued presence. The client notifies you when the peer is no longer present. The default interval is 10 seconds.
- 4 Click the *Apply* button (within the IKE Settings field) to save the configuration.
- 5 Click the *Revert* (within the IKE Settings field) to rollback to the previous configuration.
- 6 Refer to the *Pre-shared Keys* field to review the following information:

Peer IP Address	Use the Peer IP Address to associate an IP address with the specific tunnel used by a group of peers.
Key	Displays the string ID a remote peer uses to look up pre-shared keys.



NOTE

RSA keys are not supported for IKE negotiation on this controller.

- 7 Highlight an existing set of pre-shared Keys and click the *Edit* button to revise the existing peer IP address and key.
- 8 Select an existing entry and click the *Delete* button to remove it.
- 9 If the properties of an existing peer IP address and key are no longer relevant and cannot be edited, click the *Add* button to create a new pre-shared key.

- a Select the *Peer IP Address* checkbox to associate an IP address with the specific tunnel used by a group of peers or, select the *Distinguished Name* checkbox to configure the controller to restrict access to those peers with the same distinguished name, or select the *Hostname* checkbox to allow shared-key messages between corresponding hostnames.
- b Define the *Key* (string ID) a remote peer uses to look up the pre-shared to interact securely with peers within the tunnel.
- c Refer to the *Status* field for the current state of requests made from the applet. This field displays error messages if something is wrong in the transaction between the applet and the controller.
- d Click *OK* to use the changes to the running configuration and close the dialog.
- e Click *Cancel* to close the dialog without committing updates to the running configuration.

Setting IKE Policies

Each IKE negotiation is divided into two phases. Phase 1 creates the first tunnel (protecting later IKE negotiation messages) and phase 2 creates the tunnel protecting the data. To define the terms of the IKE negotiation, create one or more IKE policies. Include the following:

- An authentication scheme to ensure the credentials of the peers
- An encryption scheme to protect the data
- A HMAC method to ensure the identity of the sender, and validate a message has not been altered
- A Diffie-Hellman group establishing the strength of the of the encryption-key algorithm.
- A time limit for how long the encryption key is used before it is replaced.

If IKE policies are not defined, the controller uses the default policy (with a default priority of 10001) and contains the default values. When IKE negotiations begin, the peer initiating the negotiation sends its policies to the remote peer. The remote peer searches for a match with its own policies using the defined priority scheme.

An IKE policy matches when they have the same encryption, hash, authentication and Diffie-Hellman settings. The SA lifetime must also be less than or equal to the lifetime in the policy sent. If the lifetimes do not match, the shorter lifetime applies. If no match exists, IKE refuses negotiation.

To view the current set of IKE policies:

- 1 Select *Security > IKE Settings* from the main menu tree.
- 2 Click the *IKE Policies* tab.

Security > IKE Settings

Configuration | **IKE Policies** | SA Statistics

[Show Filtering Options](#)

Sequence Number	Encryption	Hash Value	Authentication Type	SA Lifetime (sec.)	DH Group
10001	3DES	SHA1	Pre-shared Key	86400	Group 2

Filtering is disabled

Buttons: Edit, Delete, Add, Save, Logout, Refresh, Help

- 3 Refer to the values displayed within the IKE Policies tab to determine if an existing policy requires revision, removal or a new policy requires creation.

Sequence Number Displays the sequence number for the IKE policy. The available range is from 1 to 10,000, with 1 being the highest priority value.

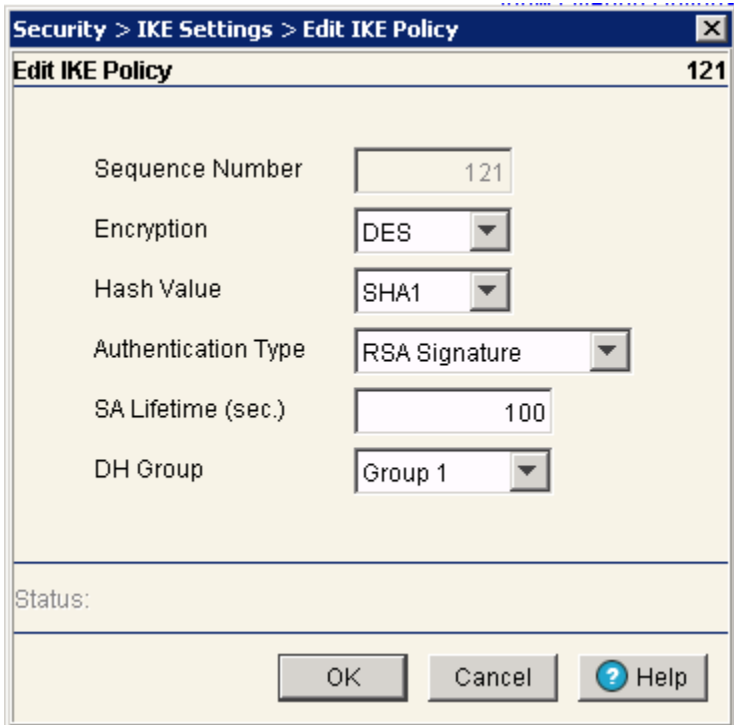
Encryption	<p>Displays the encryption method protecting data transmitted between peers. Options include:</p> <ul style="list-style-type: none"> • <i>DES 56-bit DES-CBC</i>—The default value. • <i>3DES</i>—168-bit Triple DES. • <i>AES</i>—128-bit AES. • <i>AES 192</i>—192-bit AES. • <i>AES 256</i>—256-bit AES.
Hash Value	<p>Displays the hash algorithm used to ensure data integrity. The hash value validates a packet comes from its intended destination, and has not been modified in transit. Options include:</p> <ul style="list-style-type: none"> • <i>SHA</i>—The default value. • <i>MD5</i>—MD5 has a smaller digest and is somewhat faster than SHA-1.
Authentication Type	<p>Displays the authentication scheme used to validate the identity of each peer. Pre-shared keys do not scale accurately with a growing network but are easier to maintain in a small network. Options include:</p> <ul style="list-style-type: none"> • <i>Pre-shared Key</i>—Uses pre-shared keys. • <i>RSA Signature</i>—Uses a digital certificate with keys generated by the RSA signatures algorithm.
SA Lifetime	<p>Displays an integer for the SA lifetime. With longer lifetimes, security defines future IPSec security associations quickly. Encryption strength is great enough to ensure security without using fast rekey times. Extreme Networks recommends using the default value.</p>
DH Group	<p>Displays the <i>Diffie-Hellman</i> (DH) group identifier. IPSec peers use the defined value to derive a shared secret without transmitting it to one another.</p>



NOTE

192-bit AES and 256-bit AES are not supported for manual IPSec sa configurations.

- 4 Highlight an existing policy and click the *Edit* button to revise the policy's existing sequence number, encryption scheme, hash value, authentication scheme, SA lifetime and DH group.



- 5 Select an existing policy and click the *Delete* button to remove it from the table.
- 6 If the properties of an existing policy are no longer relevant and cannot be edited to be useful, click the *Add* button to define a new policy.



a Configure a set of attributes for the new IKE policy:

Sequence Number	Define the sequence number for the IKE policy. The available range is from 1 to 10,000 with 1 being the highest priority value.
Encryption	Set the encryption method used to protect the data transmitted between peers. Options include: <ul style="list-style-type: none">• <i>DES 56-bit DES-CBC</i>—The default value.• <i>3DES</i>—168-bit Triple DES.• <i>AES</i>—128-bit AES.• <i>AES 192</i>—192-bit AES.• <i>AES 256</i>—256-bit AES.
Hash Value	Define the hash algorithm used to ensure data integrity. The hash value validates a packet comes from its intended source and has not been modified in transit. Options include: <ul style="list-style-type: none">• <i>SHA</i>—The default value.• <i>MD5</i>—MD5 has a smaller digest and is somewhat faster than SHA-1.
Authentication Type	Set the authentication scheme used to validate the identity of each peer. Pre-shared keys do not scale accurately with a growing network but are easier to maintain in a small network. Options include: <ul style="list-style-type: none">• <i>Pre-shared Key</i>—Uses pre-shared keys.• <i>RSA Signature</i>—Uses a digital certificate with keys generated by the RSA signatures algorithm.
SA Lifetime	Define an integer for the SA lifetime. With longer lifetimes, security defines future IPSec security associations quickly. Encryption strength is great enough to ensure security without using fast rekey times. Extreme Networks recommends using the default value.
DH Group	Set the Diffie-Hellman group identifier. IPSec peers use the defined value to derive a shared secret without transmitting it to one another.

- b** Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- c** Click *OK* to use the changes to the running configuration and close the dialog.
- d** Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing SA Statistics

A *security association* (SA) is a description of how two peers employ a security to interoperate securely. IKE requires SAs to identify connection attributes. IKE can negotiate and establish its own SA. An IKE SA is used by IKE only, and is bi-directional.

To view SA statistics:

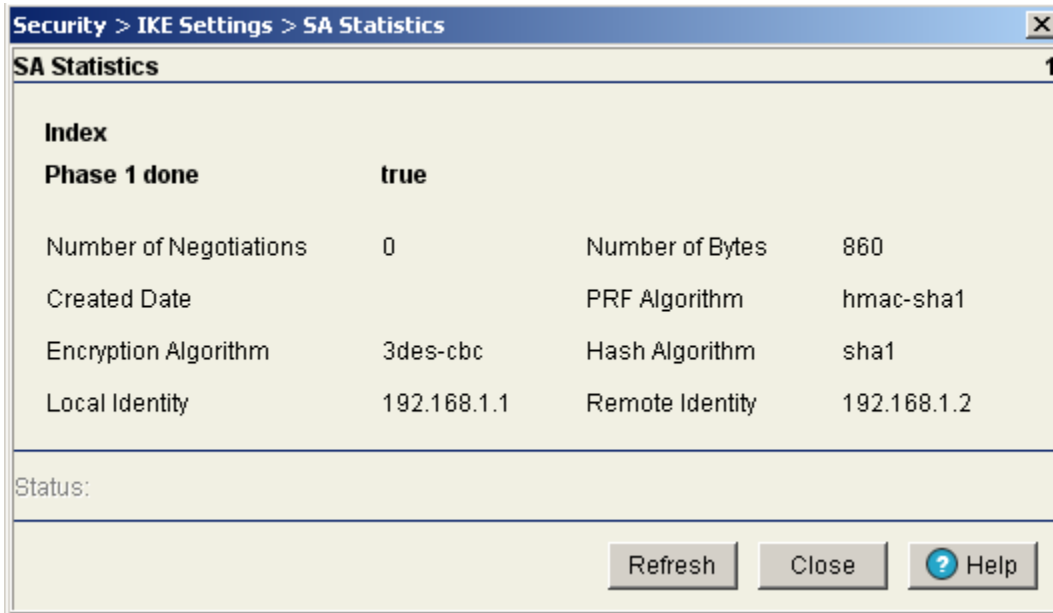
- 1 Select *Security > IKE Settings* from the main menu tree.
- 2 Click the *SA Statistics* tab.



3 Refer to the information displayed within SA Statistics tab to discern the following:

Index	Displays the alpha-numeric name (index) used to identify individual SAs.
Phase 1 done	Displays whether this index is completed with the phase 1 (authentication) credential exchanged between peers.
Created Date	Displays the exact date the SA was configured for each index displayed.
Local Identity	Specifies the address the local IKE peer uses to identify itself to the remote peer.
Remote Identity	Specifies the address the remote IKE peer uses to identify itself to a local peer.
Number of Negotiations	During IKE negotiations the peers must identify themselves to each other. This value is helpful in determining the network address information used to validate peers.
Number of Bytes	Displays the number of bytes passed between the peers for the specified index.

- 4 Select an index and click the *Details* button to display a more robust set of statistics for the selected index.



Use this information to discern whether changes to an existing IKE configuration is warranted or if a new configuration is required.

- 5 Click the *Stop Connection* button to terminate the statistic collection of the selected IKE peer.

Configuring IPsec VPN

Use IPsec *Virtual Private Network* (VPN) to define secure tunnels between two peers. Configure which packets are sensitive and should be sent through secure tunnels, and what should be used to protect these sensitive packets. Once configured, an IPsec peer creates a secure tunnel and sends the packet through the tunnel to the remote peer.

IPsec tunnels are sets of security associations (SA) established between two peers. The security associations define which protocols and algorithms are applied to sensitive packets, and what keying material is used by the two peers. Security associations are unidirectional and established per security protocol.

To configure IPsec security associations, Extreme Networks uses the Crypto Map entries. Crypto Map entries created for IPsec pull together the various parts used to set up IPsec security associations. Crypto Map entries include transform sets. A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPsec protected traffic.

The Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with the IPsec standard. IKE automatically negotiates IPsec security associations and enables IPsec secure communications without costly manual configuration. To support IPsec VPN functionality, the following configuration activities are required:

- Configure a DHCP Server to assign public IP address

An IPSec client needs an IP address before it can connect to the VPN Server and create an IPSec tunnel. A DHCP Server needs to be configured on the interface to distribute public IP addresses to the IPSec clients.

- Configure a Crypto policy (IKE)

IKE automatically negotiates IPSec security associations and enables IPSec secure communications without costly manual pre-configuration. IKE eliminates the need to manually specify all the IPSec security parameters in the Crypto Maps at both peers, allows you to specify a lifetime for the IPSec security association, allows encryption keys to change during IPSec sessions and permits *Certification Authority (CA)* support for a manageable, scalable IPSec implementation. If you do not want IKE with your IPSec implementation, disable it for IPSec peers. You cannot have a mix of IKE-enabled and IKE-disabled peers within your IPSec network.

- Configure security associations parameters

The use of manual security associations is a result of a prior arrangement between controller users and the IPSec peer. If IKE is not used for establishing security associations, there is no negotiation of security associations. The configuration information in both systems must be the same for traffic to be processed successfully by IPSec.

- Define transform sets

A transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a particular transform set for protecting data flow.

With manually established security associations, there is no negotiation with the peer. Both sides must specify the same transform set. If you change a transform set definition, the change is only applied to Crypto Map entries that reference the transform set. The change is not applied to existing security associations, but is used in subsequent negotiations to establish new security associations.

- Create Crypto Map entries

When IKE is used to establish security associations, the IPSec peers can negotiate the settings they use for the new security associations. Therefore, specify lists (such as lists of acceptable transforms) within the Crypto Map entry.

- Apply Crypto Map sets to Interfaces

Assign a Crypto Map set to each interface through which IPSec traffic flows. The security appliance supports IPSec on all interfaces. Assigning the Crypto Map set to an interface instructs the security appliance to evaluate all the traffic against the Crypto Map set and use the specified policy during connection or SA negotiation. Assigning a Crypto Map to an interface also initializes run-time data structures (such as the SA database and the security policy database). Reassigning a modified Crypto Map to the interface resynchronizes the run-time data structures with the Crypto Map configuration. With the controller, a Crypto Map cannot get applied to more than one interface at a time.

- Monitor and maintain IPSec tunnels

New configuration changes only take effect when negotiating subsequent security associations. If you want the new settings to take immediate effect, clear the existing security associations so they will be re-established with the changed configuration.

For manually established security associations, clear and reinitialize the security associations or the changes will not take effect.

For more information on configuring IPsec VPN, refer to the following:

- [Defining the IPsec Configuration on page 467](#)
- [Defining the IPsec VPN Remote Configuration on page 471](#)
- [Configuring IPSEC VPN Authentication on page 473](#)
- [Configuring Crypto Maps on page 476](#)
- [Viewing IPsec Security Associations on page 488](#)

Defining the IPsec Configuration

Use the IPsec VPN *Configuration* tab to view the attributes of existing VPN tunnels and modify the security association lifetime and keep alive intervals used to maintain the sessions between VPN peers. From the Configuration tab, transform sets can be created as existing sets, modified or deleted.

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Click the *Configuration* tab.

The screenshot displays the Summit WM3600 Controller web interface. The main content area is titled "Security > IPsec VPN" and features several tabs: Configuration, Remote, Authentication, Crypto Maps, and IPsec SAs. The "Configuration" tab is selected, showing two input fields: "SA Lifetime (secs)" with a value of 3600 and "SA Lifetime (Kb)" with a value of 4608000. To the right of these fields are "Apply" and "Revert" buttons. Below the configuration fields is a section for "Transform Sets" containing a table with the following columns: Name, AH Authentication Scheme, ESP Encryption Scheme, ESP Authentication Scheme, and Mode. The table is currently empty. At the bottom of the table are "Edit", "Delete", and "Add" buttons. A "Help" button is located at the bottom right of the main content area. The left sidebar shows a navigation tree with "Security > IPsec VPN" highlighted. At the bottom of the interface, there are "Save", "Logout", and "Refresh" buttons.

- 3 Refer to the *Configuration* field to define the following:

SA Lifetime (secs) For IKE based security associations, define a SA Lifetime (in seconds) forcing the periodic expiration and re-negotiation of peer credentials. Thus, continually validating the peer relationship. The default value is 3600 seconds.

SA Lifetime (Kb)	Causes the security association to time out after the specified amount of traffic (in kilobytes) have passed through the IPSec tunnel using the security association. The default value is 4608000 Kb.
Apply	Click <i>Apply</i> to save any updates you may have made to the screen.
Revert	Click <i>Revert</i> to disregard any changes you have made and revert back to the last saved configuration.

4 Refer to the *Transform Sets* field to view the following data:

Name	Displays a transform set identifier used to differentiate transform sets. The index is helpful when transform sets with similar attributes need to be revised or discarded.
AH Authentication Scheme	Displays the AH Transform Authentication scheme used with the index. Options include: <ul style="list-style-type: none"> • <i>None</i>—No AH authentication is used. • <i>AH-MD5-HMAC</i>—AH with the MD5 (HMAC variant) authentication algorithm. • <i>AH-SHA-HMAC</i>—AH with the SHA (HMAC variant) authentication algorithm.
ESP Encryption Scheme	Displays the ESP Encryption Transform used with the index. Options include: <ul style="list-style-type: none"> • <i>None</i>—No ESP encryption is used with the transform set. • <i>ESP-DES</i>—ESP with the 56-bit DES encryption algorithm. • <i>ESP-3DES</i>—ESP with 3DES, ESP with AES. • <i>ESP-AES</i>—ESP with 3DES, ESP with AES (128 bit key). • <i>ESP-AES 192</i>—ESP with 3DES, ESP with AES (192 bit key). • <i>ESP-AES 256</i>—ESP with 3DES, ESP with AES (256 bit key)
ESP Authentication Scheme	Displays the ESP Authentication Transform used with the index. Options include: <ul style="list-style-type: none"> • <i>None</i>—No ESP authentication is used with the transform set. • <i>MD5-HMAC</i>—AH with the MD5 (HMAC variant) authentication algorithm. • <i>SHA-HMAC</i>—AH with the SHA (HMAC variant) authentication algorithm.
Mode	Displays the current mode used with the transform set. The mode is either tunnel or transport.

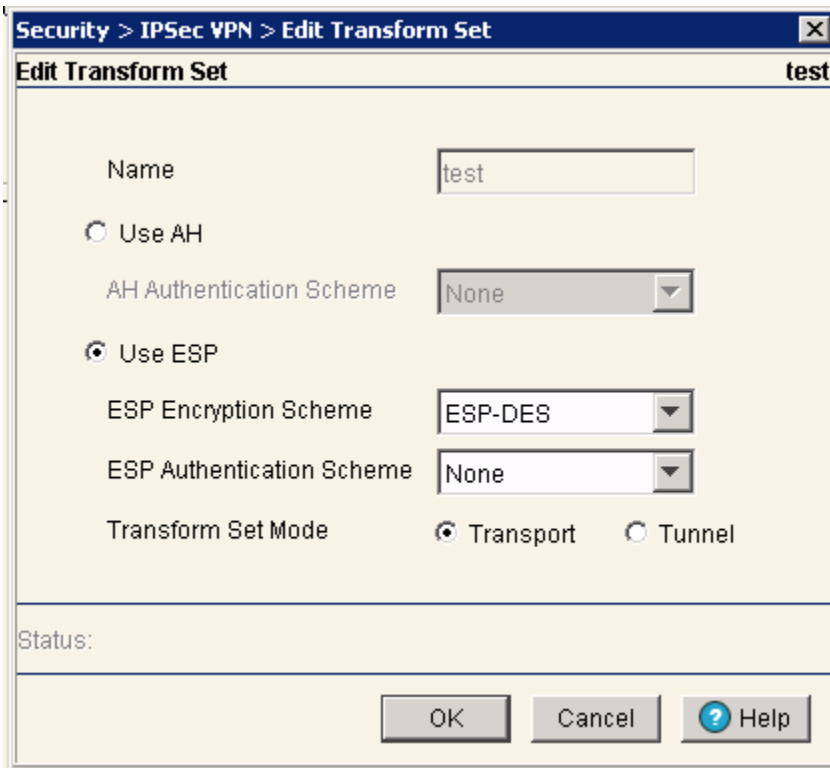
- 5 Select an IPSec VPN transform set (by its index) and click the *Edit* button to modify its properties. For more information, see [“Editing an Existing Transform Set” on page 468](#).
- 6 Select an index and click the *Delete* button to remove it from the table.
- 7 If none of the transform sets displayed appear useful, click the *Add* button to create a new one. For more information, see [“Adding a New Transform Set” on page 470](#).

Editing an Existing Transform Set

If the attributes of an existing transform set no longer lend themselves useful, consider editing the transform set to be relevant with the needs of existing VPN peers.

To edit the attributes of an existing transform set:

- 1 Select *Security > IPSec VPN* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Select an existing transform set and click the *Edit* button.



- 4 Revise the following information as required to render the existing transform set useful.

Name	The name is read-only and cannot be modified unless a new transform set is created.
AH Authentication Scheme	Select the <i>Use AH</i> checkbox (if necessary) to modify the AH Transform Authentication scheme. Options include: <ul style="list-style-type: none">• <i>None</i>—No AH authentication is used.• <i>AH-MD5-HMAC</i>—AH with the MD5 (HMAC variant) authentication algorithm.• <i>AH-SHA-HMAC</i>—AH with the SHA (HMAC variant) authentication algorithm.
ESP Encryption Scheme	Select the <i>Use ESP</i> checkbox (if necessary) to modify the ESP Encryption Scheme. Options include: <ul style="list-style-type: none">• <i>None</i>—No ESP encryption is used with the transform set.• <i>ESP-DES</i>—ESP with the 56-bit DES encryption algorithm.• <i>ESP-3DES</i>—ESP with 3DES, ESP with AES.• <i>ESP-AES</i>—ESP with 3DES, ESP with AES (128 bit key).• <i>ESP-AES 192</i>—ESP with 3DES, ESP with AES (192 bit key).• <i>ESP-AES 256</i>—ESP with 3DES, ESP with AES (256 bit key).

ESP Authentication Scheme	Select the <i>Use ESP</i> checkbox (if necessary) to modify the ESP Authentication Scheme. Options include: <ul style="list-style-type: none"> • <i>None</i>—No ESP authentication is used with the transform set. • <i>MD5-HMAC</i>—AH with the MD5 (HMAC variant) authentication algorithm. • <i>SHA-HMAC</i>—AH with the SHA (HMAC variant) authentication algorithm.
Mode	Modify (if necessary) the current mode used with the transform set. The mode is either Tunnel or Transport.

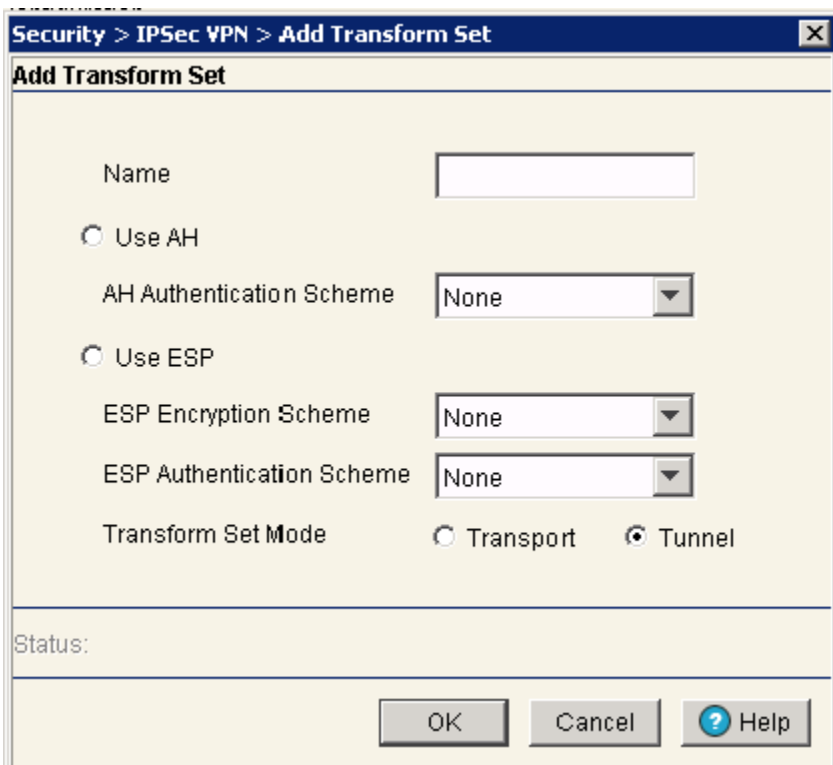
- 5 Refer to the *Status* field for the state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to use the changes to the running configuration and close the dialog.
- 7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding a New Transform Set

A transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a particular transform set for protecting data flow. If the attributes of an existing transform set no longer lend themselves useful, and an existing transform set is not required, create a new transform set to meet the needs of your network.

To edit the attributes of an existing transform set:

- 1 Select *Security > IPSec VPN* from the main menu tree.
- 2 Click the *Configuration* tab.
- 3 Click the *Add* button.



4 Define the following information as required for the new transform set.

Name	Create a name describing this new transform set.
AH Authentication Scheme	Select the <i>Use AH</i> checkbox to define the AH Transform Authentication scheme. Options include: <ul style="list-style-type: none">• <i>None</i>—No AH authentication is used.• <i>AH-MD5-HMAC</i>—AH with the MD5 (HMAC variant) authentication algorithm.• <i>AH-SHA-HMAC</i>—AH with the SHA (HMAC variant) authentication algorithm.
ESP Encryption Scheme	Select the <i>Use ESP</i> checkbox to define the ESP Encryption Scheme. Options include: <ul style="list-style-type: none">• <i>None</i>—No ESP encryption is used with the transform set.• <i>ESP-DES</i>—ESP with the 56-bit DES encryption algorithm.• <i>ESP-3DES</i>—ESP with 3DES, ESP with AES.• <i>ESP-AES</i>—ESP with 3DES, ESP with AES (128 bit key).• <i>ESP-AES 192</i>—ESP with 3DES, ESP with AES (192 bit key).• <i>ESP-AES 256</i>—ESP with 3DES, ESP with AES (256 bit key).
ESP Authentication Scheme	Select the <i>Use ESP</i> checkbox to define the ESP Authentication Scheme. Options include: <ul style="list-style-type: none">• <i>None</i>—No ESP authentication is used with the transform set.• <i>MD5-HMAC</i>—AH with the MD5 (HMAC variant) authentication algorithm.• <i>SHA-HMAC</i>—AH with the SHA (HMAC variant) authentication algorithm.
Mode	Define the current mode used with the transform set. The mode is either Tunnel or Transport.

5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

6 Click *OK* to use the changes to the running configuration and close the dialog.

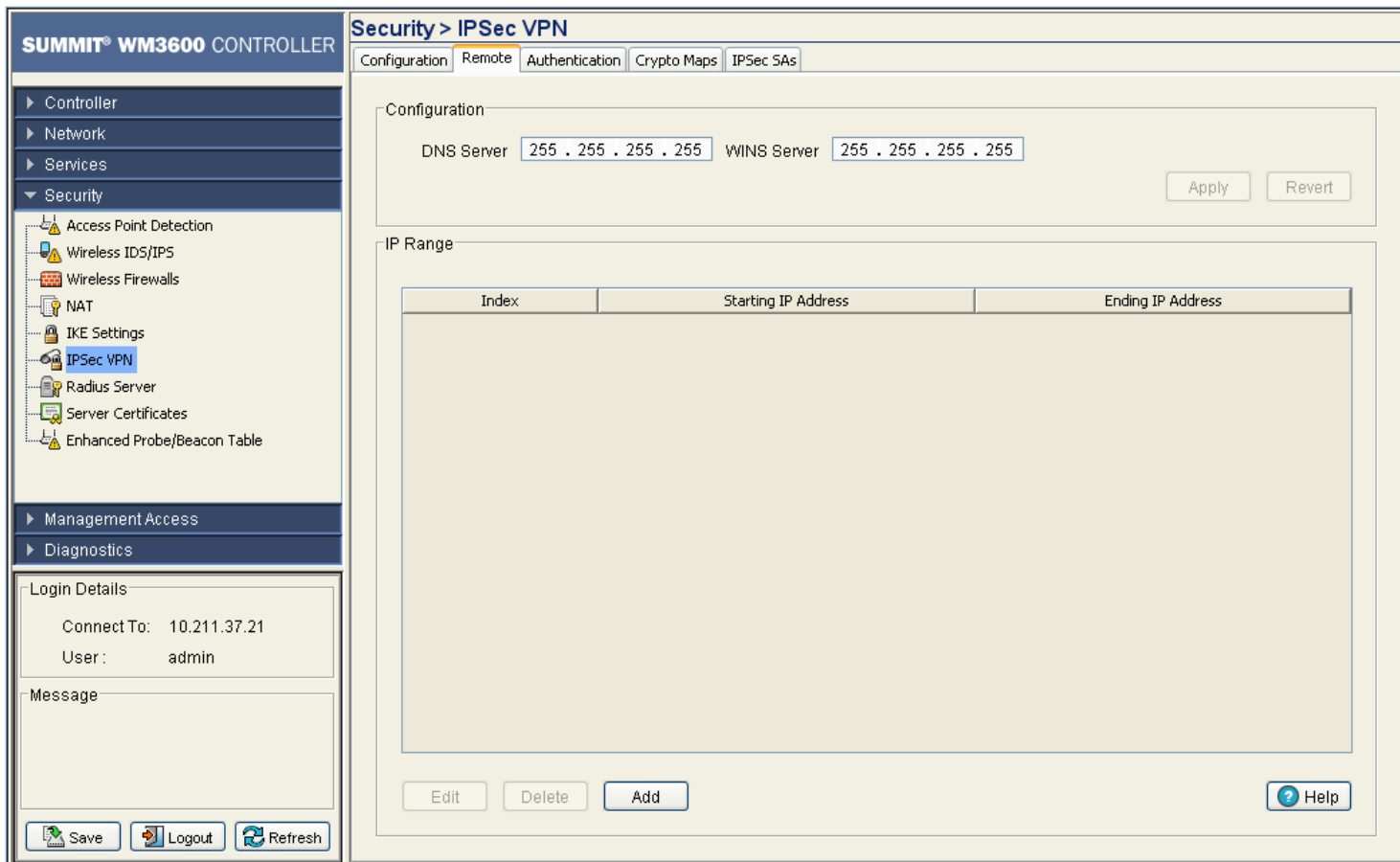
7 Click *Cancel* to close the dialog without committing updates to the running configuration.

Defining the IPsec VPN Remote Configuration

Use the *IPsec VPN Remote* tab to configure the DNS and/or WINS Servers used to route packets to the remote end of the IPsec VPN tunnel. The Remote tab is also used for defining the IP address range used within the IPsec VPN tunnel and configuring the authentication scheme for user permissions within the IPsec VPN tunnel.

To define the IPSEC VPN's remote configuration:

- 1 Select *Security* > *IPSec VPN* from the main menu tree.
- 2 Click the *Remote* tab.



3 Refer to the *Configuration* field to define the following:

- | | |
|-------------|---|
| DNS Server | Enter the numerical IP address of the DNS Server used to route information to the remote destination of the IPSEC VPN. |
| WINS Server | Enter the numerical IP address of the WINS Server used to route information to the remote destination of the IPSEC VPN. |
| Apply | Click <i>Apply</i> to save any updates made to the screen. |
| Revert | Click <i>Revert</i> to disregard changes and revert back to the last saved configuration. |

4 Click the *IP Range* tab to view the following:

- | | |
|---------------------|--|
| Index | Enter the index assigned to the range of IP addresses displayed in the Starting and Ending IP Address ranges. This index is used to differentiate the index from others with similar IP addresses. |
| Starting IP Address | Enter the numerical IP address used as the starting address for the range defined. If the Ending IP address is left blank, only the starting address is used for the remote destination. |

Ending IP Address Enter a numerical IP address to complete the range. If the Ending IP address is blank, only the starting address is used as the destination address.

- 5 Click the *Edit* button (within the IP Range tab) to modify the range of existing IP addresses displayed.
- 6 Select an IP address range index and click the *Delete* button to remove this range from those available within the IP Range tab.
- 7 To add a new range of IP addresses, click the *Add* button (within the IP Range tab) and define the range in the fields provided. Click *OK* when completed to save the changes.

The screenshot shows a dialog box titled "Security > IPsec VPN > Add IP Range". Inside the dialog, there are two input fields: "Starting IP Address" and "Ending IP Address", each with a dotted placeholder for an IP address. Below these fields is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

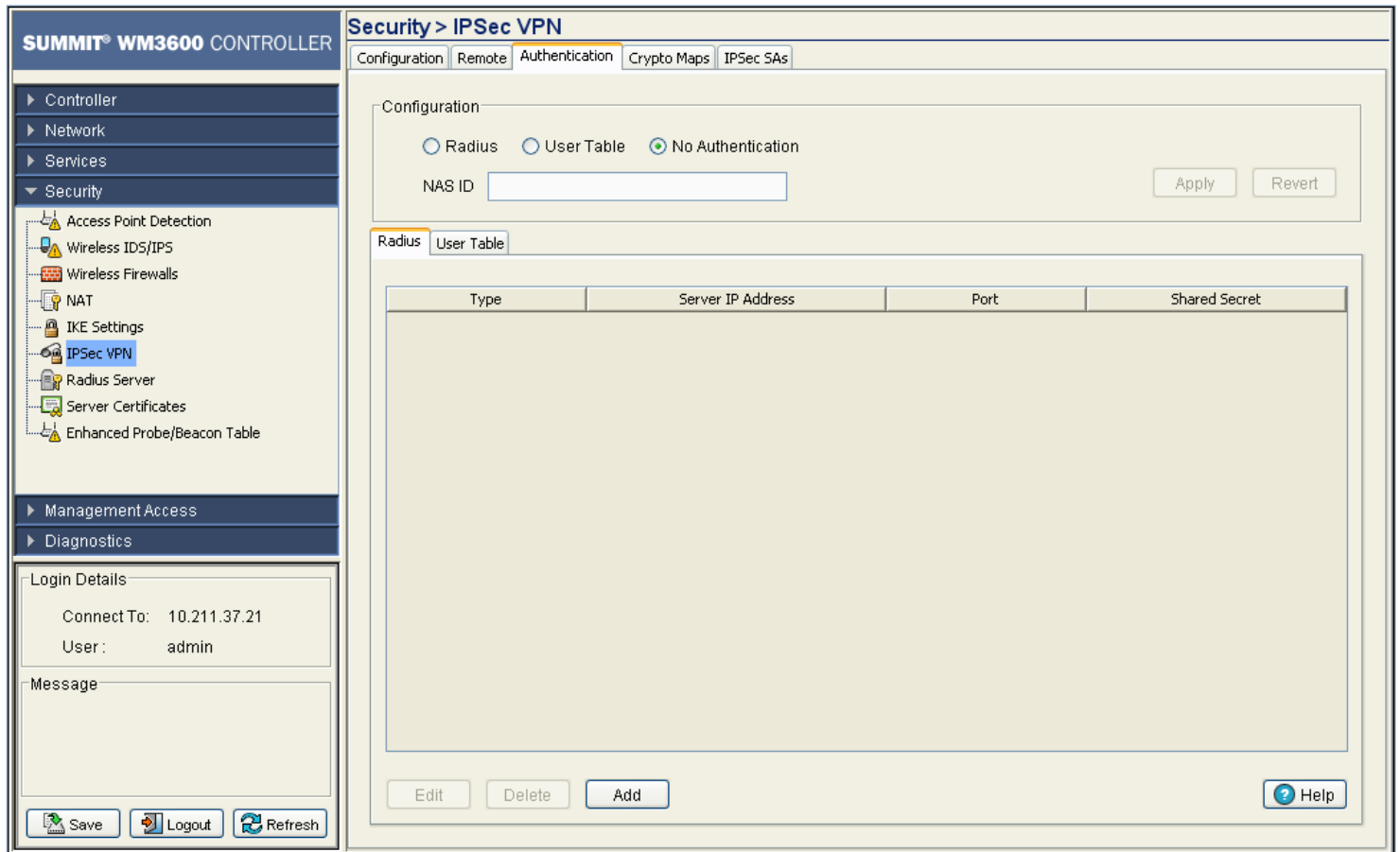
- 8 Click *Cancel* to disregard the changes and revert to the last saved configuration.

Configuring IPSEC VPN Authentication

If IKE is not used for establishing security associations, there is no negotiation of security associations. Consequently, the configuration information in both systems must be the same for traffic to be processed successfully by the IPsec resource. Select the *Authentication* tab to define the credential verification mechanisms used with the IPSEC VPN configuration.

To define the IPsec VPN authentication configuration:

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Select the *Authentication* tab.



- 3 Define whether IPsec VPN user authentication is conducted using a RADIUS Server (by selecting the *RADIUS* radio button), by a user-defined set of names and password (by selecting the *User Table* radio button) or if no authentication is used for credential verification (by selecting the *No Authentication* radio button).

- 4 Enter a *NAS ID* for the NAS port.

The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port. When the controller authorizes users, it queries the user profile database using a username representative of the physical NAS port making the connection.

- 5 If the *RADIUS Server* radio button is selected, the following server information displays within the RADIUS tab:

Type	Displays whether this target server is a Primary or Secondary RADIUS Server.
Server IP Address	Displays the IP address of the server acting as the data source for the RADIUS server.
Port	Displays the TCP/IP port number for the server acting as a data source for the RADIUS. The default port is 1812.

Shared Secret Displays a shared secret used for each host or subnet authenticating against the RADIUS server. The shared secret can be up to 7 characters in length.

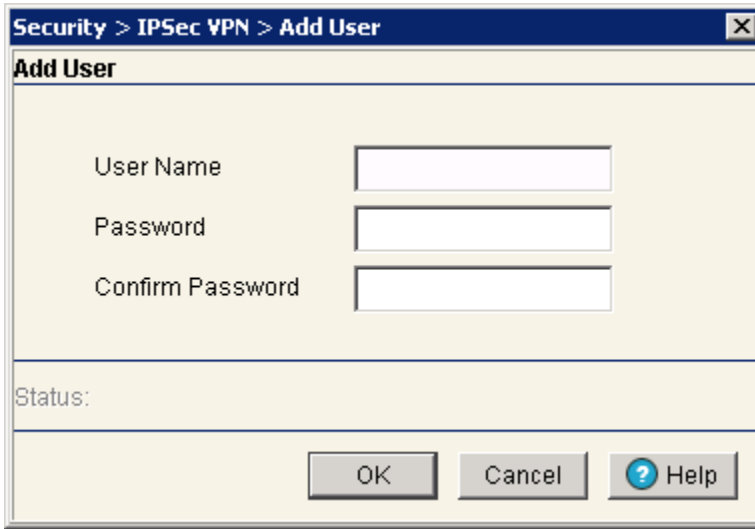
- 6 Select an existing RADIUS Server and click the *Edit* button to modify its designation as a primary or secondary RADIUS Server, IP address, port, NAS ID and shared secret password.
Extreme Networks recommends only modifying an existing RADIUS Server when its current configuration is no longer viable for providing user authentication. Otherwise, define a new RADIUS Server.
- 7 Select an existing server and click the *Delete* button to remove it from list of available RADIUS Servers. Only delete a server if its configuration does not provide a valid authentication medium.
- 8 If you require a new RADIUS Server be configured, click the *Add* button.

The screenshot shows a dialog box titled "Security > IPsec VPN > Add Radius". The main area is titled "Add Radius" and contains two radio buttons: "Primary" (which is selected) and "Secondary". Below the radio buttons are three text input fields: "Server IP Address" (with a dotted pattern), "Port", and "Shared Secret". At the bottom of the dialog, there is a "Status:" label and three buttons: "OK", "Cancel", and "Help".

Set this server's designation as a primary or secondary RADIUS Server (using the checkboxes), define the server IP address, port and shared secret password. Click *OK* when completed to save the changes.

- 9 If the *User Table* checkbox was selected from within the Configuration field, select the User Table tab to review the User Name and Passwords defined for use.

- 10 Click the *Add* button to display a screen used to add a new User and Password. Enter a User Name and Password and confirm. Click *OK* to save the changes.



The screenshot shows a dialog box titled "Security > IPSec VPN > Add User". The dialog has a title bar with a close button (X). The main area is titled "Add User" and contains three input fields: "User Name", "Password", and "Confirm Password". Below the input fields is a "Status:" label. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

- 11 To change an existing user's password, select the user from within the User Table and click the *Change Password* button. Change and confirm the updated password.
- 12 If necessary, select an existing user and click the *Delete* button to remove that user from the list available within the User Table.

Configuring Crypto Maps

Crypto Maps allow you to set restrictions preventing peers with specific certificates (especially certificates with particular DNs) from accessing selected encrypted interfaces. If restricting access, specify a fewer number of Crypto Maps (referring to large identity sections) instead of specifying a large number of Crypto Maps (referring to small identity sections).

To define the Crypto Map configuration:

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Click the *Crypto Maps* tab.

The screenshot displays the Summit WM3600 Controller web interface. The main menu on the left shows the navigation path: Security > IPsec VPN. The 'Crypto Maps' tab is selected, showing a table for 'Crypto Map Entries'. The table has columns for Priority / Seq #, Name, Mode Config, Number of Peers, SA Lifetime (secs), SA Lifetime (kb), ACL ID, and Number of Interfaces. The table is currently empty, and a message at the bottom states 'Filtering is disabled'. Below the table are buttons for 'Edit', 'Delete', and 'Add'. A 'Help' button is also present in the bottom right corner. The interface includes a 'Login Details' section with 'Connect To: 10.211.37.21' and 'User: admin', and a 'Message' field. At the bottom left, there are 'Save', 'Logout', and 'Refresh' buttons.

Priority / Seq #	Name	Mode Config	Number of Peers	SA Lifetime (secs)	SA Lifetime (kb)	ACL ID	Number of Interfaces
------------------	------	-------------	-----------------	--------------------	------------------	--------	----------------------

The Crypto Maps screen is divided into 5 tabs, each serving a unique function in the overall Crypto Map configuration. Refer to the following:

- [Crypto Map Entries on page 478](#)
- [Crypto Map Peers on page 481](#)
- [Crypto Map Manual SAs on page 483](#)
- [Crypto Map Transform Sets on page 485](#)
- [Crypto Map Interfaces on page 487](#)

Crypto Map Entries

To review, revise or add Crypto Map entries:

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Click the *Crypto Maps* tab and select *Crypto Map Entries*.

- 3 Review the following Crypto Map attributes to determine if an existing Crypto Map requires revision, deletion or if a new Crypto Map needs to be created.

Priority / Seq	Displays the numerical priority assigned to each Crypto Map.
Name	Displays the user-assigned name for this specific Crypto Map. This name can be modified using the <i>Edit</i> function or a new Crypto Map can be created by clicking the <i>Add</i> button.
Mode Config	Displays a green checkmark for the Crypto Map used with the current interface. A "X" is displayed next to other Crypto Maps not currently being used.
Number of Peers	Displays the number of peers used by each Crypto Map displayed.

SA Lifetime (secs)	Displays a SA Lifetime (in seconds) that forces the periodical expiration and re-negotiation of peer credentials. Thus, continually validating the peer relationship.
SA Lifetime (Kb)	Causes the security association to time out after the specified amount of traffic (in kilobytes) has passed through the IPSec tunnel (using the security association).
ACL ID	Displays the name of the ACL ID used for each Crypto Map.
Number of Interfaces	Displays the number of interfaces each specific Crypto Map is used with.

- 4 Select an existing Crypto Map and click the Edit button to modify the Crypto Map's attributes. If an entire Crypto Map requires revision, consider deleting the Crypto Map and creating a new one using the *Add* function.

Refer to the definitions supplied for the *Add Crypto Map* screen (on the next page) to ascertain the requirements for editing a Crypto Map.

- 5 Select an existing Crypto Map and click the *Delete* button to remove it from the list of available.
- 6 Click the *Add* button to define the attributes of a new Crypto Map.

Security > IPSec VPN > Add Crypto Map

Add Crypto Map

Seq #

Name

None

Domain Name

HostName

SA Lifetime (secs)

SA Lifetime (Kb)

ACL ID

PFS

Remote Type

Mode

SA Per Host

Mode Config

Peers (add choices)

Transform Sets (select one)

test

Status:

- a Assign a *Seq #* (sequence number) to distinguish one Crypto Map from the another.
 - b Assign the Crypto Map a *Name* to differentiate from others with similar configurations.
 - c Use the *None*, *Domain Name* or *Host Name* radio buttons to select and enter the *fully qualified domain name* (FQDN) or host name of the host exchanging identity information.
 - d Define a *SA Lifetime (secs)* to define an interval (in seconds) that (when expired) forces a new association negotiation.
 - e Define a *SA Lifetime (Kb)* to time out the security association after the specified traffic (in kilobytes) has passed through the IPSec tunnel using the security association.
 - f Use the *ACL ID* drop-down menu to permit a Crypto Map data flow using the permissions within the selected ACL.
 - g Use the *PFS* drop-down menu to specify a group to require *perfect forward secrecy* (PFS) in requests received from the peer.
 - h Use the *Remote Type* drop-down menu to specify a remote type (either *XAuth* or *L2TP*).
 - i Optionally select the *SA Per Host* checkbox to specify that separate IPSec SAs should be requested for each source/destination host pair.
 - j Refer to the *Peers (add choices)* field and use the Add and Delete functions as necessary to add or remove existing peers. For information on adding or modifying peers, see ["Crypto Map Peers" on page 481](#).
 - k Refer to the *Transform Sets (select one)* field to select and assign a transform set for v with Crypto Map. Again, a transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a particular transform set for protecting data flow.
- 7 Click *OK* to save the new Crypto Map and display it within the Crypto Map tab.

Crypto Map Peers

To review, revise or add Crypto Map peers:

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Click the *Crypto Maps* tab and select *Peers*.

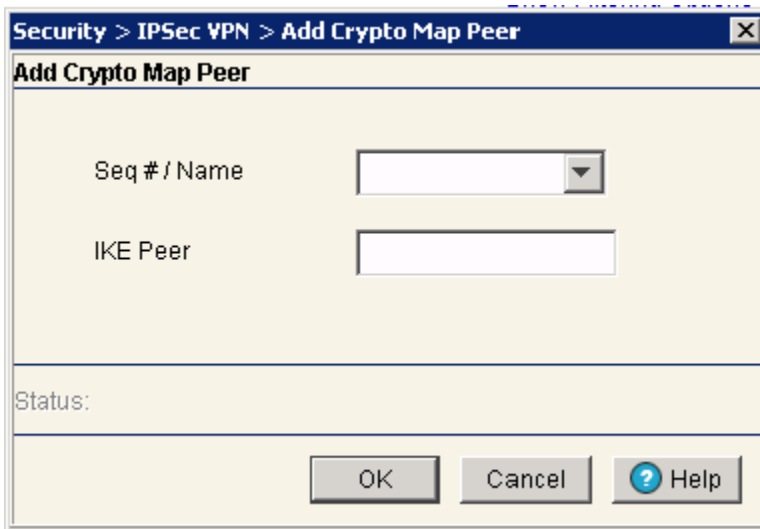
The screenshot shows the Summit WM3600 Controller web interface. The main menu on the left includes Controller, Network, Services, Security, Management Access, and Diagnostics. The Security menu is expanded, showing options like Access Point Detection, Wireless IDS/IPS, Wireless Firewalls, NAT, IKE Settings, IPsec VPN (selected), Radius Server, Server Certificates, and Enhanced Probe/Beacon Table. The main content area is titled 'Security > IPsec VPN' and has tabs for Configuration, Remote, Authentication, Crypto Maps (selected), and IPsec SAs. Under the Crypto Maps tab, there are sub-tabs for Crypto Map Entries, Peers (selected), Manual SAs, Transform Sets, and Interfaces. A table with the following columns is displayed: Priority / Seq #, Crypto Map Name, and IKE Peer. The table is empty. A link 'Show Filtering Options' is located above the table. Below the table, a message states 'Filtering is disabled'. At the bottom of the table area, there are buttons for Edit, Delete, and Add. A Help button is located in the bottom right corner of the main content area. The left sidebar also shows 'Login Details' with 'Connect To: 10.211.37.21' and 'User: admin', and a 'Message' field. At the bottom of the sidebar are buttons for Save, Logout, and Refresh.

- 3 Refer to the read-only information displayed within the *Peers* tab to determine whether a peer configuration (among those listed) requires modification or a new peer requires creation.

Priority / Seq #	Displays each peer's Seq # (sequence number) to distinguish one from the other.
Crypto Map Name	Displays the name assigned to the peer to differentiate it from others with similar configurations.
IKE Peer	Displays the IKE peer used with the Crypto Map to build an IPsec security association.

- 4 If a Crypto Map Seq # or IKE peer requires revision, select it from among those displayed and click the *Edit* button.
- 5 Select an existing Crypto Map and click the Delete button to remove it from the list of those available to the controller.

- 6 If a new peer requires creation, click the *Add* button.



The screenshot shows a dialog box titled "Security > IPsec VPN > Add Crypto Map Peer". The dialog has a title bar with a close button (X). The main area is titled "Add Crypto Map Peer" and contains two input fields: "Seq # / Name" with a dropdown arrow and "IKE Peer" with a text box. Below these fields is a "Status:" label. At the bottom, there are three buttons: "OK", "Cancel", and "Help" (with a question mark icon).

- a Define the *Seq # /Name* for the new peer.
 - b Enter the name of the *IKE Peer* used with the Crypto Map to build an IPsec security association.
- 7 Click *OK* to save the configuration of the new Crypto Map peer.

Crypto Map Manual SAs

To review, revise or add a Crypto Map using a manually defined security association:

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Click the *Crypto Maps* tab and select *Manual SAs*.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation tree with 'Security' expanded to 'IPsec VPN'. The main content area is titled 'Security > IPsec VPN' and has tabs for 'Configuration', 'Remote', 'Authentication', 'Crypto Maps', and 'IPsec SAs'. Under 'Crypto Maps', there are sub-tabs for 'Crypto Map Entries', 'Peers', 'Manual SAs', 'Transform Sets', and 'Interfaces'. The 'Manual SAs' tab is active, showing a table with the following columns: 'Priority / Seq #', 'Name', 'IKE Peer', 'ACL ID', and 'Transform Set'. The table is empty. Below the table, it says 'Filtering is disabled'. At the bottom of the table area are buttons for 'Edit', 'Delete', 'Add', and 'Help'. On the left sidebar, there is a 'Login Details' section with 'Connect To: 10.211.37.21' and 'User: admin', and a 'Message' field. At the bottom of the sidebar are 'Save', 'Logout', and 'Refresh' buttons.

- 3 Refer to the read-only information displayed within the *Manual SAs* tab to determine whether a Crypto Map (with a manually defined security association) requires modification or if a new one requires creation.

Priority / Seq #	Displays the Seq # (sequence number) used to determine priority. the lower the number the higher the priority.
Name	Displays the name assigned to the security association.
IKE Peer	Displays the IKE peer used with the Crypto Map to build an IPsec security association.
ACL ID	Displays the ACL ID the Crypto Map's data flow uses to establish access permissions.
Transform Set	Displays the transform set representing a combination of security protocols and algorithms. During the security association negotiation, peers agree to use a particular transform set for protecting the data flow.

- 4 If a Crypto Map with a manual security association requires revision, select it from among those displayed and click the *Edit* button to revise its Seq #, IKE Peer, ACL ID and security protocol.

- 5 Select an existing table entry and click the *Delete* button to remove it from the list of those available to the controller.
- 6 If a new Crypto Map manual security association requires creation, click the *Add* button.

- a Define the *Seq #*. The sequence number determines priority among Crypto Maps. The lower the number, the higher the priority.
 - b Provide a unique *Name* for this Crypto Map to differentiate it from others with similar configurations.
 - c Enter the name of the *IKE Peer* used to build an IPsec security association.
 - d Use the *ACL ID* drop-down menu to permit a Crypto Map data flow using the unique permissions within the selected ACL.
 - e Select either the *AH* or *ESP* radio button to define whether the Crypto Map's manual security association is an *AH Transform Authentication* scheme or an *ESP Encryption Transform* scheme. The *AH SPI* or *ESP SPI* fields become enabled depending on the radio button selected.
 - f Define the *In AH SPI* and *Auth Keys* or *In Esp* and *Cipher Keys* depending on which option has been selected.
 - g Use the *Transform Set* drop-down menu to select the transform set representing a combination of security protocols and algorithms. During the IPsec security association negotiation, peers agree to use the transform set for protecting the data flow. A new manual security association cannot be generated without the selection of a transform set. A default transform set is available (if none are defined).
- 7 Click *OK* when completed to save the configuration of the Crypto Map security association.

Crypto Map Transform Sets

A transform set is a combination of security protocols and algorithms defining how the controller protects data.

To review, revise or add a Crypto Map transform set:

- 1 Select *Security > IPSec VPN* from the main menu tree.
- 2 Click the *Crypto Maps* tab and select *Transform Sets*.

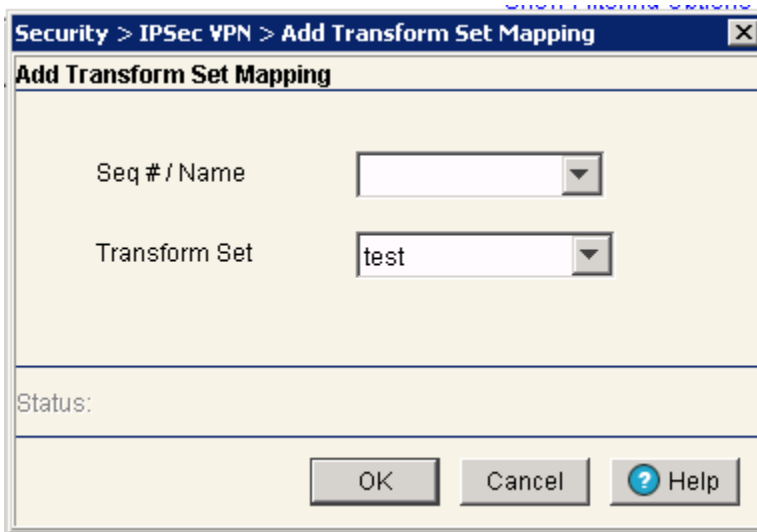
The screenshot shows the Summit WM3600 Controller web interface. The main menu on the left includes Controller, Network, Services, Security, Management Access, and Diagnostics. The Security menu is expanded, showing options like Access Point Detection, Wireless IDS/IPS, Wireless Firewalls, NAT, IKE Settings, IPSec VPN (selected), Radius Server, Server Certificates, and Enhanced Probe/Beacon Table. The main content area is titled 'Security > IPSec VPN' and has tabs for Configuration, Remote, Authentication, Crypto Maps (selected), and IPSec SAs. Under the Crypto Maps tab, there are sub-tabs for Crypto Map Entries, Peers, Manual SAs, Transform Sets (selected), and Interfaces. A table with the following columns is displayed: Priority / Seq #, Crypto Map Name, and Transform Set. The table is empty. Below the table, a message reads 'Filtering is disabled'. At the bottom of the table area, there are buttons for Edit, Delete, and Add, along with a Help button. A 'Login Details' section on the left shows 'Connect To: 10.211.37.21' and 'User: admin'. At the bottom left, there are buttons for Save, Logout, and Refresh.

- 3 Refer to the read-only information displayed within the *Transform Sets* tab to determine whether a Crypto Map transform set requires modification or a new one requires creation.

Priority / Seq #	Displays the Seq # (sequence number) used to determine priority.
Name	Displays the name assigned to the Crypto Map that is using the transform set.
Transform Set	Displays the transform set representing a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use the transform set for protecting the data flow.

- 4 Select an existing Crypto Map and click the *Edit* button to revise its Seq #, Name and Transform Set.
- 5 Select an existing entry from the table and click the *Delete* button to remove it from the list.

- 6 If a new Crypto Map transform set requires creation, click the *Add* button.



- a Select the *Seq #/Name*.
 - b Enter the name of the *Transform set* used with the Crypto Map.
- 7 Click *OK* when completed to save the configuration of the Crypto Map transform set.

Crypto Map Interfaces

To review the interfaces currently available to the Crypto Maps or assign an interface:



NOTE

A Crypto Map cannot get applied to more than one interface at a time. To apply the same Crypto Map settings to multiple interfaces, create a unique Crypto Map for each interface.

- 1 Select *Security > IPsec VPN* from the main menu tree.
- 2 Click the *Crypto Maps* tab and select *Interfaces*.

- 3 Refer to the following read-only information displayed within the *Interfaces* tab.

Name	Lists the name of the Crypto Maps available for the interface.
Interface Name	Displays the name of the interface through which IPsec traffic flows. Applying the Crypto Map set to an interface instructs the controller to evaluate all the interface's traffic against the Crypto Map set and to use the specified policy during connection or security association negotiation on behalf of traffic protected by crypto (either CET or IPsec).

- 4 Click the *Assign Interface* button to assign a Crypto Map to each interface through which IPsec traffic flows.

Assigning the Crypto Map set to an interface instructs the security appliance to evaluate all the traffic against the Crypto Map set and use the specified policy during connection or SA negotiation. Assigning a Crypto Map to an interface also initializes run-time data structures (such as the SA database and the security policy database). Reassigning a modified Crypto Map to the interface resynchronizes the run-time data structures with the Crypto Map configuration. Also, adding new peers through the new sequence numbers and reassigning the Crypto Map does not break existing connections.

Viewing IPSec Security Associations

Refer to the *IPSec SAs* tab to review the various *security associations* (SAs) between the local and remote peers comprising an IPSec VPN connection. The IPSec SA tab displays the authentication and encryption schemes used between the VPN peers as well other device address information.

To display IPSec VPN security associations:

- 1 Select *Security > IPSec VPN* from the main menu tree.
- 2 Click the *IPSec SAs* tab.

The screenshot shows the web interface for a Summit WM3600 Controller. The left sidebar contains a navigation tree with 'Security > IPSec VPN' selected. The main content area displays the 'IPSec SAs' configuration page. At the top, there are tabs for 'Configuration', 'Remote', 'Authentication', 'Crypto Maps', and 'IPSec SAs'. Below the tabs is a table with the following columns: Index, Local Peer, Remote Peer, ESP SPI In, ESP SPI Out, AH SPI In, AH SPI Out, Cipher Algorithm, and MAC Algorithm. The table is currently empty. Below the table, there is a status bar that reads 'Filtering is disabled Page 1 of 1 loaded.' At the bottom of the page, there are buttons for 'Save', 'Logout', 'Refresh', 'Stop Connection', and 'Help'.

- 3 Refer to the following security association data:

Index	Displays the numerical (if defined) ID for the security association. Use the index to differentiate the index from others with similar configurations.
-------	--

Local Peer	Displays the name of the local peer at the near side of the VPN connection.
Remote Peer	Displays the name of the remote peer at the far side of the VPN connection.
ESP SPI In	SPI specified in the <i>Encapsulating Security Payload</i> (ESP) inbound header.
ESP SPI Out	SPI specified in the <i>Encapsulating Security Payload</i> (ESP) outbound header.
AH SPI In	Displays the inbound <i>Authentication Header</i> (AH).
AH SPI Out	Displays the outbound <i>Authentication Header</i> (AH).
Cipher Algorithm	Displays the algorithm used with the ESP cipher.
MAC Algorithm	Displays the algorithm used with the security association.

- Use the page navigation facility (found on top of the table next to the *Show Filtering Options* link) to view the list of security associations.



The controller can display a maximum of 600 security associations. To enable a search through the list, the Security > IPSec VPN screen provides a page navigation facility. Up to 30 security associations display per page.

The following navigation and pagination options are available:

View All	Displays all SAs in one screen.
View By Page	Use this option to split the list into pages and view them one page at a time.

The following controls are enabled when the *View By Page* option is selected.

<<	Use this control to navigate to the first page.
<	Use this control to navigate to the previous page.
Page	Use this text box to enter the page number to jump directly to. This value cannot exceed the total number of pages.
Go	Use the Go button to jump to the page specified in the Page text box.
>	Use this control to navigate to the next page.
>>	Use this control to navigate to the last page.

- If necessary, select a security association from those displayed and click the *Stop Connection* button to stop the security association.

Configuring the RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software enabling remote access servers to communicate with the controller to authenticate users and authorize their access to the controller managed network. For an overview on the controller's RADIUS deployment, see "[RADIUS Overview](#)" on page 490.

Setting up RADIUS on the controller entails the following configuration activities:

- [Defining the RADIUS Configuration on page 493](#)

- [Configuring RADIUS Authentication and Accounting on page 496](#)
- [Configuring RADIUS Users on page 499](#)
- [Configuring RADIUS User Groups on page 503](#)
- [Viewing RADIUS Accounting Logs on page 508](#)



NOTE

For hotspot deployment, Extreme Networks recommends using the controller's onboard RADIUS server and built-in user database. This is the easiest setup option and offers a high degree of security and accountability.

RADIUS Overview

RADIUS enables centralized management of controller authentication data (usernames and passwords). When an MU attempts to associate to the RADIUS supported controller, the controller sends the authentication request to the RADIUS server. The communications between the controller and server are authenticated and encrypted through the use of a shared secret password (not transmitted over the network).

The controller's local RADIUS server stores the authentication data locally, but can also be configured to use a remote user database. A RADIUS server as the centralized authentication server is an excellent choice for performing accounting. RADIUS can significantly increase security by centralizing password management.



NOTE

The controller can be configured to use its own local RADIUS server or an external RADIUS server you define and configure. For information on the benefits and risks of using the controller's resident RADIUS Server (as opposed to an external RADIUS Server), see ["Using the Controller's RADIUS Server Versus an External RADIUS" on page 492](#).



CAUTION

When restarting or rebooting the controller, the RADIUS server is restarted regardless of its state before the reboot.

The RADIUS server defines authentication and authorization schemes for granting the access to wireless clients. RADIUS is also used for authenticating hotspot and remote VPN Xauth. The controller can be configured to use 802.1x EAP for authenticating wireless clients with a RADIUS server. The following EAP authentication types are supported by the controller's onboard RADIUS server:

- TLS
- TLS and MD5
- TTLS and PAP
- TTLS and MSCHAPv2
- PEAP and GTC
- PEAP and MSCHAPv2

Apart from EAP authentication, the controller allows the enforcement of user-based policies. User-based policies include dynamic VLAN assignment and access based on time of day.

The controller uses a default trustpoint. A certificate is required for EAP TTLS, PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after authentication with the RADIUS server. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the User associates.

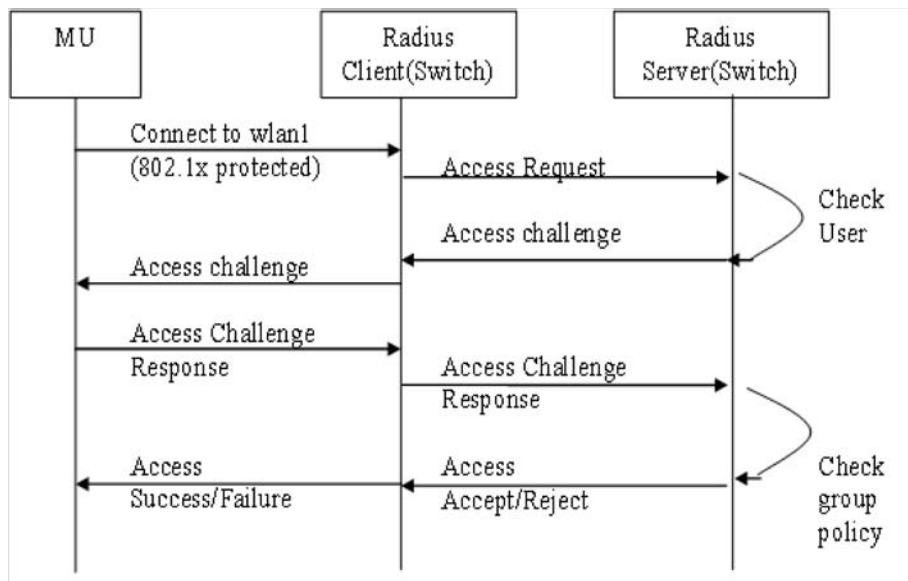


NOTE

For a RADIUS supported VLAN to function properly, the “Dynamic Assignment” checkbox must be enabled for the WLAN supporting the VLAN. For more information, see [“Editing the WLAN Configuration” on page 134](#).

For 802.1x EAP authentication, the controller initiates the authentication process by sending an EAPoL message to the Access Port only after the wireless client joins the wireless network. The RADIUS client in the controller processes the EAP messages it receives. It encapsulates them to RADIUS access requests and sends them to the configured RADIUS server (in this case the controller’s local RADIUS server).

The RADIUS server validates the user’s credentials and challenge information received in the RADIUS access request frames. If the user is authorized and authenticated, the client is granted access by sending a RADIUS access accept frame. The frame is transmitted to the client in an EAPoL frame format.



User Database

User group names and associated users (in each group) can be created in the local database. The User ID in the received access request is mapped to the associated wireless group for authentication. The controller supports the creation of 500 users and 100 groups within its local database. Each group can have a maximum of 500 users.

Authentication of Terminal/Management User(s)

The local RADIUS server can be used to authenticate users. A normal user (with a password) should be created in the local database. These users should not be a part of any group.

Access Policy

Access policies are defined for a group created in the local database. Each user is authorized based on the access policies defined for the groups to which the user belongs. Access policies allow the administrator to control access to a set of users based on the WLANs (ESSID).

Group to WLAN access is controlled using a “Time of the day” access policy.

Consider User1 (part of Group 1), which is mapped to WLAN1 (ESSID of WLAN1). When the user tries to connect to WLAN1, the user is prompted to enter his/her credentials. Once the authentication and authorization phases are successful, only User1 is able to access WLAN1 for the allowed duration (but not any other WLAN). Each user group can be configured to be a part of one VLAN. All the users in that group are assigned the same VLAN ID if dynamic VLAN authorization has been enabled on the WLAN.

Proxy to External RADIUS Server

Proxy realms are configured on the controller, which has the details of the external RADIUS server to which the corresponding realm users are to be proxied. The obtained user ID is parsed in a (user@realm, realm/user, user%realm, user/realm) format to determine which proxy RADIUS server is to be used.

LDAP

An external data source based on LDAP can be used to authorize users. The RADIUS server looks for user credentials in the configured external LDAP server and authorizes users. The controller supports two LDAP server configurations.

Accounting

Accounting should be initiated by the RADIUS client. Once the Local/Onboard RADIUS server is started, it listens for both authentication and accounting records.

Using the Controller’s RADIUS Server Versus an External RADIUS

The controller ships with a default configuration defining the local RADIUS Server as the primary authentication source (default users are admin with superuser privileges and operator with monitor privileges). No secondary authentication source is specified. However, Extreme Networks recommends using an external RADIUS Server as the primary authentication source and the local controller RADIUS Server as the secondary user authentication source. For information on configuring an external RADIUS Server, see [“Configuring External RADIUS Server Support” on page 155](#). For instructions on how to configure the controller’s local RADIUS Server, see [“Defining the RADIUS Configuration” on page 493](#).

If an external RADIUS server is configured as the controller’s primary user authentication source and the controller’s local RADIUS Server is defined as an alternate method, the controller first tries to

authenticate users using the external RADIUS Server. If an external RADIUS Server is unreachable, the controller reverts to the local Server's user database to authenticate users. However, if the external RADIUS server is reachable but rejects the user or if the user is not found in the external Server's database, the controller will not revert to the local RADIUS Server and the authentication attempt fails.

If the controller's local RADIUS Server is configured as the primary authentication method and an external RADIUS Server is configured as an alternate method, the alternate external RADIUS Server will not be used as an authentication source if a user does not exist in the local Server's database, since the primary method has rejected the authentication attempt.

Defining the RADIUS Configuration

To configure RADIUS support on the controller:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Ensure the *Configuration* tab is selected.

The screenshot displays the Summit WM3600 Controller web interface. The left sidebar shows a navigation tree with 'Security > Radius Server' selected. The main content area is titled 'Security > Radius Server' and has tabs for 'Configuration', 'Authentication', 'Users', 'Groups', and 'Accounting Logs'. The 'Configuration' tab is active, showing 'Global Settings' with a 'Start the RADIUS server' link, a 'Timeout' field set to 5 (with a range of 5-10 seconds), and a 'Retries' field set to 3 (with a range of 3-6). There are 'Apply' and 'Revert' buttons. Below this is a 'Clients' section with a 'Proxy Servers' tab and an empty table with columns for 'Realm Name', 'IP Address', and 'Port Number'. At the bottom of the table are 'Delete' and 'Add' buttons. The interface also includes a 'Login Details' section with 'Connect To: 10.211.37.21' and 'User: admin', a 'Message' field, and a footer with 'Save', 'Logout', and 'Refresh' buttons.

- 3 Click the *Start the RADIUS server* link to use the controller's own RADIUS server to authenticate users accessing the controller managed network. Again, this is recommended as the secondary means of authenticating users.
- 4 Set a *Timeout* interval (between 5 and 10 seconds) to define how long the controller waits for a reply to a RADIUS request before retransmitting the request. The default value is 5.
Ensure the value is set long enough to compensate for the heaviest periods of data traffic within the controller managed network.

- 5 Set a *Retires* value (between 3 and 6) to define the number of times the controller transmits each RADIUS request to the server before giving up. The default value is 3.
- 6 Click the *Apply* button to save the changes made to within the Global Settings field.
- 7 Click the *Revert* button to cancel any changes made within the Global Settings field and revert back to the last saved configuration.

**NOTE**

The appearance of the bottom portion of the Configuration tab differs depending on whether Clients or Proxy Servers is selected. Select the Clients tab to display the IP Address and Subnet Mask of existing RADIUS clients. Existing clients can be modified or new clients added. Select the Proxy Servers tab to display the ID suffix, IP address and Port Number of existing RADIUS proxy servers. Existing servers can be modified or new proxy servers added. For more information, see [“RADIUS Proxy Server Configuration” on page 495](#).

RADIUS Client Configuration

A RADIUS client implements a client/server mechanism enabling the controller to communicate with a central server to authenticate users and authorize access to the controller managed network. A RADIUS client is often an embedded device since it alleviates the need to store detailed user information locally.

To configure RADIUS client support:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Ensure the *Configuration* tab is selected.
- 3 Select the *Clients* tab from the bottom portion of the Configuration tab.
The Clients tab displays the IP address and subnet mask of existing RADIUS clients.
- 4 To edit an existing RADIUS client configuration, select it from the table and click the *Edit* button.
The Edit screen displays the RADIUS client's existing IP address, subnet mask and shared secret password used for credential verification. Modify these settings as required.
- 5 To remove an existing RADIUS client configuration from the table of configurations available to the controller, select a configuration and click the *Delete* button.
- 6 To create a new RADIUS client configuration, click the *Add* button at the bottom of the screen.

- a Specify the *IP Address/Mask* of the subnet or host authenticating with the RADIUS client.
- b Specify a RADIUS *Shared Secret* for authenticating the RADIUS client. Shared secrets used to verify RADIUS messages (with the exception of the Access-Request message) are sent by a

RADIUS -enabled device configured with the same shared secret. The shared secret is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 31 characters to protect the RADIUS server from brute-force attacks.

- c Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something is wrong in the transaction between the applet and the controller.
- d Click *OK* to use the changes to the running configuration and close the dialog.
- e Click *Cancel* to close the dialog without committing updates to the running configuration

RADIUS Proxy Server Configuration

The controller can be configured to send RADIUS requests to a proxy radius server. A user's access request is sent to a proxy server if it cannot be authenticated by a local server. The proxy server forwards the access request to a proxy server that can authenticate the user. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy target server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

To configure RADIUS proxy server support:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Ensure the *Configuration* tab is selected.
- 3 Select the *Proxy Servers* tab from the bottom of the Configuration tab.
The Proxy Servers tab displays the user ID suffix (index), IP address and port number of the controller's existing proxy server configurations.
- 4 To remove an existing RADIUS proxy server configuration from the table of configurations available to the controller, select the configuration and click the *Delete* button.
- 5 Click the *Add* button at the bottom of the screen to create a new RADIUS proxy server configuration.

The screenshot shows a dialog box titled "Security > Radius Server > ADD". The dialog contains the following elements:

- ADD**: A label indicating the purpose of the dialog.
- Realm Name**: A text input field.
- IP Address**: A text input field with a dotted separator (.) for the IP address format.
- Port Number**: A text input field.
- Shared Secret**: A text input field.
- Status:**: A label for the status of the configuration.
- Buttons**: Three buttons at the bottom: "OK", "Cancel", and "Help".

- a Create a new *User ID Suffix* as an abbreviation to differentiate the configuration from others with similar attributes.
- b Specify the *IP Address* of the new RADIUS proxy server.

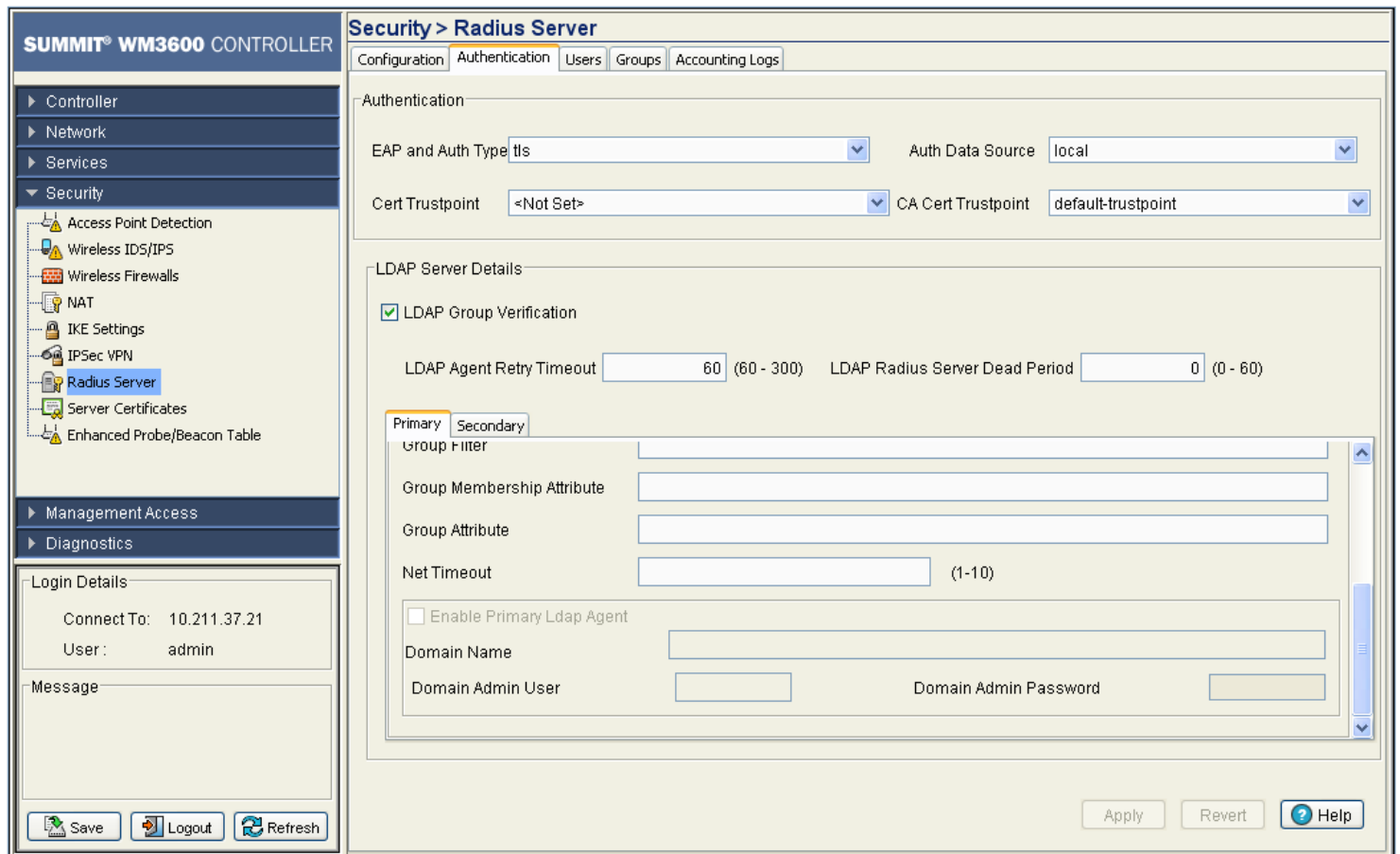
- c Enter the TCP/IP port number used by the proxy RADIUS server.
- d Specify a RADIUS *Shared Secret* for authenticating the RADIUS client.
The shared secret is used to verify RADIUS messages. It is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 31 characters long to protect the RADIUS server from brute-force attacks.
- e Shared secrets verify RADIUS messages (with the exception of the Access-Request message) are sent by a RADIUS-enabled device configured with the same shared secret.
The shared secret is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 22 characters long to protect the RADIUS server from brute-force attacks. The max length of the shared secret is 31 characters.
- f Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- g Click *OK* to use the changes to the running configuration and close the dialog.
- h Click *Cancel* to close the dialog without committing updates to the running configuration

Configuring RADIUS Authentication and Accounting

Deploy one or more RADIUS servers to manage security and retrieve accounting information from the controller managed network. RADIUS accounting supplies administrators with user data as RADIUS sessions are started and terminated.

To define the RADIUS authentication and accounting configuration:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Select the *Authentication* tab.



3 Refer to the *Authentication* field to define the following RADIUS authentication information:

- | | |
|-------------------|--|
| EAP and Auth Type | Specify the EAP type for the RADIUS server. <ul style="list-style-type: none"> • <i>PEAP</i> uses a TLS layer on top of EAP as a carrier for other EAP modules. PEAP is an ideal choice for networks using legacy EAP authentication methods. • <i>TTLS</i> is similar to EAP-TLS, but the client authentication portion of the protocol is not performed until after a secure transport tunnel has been established. This allows EAP-TTLS to protect legacy authentication methods used by some RADIUS servers. |
| Auth Data Source | Use <i>Auth Data Source</i> drop-down menu to select the data source for the local RADIUS server. <ul style="list-style-type: none"> • If <i>Local</i> is selected, the controller's internal user database serves as the data source for user authentication. Refer to the <i>Users</i> and <i>Groups</i> tabs to define user and group permissions for the controller's local RADIUS server. • If <i>LDAP</i> is selected, the controller uses the data within an LDAP server. |

- Cert Trustpoint** Click the *View/Change* button to specify the trustpoint from which the RADIUS server automatically grants certificate enrollment requests. A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. If the server certificate trustpoint is not used, the default trustpoint is used instead.
- CA Cert Trustpoint** Click the *View/Change* button to specify the CA certificate trustpoint from which the RADIUS server automatically grants certificate enrollment requests. A trustpoint is a representation of a CA or identity pair. A trustpoint contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.

If a CA trustpoint is not specified, the default trustpoint's CA certificate is used as a CA certificate. If the "Default trustpoint" does not have a CA certificate, the server certificate is used as the CA certificate.



NOTE

EAP-TLS will not work with a default trustpoint. Proper CA and Server trustpoints must be configured for EAP-TLS. For information on configuring certificates for the controller, see ["Creating Server Certificates" on page 509](#).

- 4 Select LDAP Group Verification Details checkbox. Refer to the *LDAP Server Details* field to define the primary and secondary RADIUS LDAP server configuration providing access to an external database used with the local RADIUS server.

- IP Address** Enter the IP address of the external LDAP server acting as the data source for the RADIUS server. This server must be accessible from an active controller subnet.
- Port** Enter the TCP/IP port number for the LDAP server acting as the data source.
- Password Attribute** Enter the password attribute used by the LDAP server for authentication.
- Bind DN** Specify the distinguished name to bind with the LDAP server.
- Bind Password** Enter a valid password for the LDAP server.
- Base DN** Specify a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.
- User Login Filter** Enter the login used by the LDAP server for authentication.
- Group Filter** Specify the group filters used by the LDAP server.
- Group Membership Attribute** Specify the Group Member Attribute sent to the LDAP server when authenticating users.
- Group Attribute** Specify the group attribute used by the LDAP server.
- Net Timeout** Enter a timeout value (between 1-10 seconds) the system uses to terminate the connection to the RADIUS Server if no activity is detected.

- 5 Enable the *Enable Primary Ldap Agent* checkbox to support the PEAP-MSCHAPv2 authentication system with user/password database as Active Directory.

- Domain Name** Enter the Active Directory domain name. e.g. [ExtremeAD.com](#)
- Domain Admin User** Enter the Administrator Username of the LDAP server
- Domain Admin Password** Enter the Administrator User password

LDAP Agent Retry Timeout	Defines the time interval after which the LDAP Agent will try to reconnect with the LDAP server if the previous join attempt had failed.
LDAP Server Dead Period	This is a period in seconds for which the RADIUS server does not attempt any connection with the LDAP server after the LDAP server was found to be unavailable.



NOTE

Administrator Username and Administrator User password are required for the controller (which runs radius server) to become part of the Windows domain of which the Active Directory Server is part of.



NOTE

The same configuration is supported for the Secondary LDAP agent of the Secondary LDAP server.

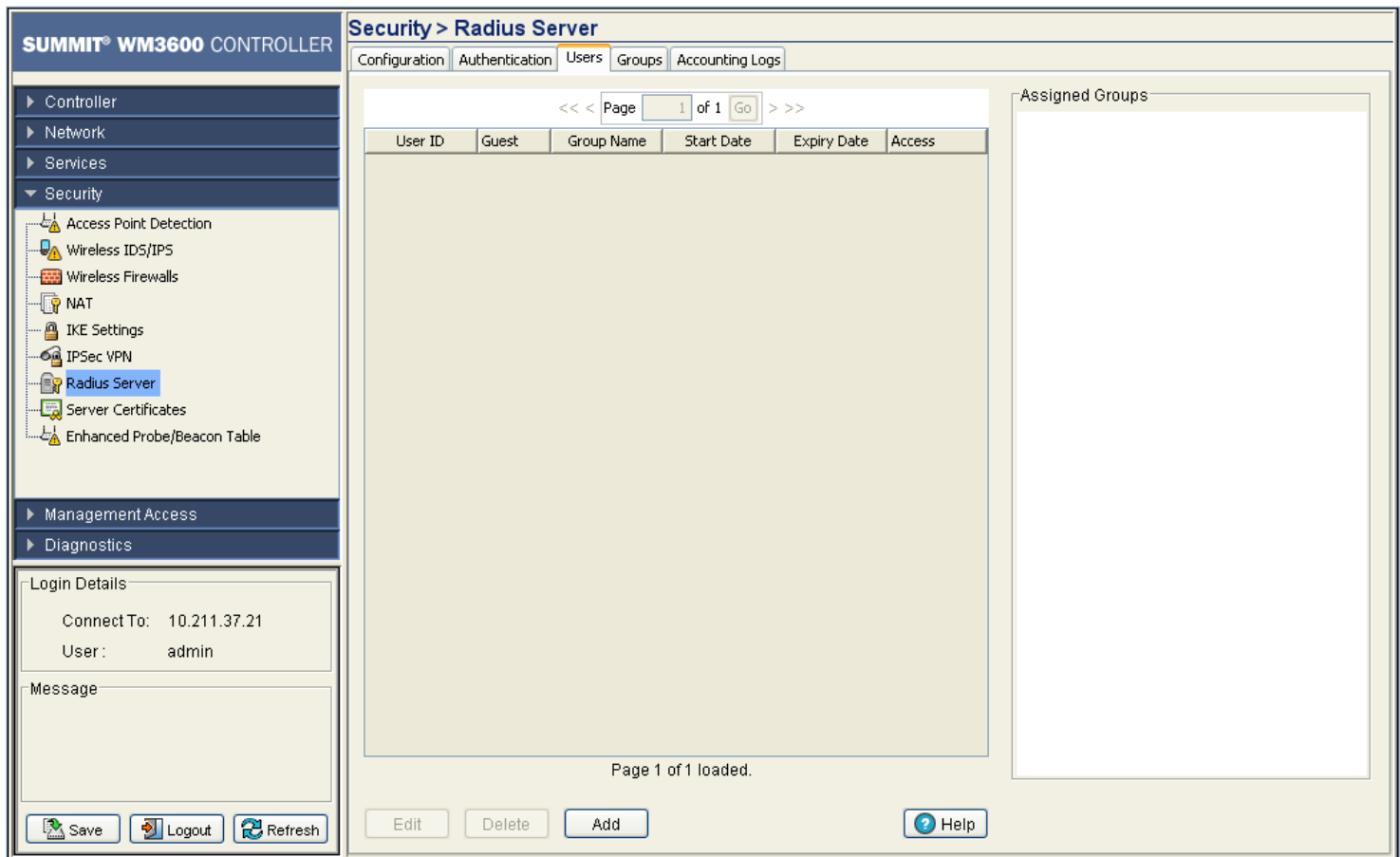
- 6 Click the *Apply* button to save the changes made to within the screen.
- 7 Click the *Revert* button to cancel any changes made within the screen and revert back to the last saved configuration.

Configuring RADIUS Users

Refer to the *Users* tab to view the current set of users and groups assigned for the RADIUS server. The *Users* tab is employed when *Local* is selected as the Auth Data Source within the *Authentication & Accounting* tab.

To define the RADIUS user permissions for controller access:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Select the *Users* tab.



- 3 Refer to the following to assess whether an existing user can be used with the local RADIUS server as is, requires modification or if a new user is required.

User ID	Displays the username for this specific user. The name assigned should reflect the user’s identity and perhaps their status within the controller managed network (guest versus secure user).
Guest User	Displays whether a specific user has been defined as a guest user (with a green check) or has been configured as permanent user. Guest users have temporary access.
Group Name	Displays the unique name assigned to each group. The group name should be indicative of the user population and their shared activity within the controller-managed network.
Start Date	Defines the time when Guest User’s privileges commence.
Expiry Date	If the user has been assigned guest privileges, they were also assigned a date when their RADIUS privileges expire.
Access Duration	Defines the authentication period set by the user. Check this option to enter a user-defined interval in the text field.
	Note: It is strictly recommended to set “Hotspot Simultaneous Users” to “1” in the Hotspot page while using the Guest User option. This denies authentication to the second MU when it uses a login already in use.

-
- 4 Refer to the *Available Groups* field to view the memberships for existing users.

If the group assignment is insufficient, use the *Edit* or *Add* functions to modify/create users or modify their existing group assignments. For guest users, only the password is editable. For normal (non-guest) users, the password and group association can be modified.

To modify the attributes of an existing user, select the user from the list and click the *Edit* button.

Modify the existing user's guest designation, password, expiry date and group assignments as required to reflect the user's current local RADIUS authentication requirements.

- 5 If an existing user is no longer needed, select the user from those displayed and click the *Delete* button to permanently remove the user.
- 6 To create a new user for use with the local RADIUS server, click the *Add* button and provide the following information.



CAUTION

If password encryption is not enabled, RADIUS user passwords are stored in the running configuration file in clear text. The user passwords are shown as encrypted if the global password encryption is enabled. The maximum for the file is 5000 users, 100 groups, 25 clients, 5 realms and 2 LDAP servers.

- User ID Define a unique user ID that differentiates this user from others with similar attributes.
- Guest User Select the *Guest User* checkbox to assign this particular user temporary access to the local RADIUS server, thus restricting their authentication period to a user defined interval.
- Password Enter the password that adds the user to the list of approved users displayed within the Users tab.
- Confirm Password Re-enter (confirm) the password used to add the user to the list of approved users displayed within the Users tab.

Current Controller Time	Displays the read only controller time. This is the time used for expiry data and time.sers tab.
Start Date & Time	Defines the start date and time (in dd:MM:yyyy-hh:mm format) to login guest users defined with temporary permissions.
Expiry Date & Time	Defines the date and time (in dd:MM:yyyy-hh:mm format) to timeout guest users defined with temporary permissions.
Access Duration	Defines the authentication period set by the user. Check this option to enter a user-defined interval in the text field. It is strictly recommended to set "Hotspot Simultaneous Users" to "1" in the Hotspot page while using the Guest User option. This denies authentication to the second MU when it uses a login already in use.
Available Groups	Use the Available Groups <i>Add -></i> and <i>Remove <-</i> functions to map groups (for inclusion) for this specific user.
Configured Group	Displays existing groups available for the user.

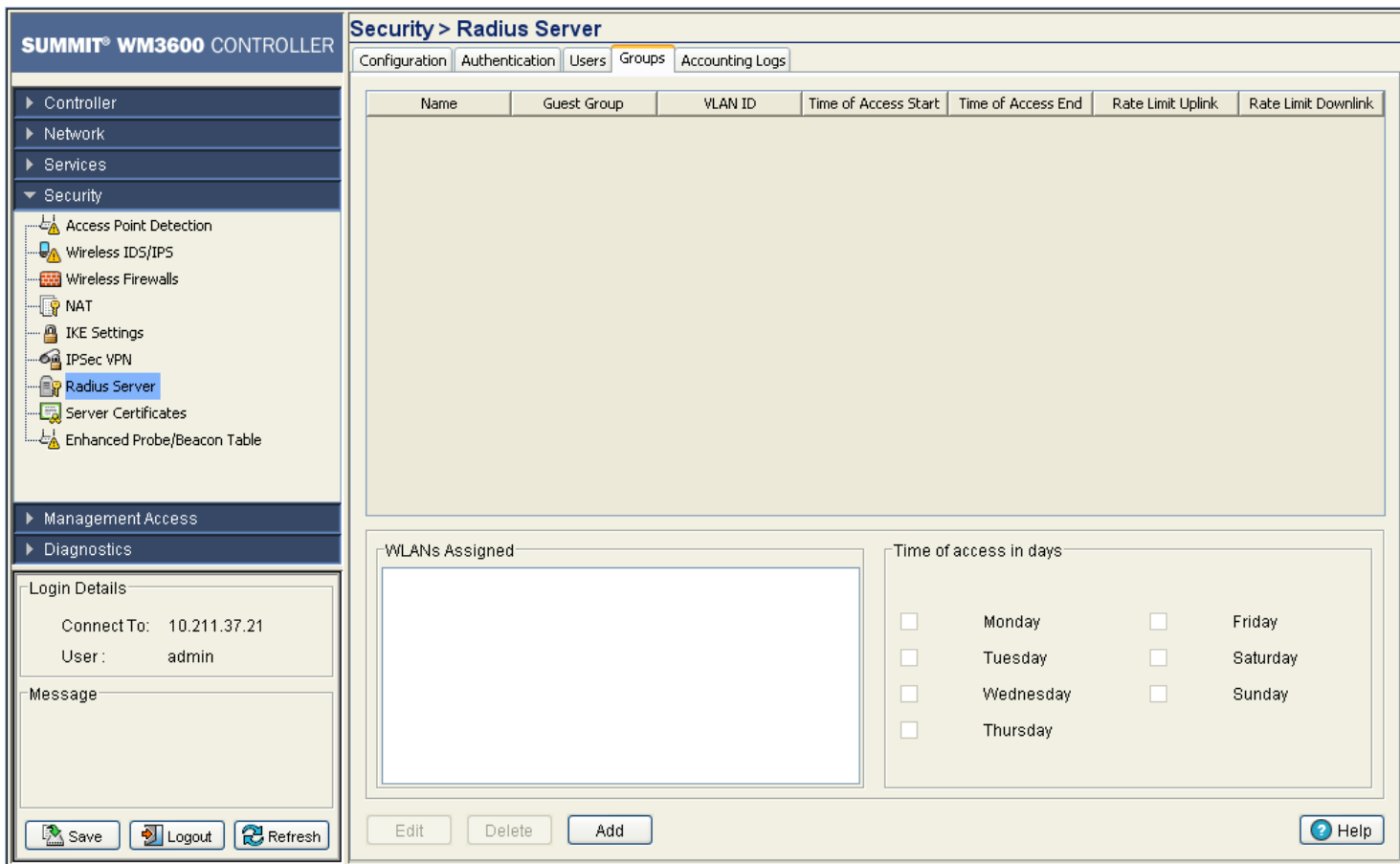
- a Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- b Click *OK* to use the changes to the running configuration and close the dialog.
- c Click *Cancel* to close the dialog without committing updates to the running configuration

Configuring RADIUS User Groups

The *Groups* tab displays a list of all groups in the local RADIUS server's database. The groups are listed in the order added. The existing configuration for each group is displayed to provide the administrator the option of using a group as is, modifying an existing group's properties or creating a new group.

To access the configuration of existing user groups:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Select the *Groups* tab.



3 Refer to the user groups listed to review the following read-only attributes for each group:

Name	Displays the unique name assigned to each group. The group name should be indicative of the user population within and their shared activity within the controller managed network.
Guest Group	Displays whether a specific group has been defined as a guest group (indicated with a green check mark) or has been configured as permanent group (indicated with a red X). Guest users have temporary RADIUS server access.
VLAN ID	Display the VLAN ID(s) used by each group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate with one another within the controller managed network (once authenticated by the local RADIUS server).
Time of Access Start	Displays the time each group is authenticated to interoperate within the controller managed network. Each user within the group is authenticated with the local RADIUS server. Group members successfully authenticated are allowed access to the controller managed network under the restrictions defined for that group.

Time of Access End	Displays the time each group's user base will lose access privileges. After this time, users within this group will not be authenticated by the local RADIUS server. However, if a user is part of a different group that has not exceeded their access interval, then the user may still interoperate with the controller (remain authenticated) as part of that group.
Rate Limit Uplink	Set the rate limit from the wireless client to the network when using the RADIUS authentication. A rate limit of 0 disables rate limiting for this direction. Any rate limit obtained through RADIUS server authentication overwrites the initial user rate limit for the given MU.
Rate Limit Downlink	Set the rate limit from the network to the wireless client when using the RADIUS authentication. Any rate limit obtained through radius server authentication overwrites the initial user rate limit for the given MU.

- 4 Refer to the *WLANs Assigned* area of the Groups tab to review which controller WLANs are available for use with configured groups.
- 5 Refer to the *Time of access in days* field to assess the intervals (which days) the group has been assigned access to the controller managed network (after each user has been authenticated). At least one day is required.

This value is read-only within the Groups tab. Click *Edit* to modify the access assignments of an existing group or click *Add* to create a new group with unique access assignments.

Security > Radius Server > ADD

ADD

Name

Guest Group

VLAN ID

Time of Access Start (HHMM)

Time of Access End (HHMM)

Rate Limit Uplink (0, 100 - 100000) kbps

Rate Limit Downlink (0, 100 - 100000) kbps

Available WLANs

- WLAN 1 (ESS ID : 101)
- WLAN 2 (ESS ID : 102)
- WLAN 3 (ESS ID : 103)
- WLAN 4 (ESS ID : 104)
- WLAN 5 (ESS ID : 105)
- WLAN 6 (ESS ID : 106)
- WLAN 7 (ESS ID : 107)

Configured WLANs

Add →

← Remove

Time of Access in days

Monday Tuesday Wednesday Thursday

Friday Saturday Sunday

Select All

Status:

OK Cancel ? Help

- To modify the attributes of an existing group, select the group from the list of groups displayed and click the *Edit* button.

Modify the existing group's guest designation, VLAN ID, access period and WLAN assignment.

- If an existing group is no longer needed (perhaps obsolete in function), select the group and click the *Delete* button to permanently remove the group from the list. The group can only be removed if all the users in the group are removed first.

8 To create a new group, click the *Add* button and provide the following information.

Name	Define a unique group name that differentiates this new group from others with similar attributes.
Guest Group	Select the <i>Guest Group</i> checkbox to assign this particular group (and the users within) only temporary access to the local RADIUS server, thus restricting their authentication period to a user defined access interval.
VLAN ID	Define the VLAN ID for the new group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the controller managed network (once authenticated by the local RADIUS server).
Time of Access Start	Set the time the group is authenticated to interoperate. Each user within the group is authenticated with the local RADIUS server. Those group members successfully authenticated are allowed access to the controller using the restrictions defined for the group.
Time of Access End	Set the time each group's user base will loose access privileges within the controller managed network. After this time, users within this group will not be authenticated by the local RADIUS server. However, if a user is part of a different group that has not exceeded their access end interval, the user may still interoperate with the controller (remain authenticated) as part of that group.
Rate Limit Uplink (0,100-100000)	Set the rate limit from the wireless client to the network when using RADIUS authentication. A rate limit of 0 disables rate limiting for this direction. Any rate limit obtained through RADIUS server authentication overwrites the initial user rate limit for the given MU.
Rate Limit Downlink (0,100-100000)	Set the rate limit from the network to the wireless client when using RADIUS authentication. Any rate limit obtained through RADIUS server authentication overwrites the initial user rate limit for the given MU.
Available WLANs	Use the Available WLANs <i>Add</i> -> and <i>Remove</i> <- functions to move WLANs for this new group from the available list to the configured list. Once on the configured list (and the changes applied), the members of this group can interoperate with the controller on these WLANs (once authenticated by the local RADIUS server).
Configured WLANs	The Configured WLANs columns displays the WLANs this new group can operate within (once users are configured). Use the <i>Add</i> -> and <i>Remove</i> <- functions to move WLANs from the available list to the configured list.
Time of access in days	Select the checkboxes corresponding to the days of the week you would like this new group to have access to the controller managed network. Of course, the user base within the group still needs to be authenticated by the local RADIUS server first.



NOTE

Rate limiting parameters need to be part of RADIUS Access Accept packets. If any RADIUS server doesn't send rate limit parameters in RADIUS Access Accept packet, these parameters will not be configured.

9 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

10 Click *OK* to use the changes to the running configuration and close the dialog.

11 Click *Cancel* to close the dialog without committing updates to the running configuration.

Viewing RADIUS Accounting Logs

Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to a location outside of the controller for periodic network and user permission administration.

To display the RADIUS accounting logs:

- 1 Select *Security > Radius Server* from the main menu.
- 2 Select the *Accounting Logs* tab.

The screenshot displays the Summit WM3600 Controller web interface. The left sidebar shows the navigation menu with 'Security' expanded to 'Radius Server'. The main content area is titled 'Security > Radius Server' and has the 'Accounting Logs' tab selected. Below the breadcrumb navigation, there is a file browser view showing the path 'flash:/log/radius/' and a table with columns for 'Filename', 'Type', and 'Size'. The table is currently empty. At the bottom of the interface, there are buttons for 'Save', 'Logout', 'Refresh', 'Transfer Files', and 'Help'.

- 3 Refer to the following information as displayed within the *Accounting Logs* tab.

Filename	Displays the name of each accounting log file. Use this information to differentiate files with similar attributes.
Type	Displays the type of file each file is.
Size	Display the size of the file.



NOTE

An explicit purge operation is not supported, the accounting logs are purged automatically once they reach their limit.

Creating Server Certificates

Use the *Server Certificates* screen to view existing self-signed certificate values. The values displayed are read-only. The Server Certificates screen also allows an administrator to:

- Create a certificate request
- Send it to a Certificate Authority (CA)
- Create a self signed certificate
- Upload an external certificate
- Delete a server certificate and/or root certificate of a trustpoint
- Create a new key
- Upload/download keys to and from the controller to and from a server or local disk
- Delete all the keys in the controller.

Server certificates are issued to Web Servers and used to authenticate Web Servers to browsers while establishing a *Secure Socket Layer* (SSL) connection.

The *Server Certificates* screen displays two tabs supporting the following:

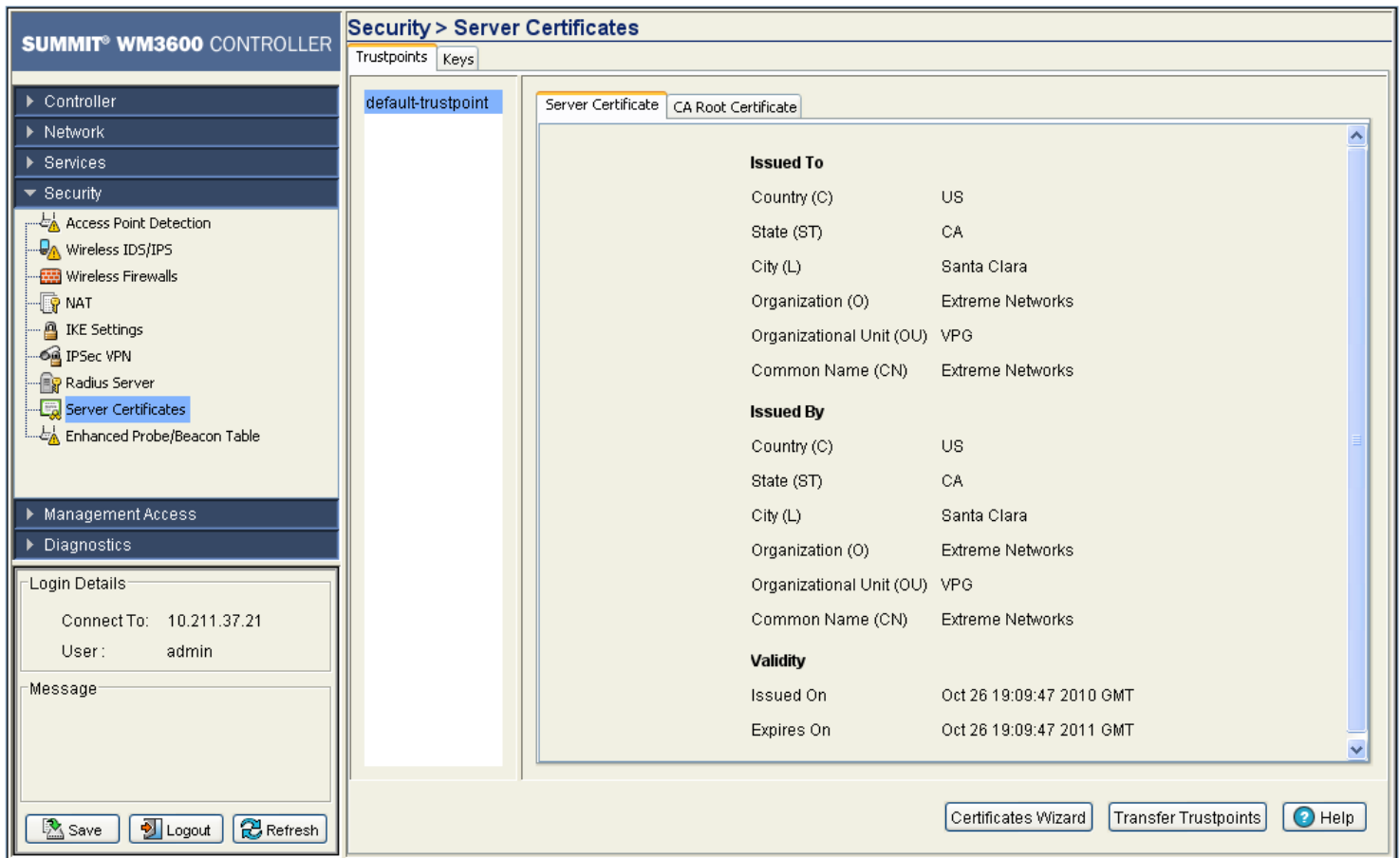
- [Using Trustpoints to Configure Certificates on page 509](#)
- [Certificate Authority Root Certificates on page 520](#)

Using Trustpoints to Configure Certificates

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

To view current certificates values:

- 1 Select *Security > Server Certificates* from the main menu tree.
- 2 Select the *Trustpoints* tab.



A panel (on the left of the screen) displays currently enrolled trustpoints.

The *Server Certificate* and *CA Root Certificate* tabs display read-only credentials for the certificates in use by the controller. A table displays the following *Issued To* and *Issued By* details for each:

Issued To

- Country (C) Displays the country of usage for which the certificate was assigned.
- State (ST) Displays the state (if within the US) or province within the country listed above wherein the certificate was issued.
- City (L) Lists the city wherein the server certificate request was made. The city should obviously be within the State/Prov. stated.
- Organization (O) Displays the name of the organization making the certificate request.
- Org. Unit (OU) Displays the name of the organizational unit making the certificate request.
- Common Name (CN) If there is a common name (IP address) for the organizational unit making the certificate request, it displays here.

Issued By

- Country (C) Displays the country of the certificate issuer.

State (ST)	Displays the state or province for the country the certificate was issued.
City (L)	Displays the city representing the state/province and country from which the certificate was issued.
Organization (O)	Displays the organization representing the certificate authority
Organizational Unit	If a unit exists within the organization that is representative of the certificate issuer, that name should be displayed here.
Common Name	If there is a common name (IP address) for the organizational unit issuing the certificate, it displays here.

Validity

Issued On	Displays the date the certificate was originally issued.
Expires On	Displays the expiration date for the certificate.

- 3 Click the *Certificate Wizard* button to create a self signed certificate, upload an external server certificate (and/or a root certificate) or delete a server certificate (and/or a root certificate) of a trustpoint. For more information, see [“Using the Wizard to Create a New Certificate”](#) on page 513.

Creating a Server / CA Root Certificate

To create a Server Certificate or import a CA Root Certificate:

- 1 Select *Security > Server Certificates* from the main menu tree.
- 2 Click the *Certificates Wizard* button on the bottom of the screen.

The screenshot shows the Summit WM3600 Controller web interface. The main menu on the left includes Controller, Network, Services, Security, Management Access, and Diagnostics. The Security menu is expanded, showing options like Access Point Detection, Wireless IDS/IPS, Wireless Firewalls, NAT, IKE Settings, IPsec VPN, Radius Server, Server Certificates, and Enhanced Probe/Beacon Table. The Server Certificates page is displayed, with the 'default-trustpoint' tab selected. The 'Server Certificate' sub-tab is active, showing a form with the following fields:

Issued To	
Country (C)	US
State (ST)	CA
City (L)	Santa Clara
Organization (O)	Extreme Networks
Organizational Unit (OU)	VPG
Common Name (CN)	Extreme Networks

Issued By	
Country (C)	US
State (ST)	CA
City (L)	Santa Clara
Organization (O)	Extreme Networks
Organizational Unit (OU)	VPG
Common Name (CN)	Extreme Networks

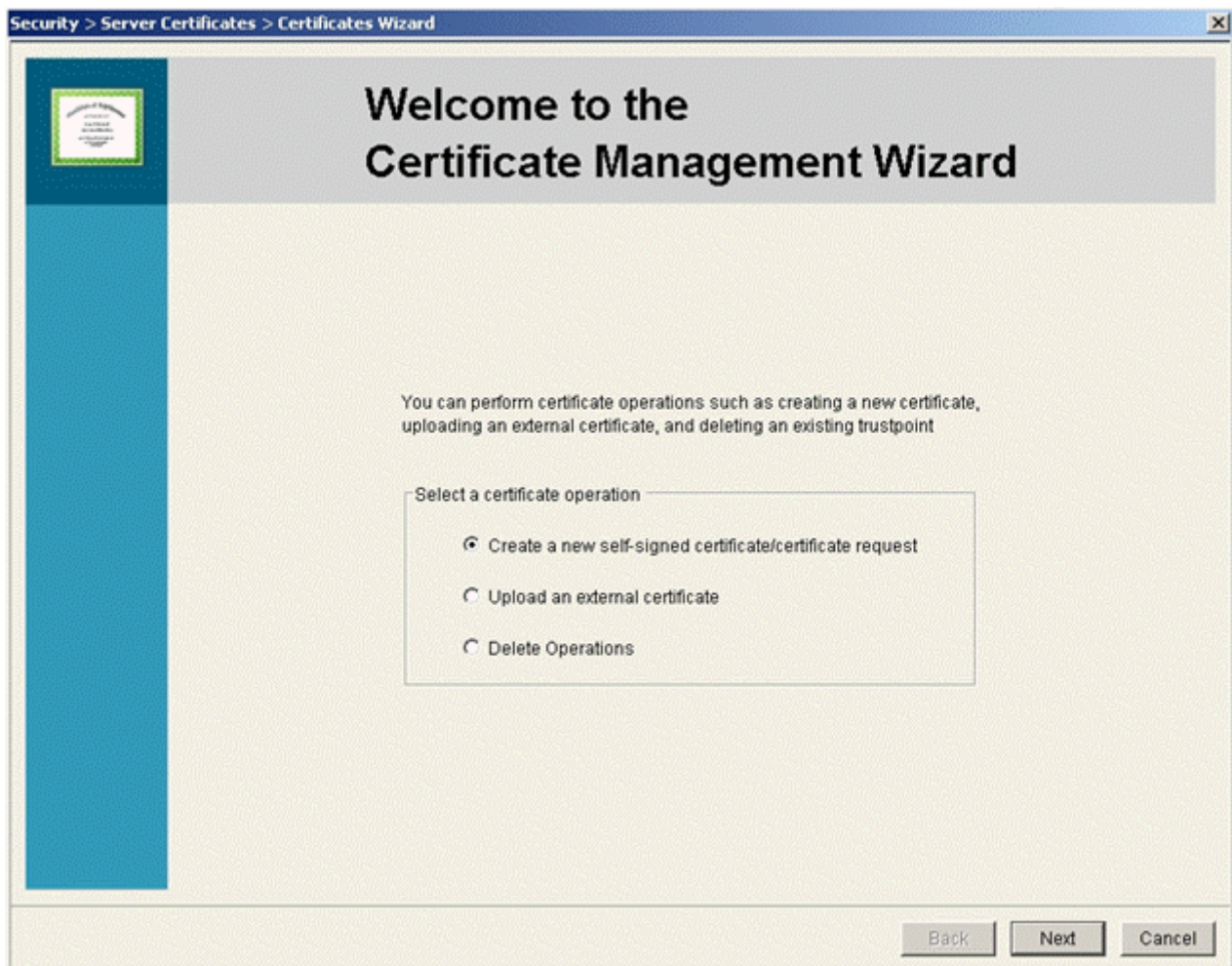
Validity	
Issued On	Oct 26 19:09:47 2010 GMT
Expires On	Oct 26 19:09:47 2011 GMT

At the bottom of the page, there are buttons for 'Certificates Wizard', 'Transfer Trustpoints', and 'Help'. The 'Certificates Wizard' button is highlighted.

- 3 Use this wizard for:
 - Creating a new self-signed certificate or certificate request
 - Uploading an external certificate
 - Delete Operations
- 4 Select the *Create new certificate* radio button to generate a new self-signed certificate or prepare a certificate request which can be sent to a Certificate Authority (CA).
For more information, see [“Using the Wizard to Create a New Certificate” on page 513](#).
- 5 Select the *Upload an external certificate* radio button to upload an existing Server Certificate or CA Root Certificate.
For more information, see [“Using the Wizard Delete Operation” on page 518](#).
- 6 Select the *Delete Operations* radio button to delete trustpoints and all related keys.
For more information, see [“Using the Wizard Delete Operation” on page 518](#).

Using the Wizard to Create a New Certificate. To generate a new self-signed certificate or prepare a certificate request:

- 1 Select the *Create new self-signed certificate /certificate request* radio button in the wizard and click the *Next* button.



The second page of the wizard contains three editable fields, *Select Certificate Operation*, *Select a Trustpoint*, and *Specify a key for you new certificate*.

- 2 Use the second page to create either a self signed certificate or prepare a certificate request. For certificate creation, select one of the following options:
- *Generate a self signed certificate*—Configure the properties of a new self-signed certificate. Once the values of the certificate are defined, the user can create and install the certificate.
 - *Prepare a certificate request to send to a Certificate Authority*—Configure and save a valid certificate request. Once the values of the certificate are defined, the user can configure and enroll the trustpoint.

You can generate a new self-signed certificate, or prepare a certificate request to send to a certificate authority.

Select a certificate operation

Generate a self-signed certificate

Prepare a certificate request to send to a certificate authority

Select a trustpoint for the new certificate

Use existing trustpoint

Create a new trustpoint

Specify a key for your new certificate

Automatically generate a key

Use existing key

Create a new key

Key Name

Key Size (Bytes) (1024 - 2048)

Select a trustpoint for the new certificate.

- *Use existing trustpoint*—Select an existing trustpoint from the drop-down menu.
- *Create a new trustpoint*—Provide a name for the new trustpoint in the space provided.

To specify a key for a new certificate, select one of the following:

- *Automatically generate a key*—Automatically generates a key for the trustpoint.
- *Use existing key*—Specify an existing key using the drop-down menu.
- *Use a new key*—Select this option to create a new key for the trustpoint. Define a key name and size as appropriate.

Associate the certificate selected with one of the options provided in the *Specify a key for your new certificate* and click the *Next* button.

If generating a new self-signed certificate (as selected in page 2 of the wizard), the wizard continues the installation. Use the third page of the wizard to enter a unique trustpoint name and other credentials required to create the new certificate.

You have successfully configured the trustpoint bb. A key will be automatically generated for your new certificate.

Enter other credentials for the new certificate.
To generate a default certificate, select the 'Automatically generate certificate with default values' option.

Configure the trustpoint

Automatically generate certificate with default values.

Enter certificate credentials:

Country (C)* (2 characters)

State (ST)* (2-128 characters)

City (L)* (2-128 characters)

Organization (O)* (2-64 characters)

Organizational Unit (OU)* (2-64 characters)

Common Name (CN)* (2-64 characters)

Email Address (2-64 characters)

FQDN (9-64 characters)

IP Address

Enroll the trustpoint

A trustpoint is enrolled if it contains either a server certificate or a pending request for a server certificate

Back Next Cancel

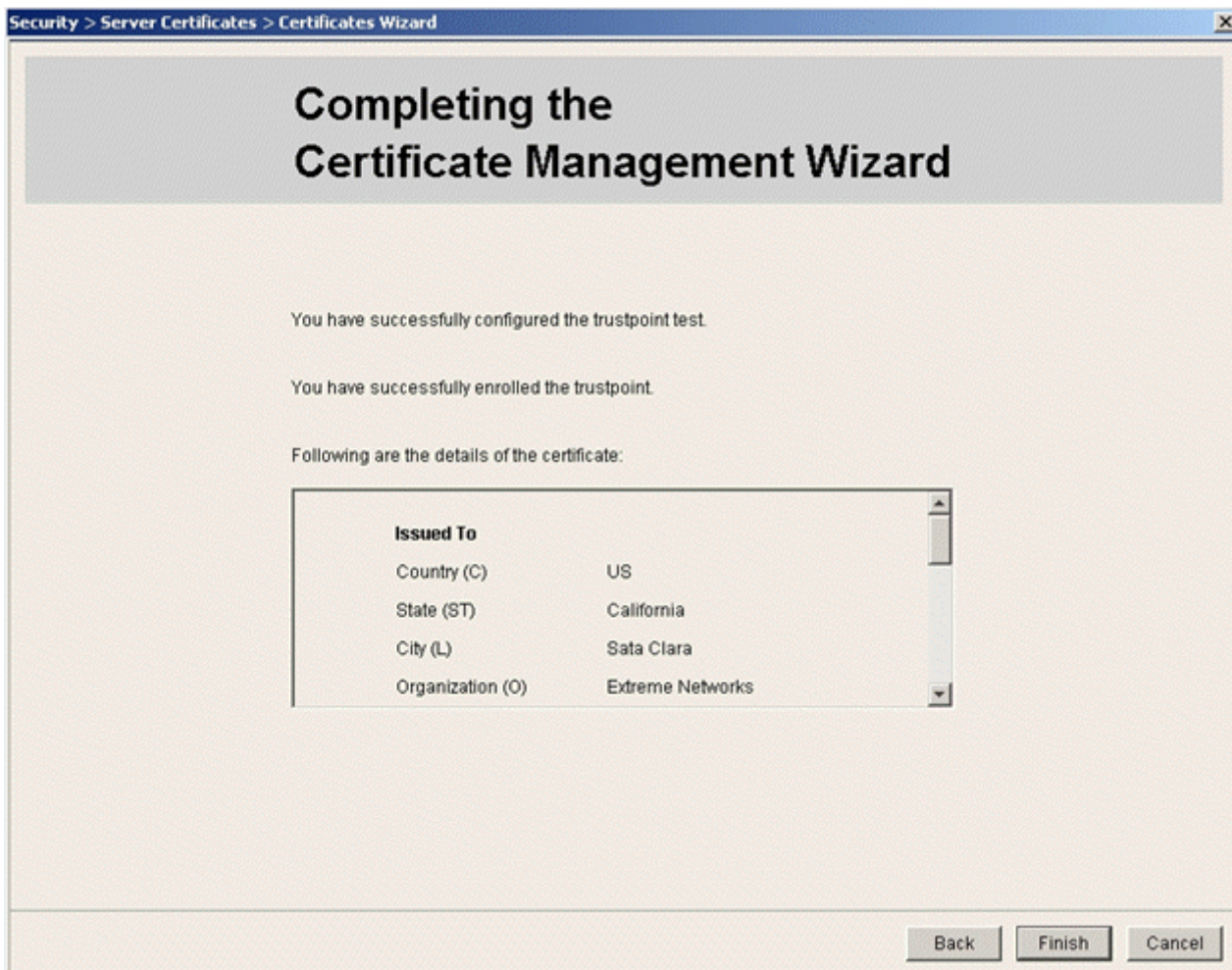
- 3 Select the *Configure the trustpoint* checkbox to enable the new self signed certificate configured as a trustpoint.
- 4 Select the *Automatically generate certificate with default values* checkbox to create a certificate using values the controller assigns by default.
This option is recommended for generic certificates that do not represent a unique or custom controller configuration.
- 5 Select the *Enter certificate credentials* radio button to manually enter the values of a unique certificate. If you anticipate using generic (default) values, consider using the *Automatically generate certificate with default values* option.
- 6 Provide the following information for the certificate:

Country	Define the Country used in the Self-Signed Certificate. By default, the Country is US. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.
State	Enter a State/Prov. for the state or province name used in the Self-Signed Certificate. By default, the State/Prov. field is CA. This is a required field.
City	Enter a City to represent the city name used in the Self-Signed Certificate. By default, the City name is San Jose. This is a required field.

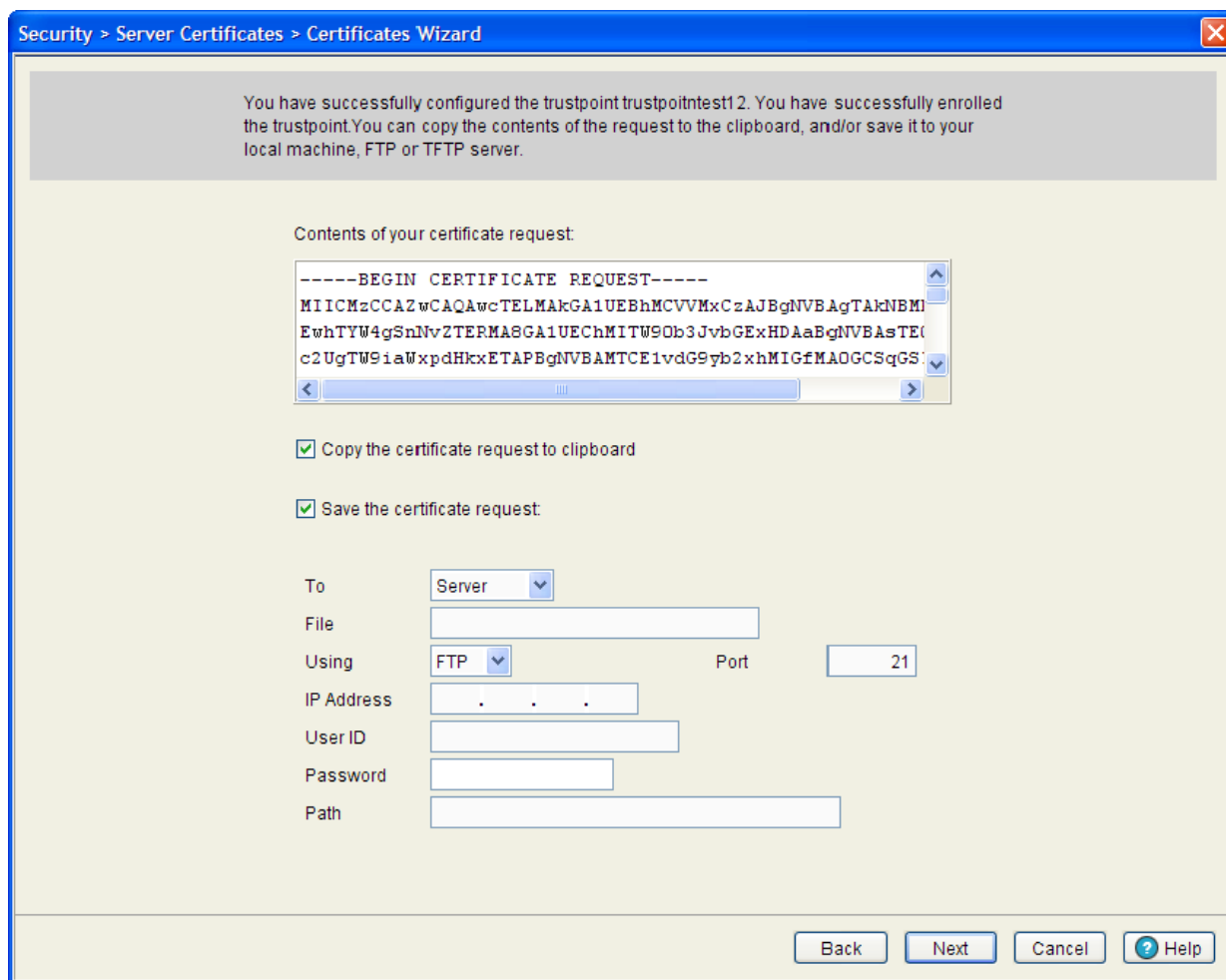
Organization	Define an Organization for the organization used in the Self-Signed Certificate. By default, it is Extreme Networks. The user is allowed to modify the Organization name. This is a required field.
Organization Unit	Enter an Org. Unit for the name of the organization unit used in the Self-Signed Certificate. By default, it is Wireless Controller Division. This is a required field.
Email Address	Provide an email address used as the contact address for issues relating to this certificate request.
FQDN	Enter a <i>fully qualified domain name</i> (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. ex: somehost.example.com. An FQDN differs from a regular domain name by its absoluteness; as a suffix is not added.
IP Address	Specify the controller IP address used as the controller destination for certificate requests.

- 7 Select the *Enroll the trustpoint* checkbox to enroll the certificate request with the CA.
- 8 Click *Next* to proceed with the certificate creation.

If you created a self-signed certificate on page 2, the wizard completes and displays the details of the newly created self-signed certificate.



If you selected to prepare a certificate request in the page 2, the wizard continues, prompting the user for the required information to complete the certificate request. Click *Next* to continue.



- 9 Check the *Copy the certificate request to clipboard* option to add the contents of the certificate request to the clipboard which can then be copied to other locations.
- 10 Check the *Save the certificate request option* to save the certificate request to an external server and provide the server information in the fields below:

To	Use the <i>To</i> field to define whether the target certificate is to be sent to the system's local disk (<i>Local Disk</i>) or to an external server (<i>Server</i>).
File	Specify a filename for the certificate to be save as on the target server or local disk.
Using	Use the Using drop down-menu to configure whether the log file transfer is sent using <i>FTP</i> or <i>TFTP</i> .
IP Address	Specify the server <i>IP Address</i> used as the controller destination for certificate requests.
User ID	Enter the <i>User ID</i> credentials required to send the file to the target location.
Password	Use the User ID for FTP transfers only Enter the <i>Password</i> required to send the file to the target location using FTP.

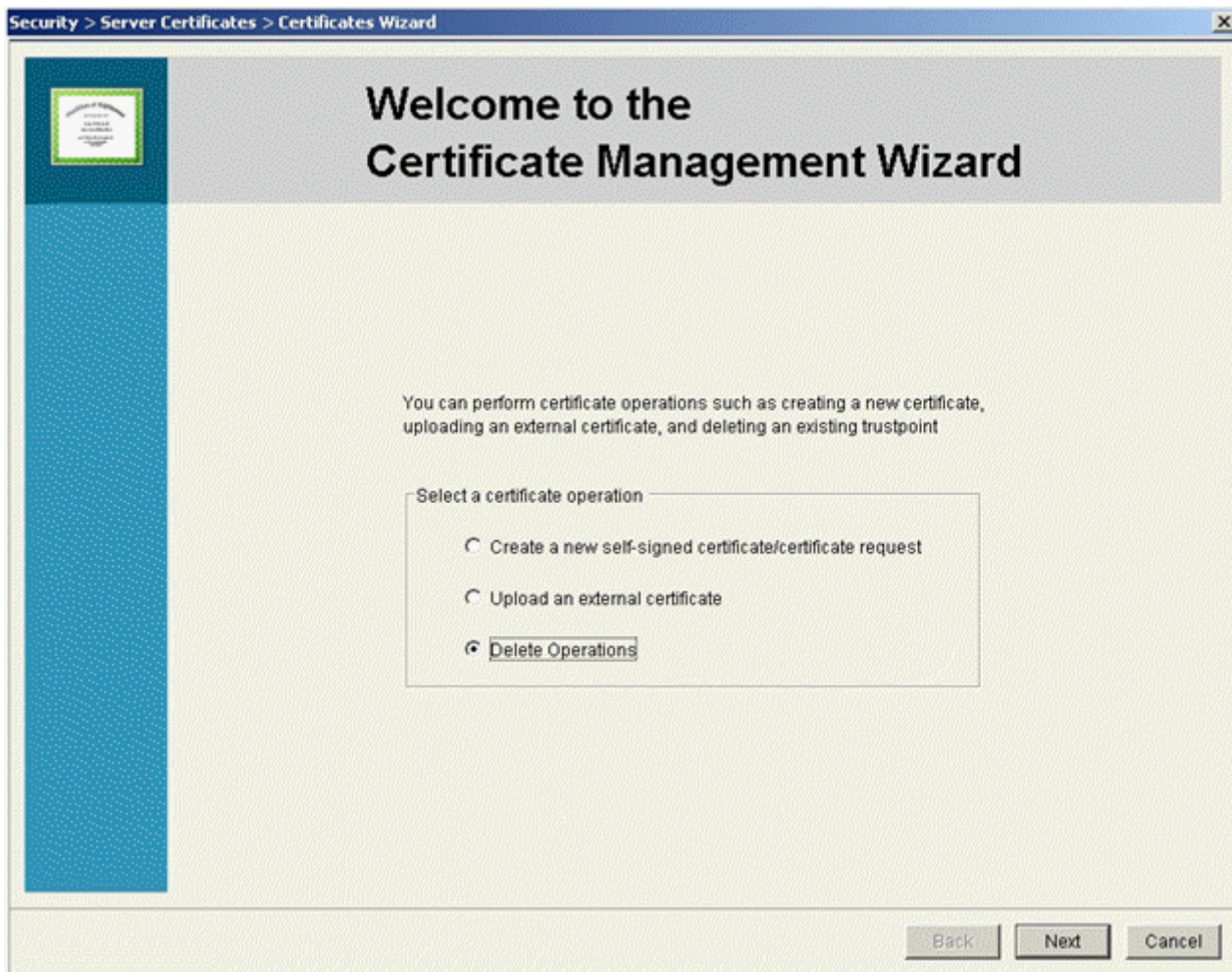
Path Specify the appropriate *Path* name to the target directory on the local system disk or server as configured using the “To” parameter.

11 Click the *Next* button to complete the certificate request.

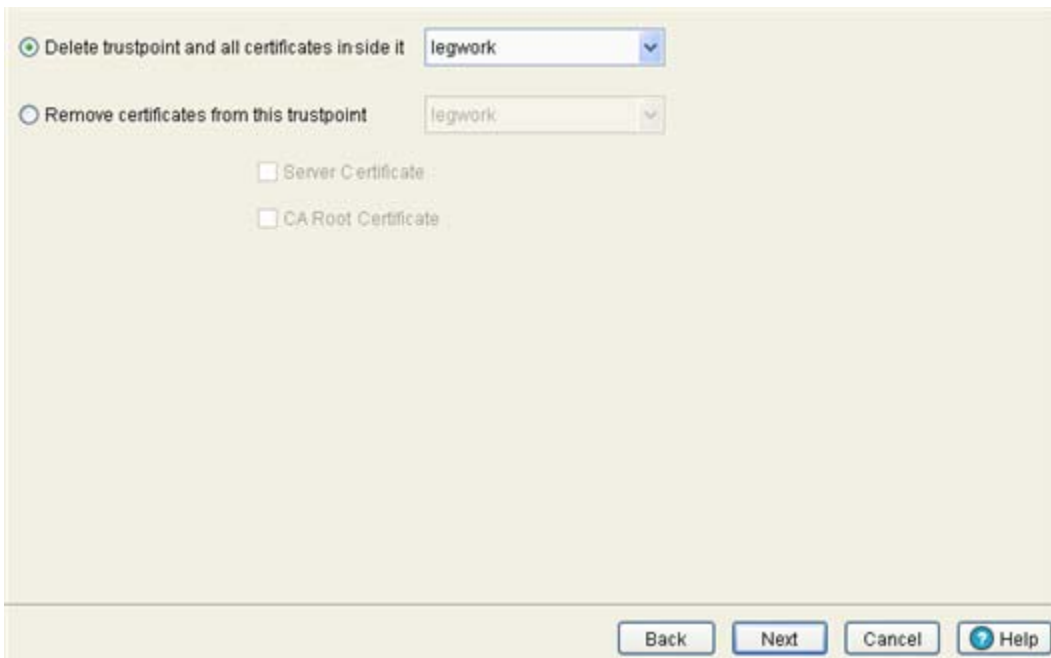
Using the Wizard Delete Operation. The wizard can also be used to delete entire trustpoints, the certificate used with a trustpoint or the CA root certificate use with a trustpoint. Delete trustpoint properties as they become obsolete or the properties of a certificate are no longer relevant to the operation of the controller.

To use the wizard to delete trustpoint properties:

1 Select the *Delete Operations* radio button and click the *Next* button.



The next page of the wizard is used to delete a trustpoint.



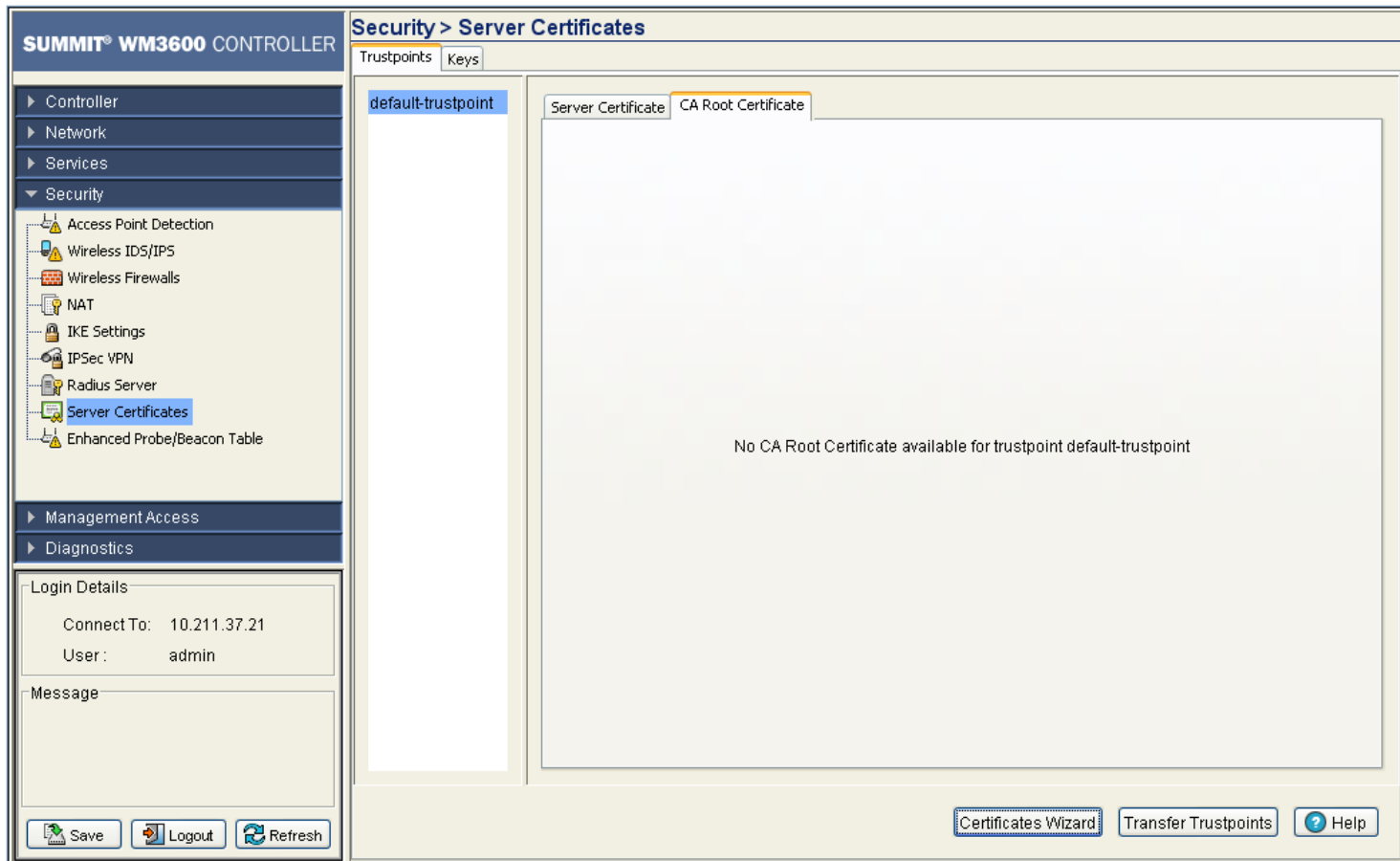
The screenshot shows a wizard dialog box with a light beige background. At the top, there are two radio button options. The first option, "Delete trustpoint and all certificates inside it", is selected and has a dropdown menu showing "legwork". The second option, "Remove certificates from this trustpoint", is unselected and also has a dropdown menu showing "legwork". Below the second option, there are two checkboxes: "Server Certificate" and "CA Root Certificate", both of which are currently unchecked. At the bottom of the dialog, there are four buttons: "Back", "Next", "Cancel", and "Help". The "Next" button is highlighted with a blue border.

- 2 Select and use the *Delete trustpoint and all certificates inside it* drop-down menu to define the target trustpoint for removal.
- 3 Select and use the *Remove certificates from this trustpoint* drop-down menu define the trustpoint that will have either its *Server Certificate* or *CA Root Certificate* removed
- 4 Click the *Next* button to proceed and complete the trustpoint removal.

Certificate Authority Root Certificates

To prepare a certificate request which can be sent to a Certificate Authority (CA):

- 1 Select *Security > Server Certificates* from the main menu tree.
- 2 Click the *CA Root Certificate* tab.



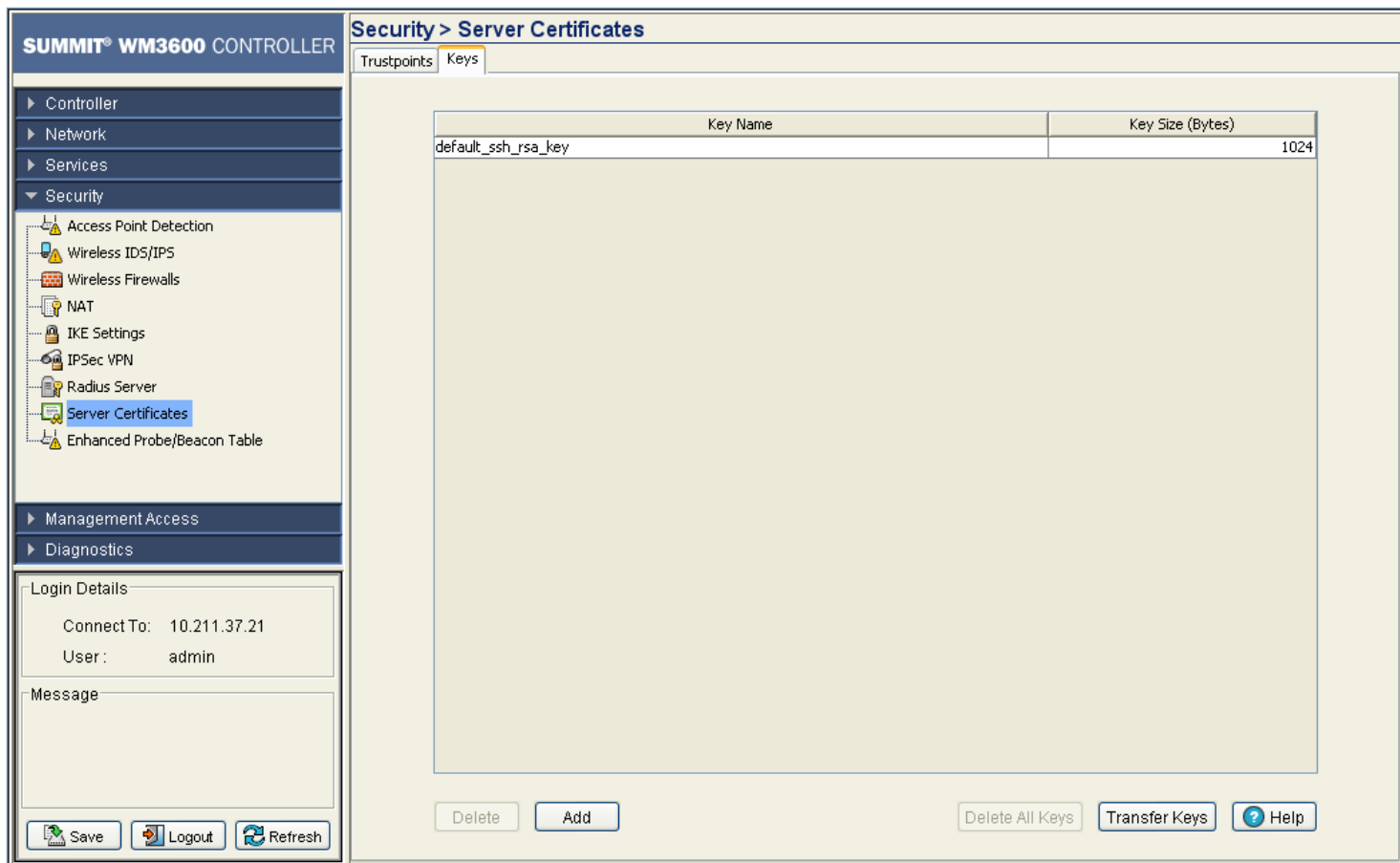
- 3 Follow the instructions in [Using the Wizard to Create a New Certificate](#) on page 513 and [Using the Wizard Delete Operation](#) on page 518.

Configuring Trustpoint Associated Keys

Trustpoint keys allow a user to use different *Rivest*, *Shamir*, an *Adelman* (RSA) key pairs. Therefore, the controller can maintain a different key pair for each certificate to significantly enhance security.

To configure the keys associated with trustpoints:

- 1 Select *Security > Server Certificates* from the main menu tree.
- 2 Select the *Keys* tab.



The Keys tab displays the following:

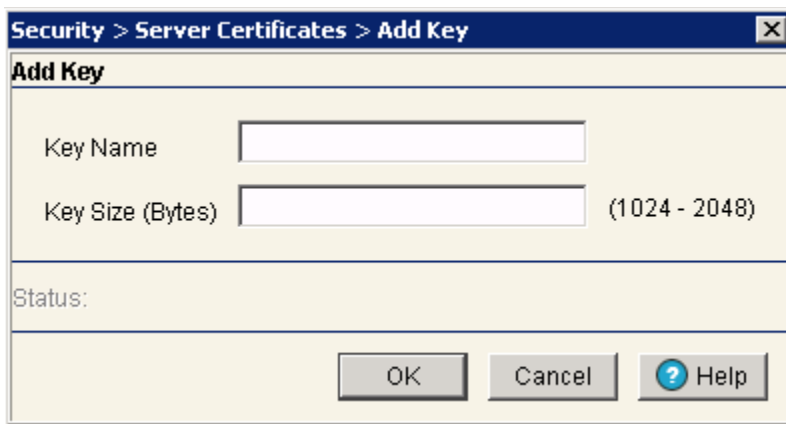
Key Name	Displays the name of the key pair generated separately, or automatically when selecting a certificate. Specify the option within the wizard.
Key Sizes	Displays the size of the desired key. If not specified, a default key size of 1024 is used.

- 3 Highlight a Key from the table and click the *Delete* button to delete it from the controller.
- 4 Click the *Add* button to add a new key label to the list of keys available to the controller. For more information, see [“Adding a New Key” on page 521](#).
- 5 Select the *Delete All Keys* options to delete all of the keys displayed.
- 6 Click *Transfer Keys* to archive the keys to a user-specified location. For more information, see [“Transferring Keys” on page 522](#).

Adding a New Key

If none of the keys listed within the Keys tab are suitable for use with a certificate, consider creating a new key pair.

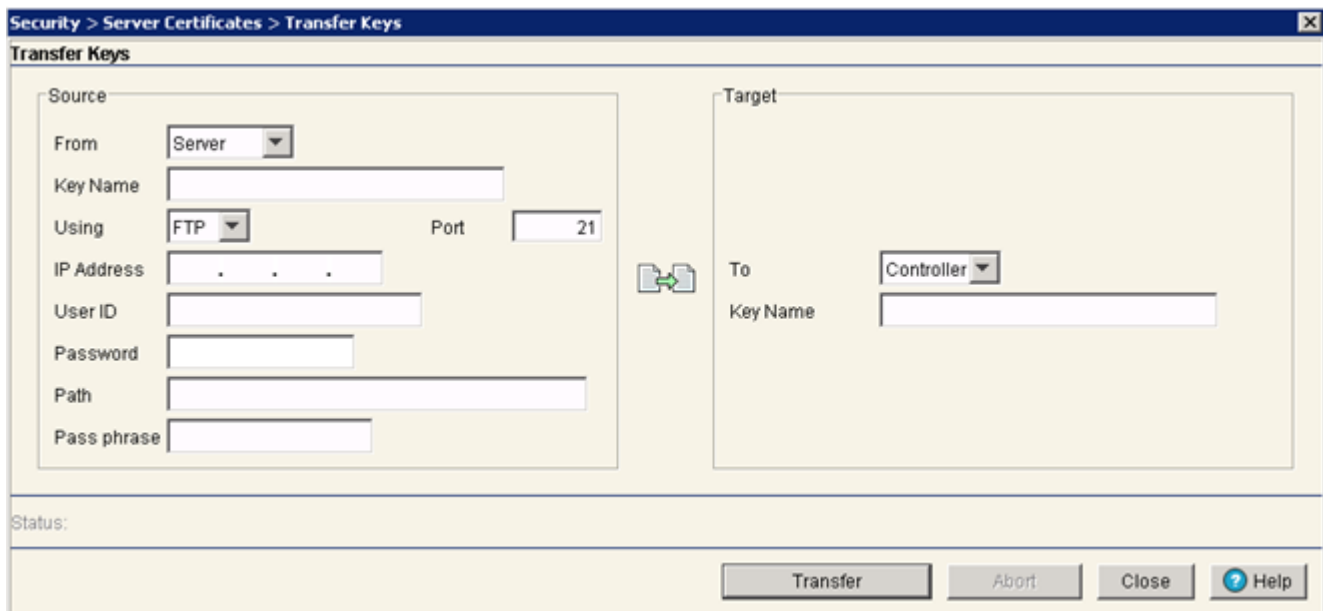
- 1 Select *Security > Server Certificates* from the main menu tree.
- 2 Select the *Keys* tab.
- 3 Click the *Add* button at the bottom of the screen.



- 4 Enter a *Key Label* in the space provided to specify a name for the new key pair.
- 5 Define the *Key Size* between 1024 and 2048 bytes.
- 6 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 7 Click *OK* to save the changes to the running configuration and close the dialog.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Transferring Keys

The *Transfer* screen allows for the transfer of keys to and from the controller to (and from) a server or local disk. Transferring keys is recommended to ensure server certificate key information is available if problems are encountered with the controller and the data needs to be retrieved.



-
- 1 Select *Security > Server Certificate* from the main menu tree.
 - 2 Click the *Keys* Tab.
 - 3 Highlight a target file, and select the *Transfer Keys* button.
 - 4 Use the *From* drop-down menu to specify the location from which the log file is sent. If only the applet is available as a transfer location, use the default controller option.
 - 5 Select a target file for the file transfer from the *File* drop-down menu.
The drop-down menu contains the log files listed within the Server Certificate screen.
 - 6 Use the *To* drop-down menu to define whether the target log file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
 - 7 Provide the name of the file to be transferred to the location specified within the *Target* field.
 - 8 Use the *Using* drop down-menu to configure whether the log file transfer is sent using FTP or TFTP.
 - 9 Enter the *IP Address* of destination server or system receiving the target log file.
 - 10 Enter the *User ID* credentials required to send the file to the target location.
Use the user ID for FTP transfers only.
 - 11 Enter the *Password* required to send the file to the target location using FTP.
 - 12 Specify the appropriate *Path* name to the target directory on the local system disk or server as configured using the "To" parameter.
If the local server option is selected, use the browse button to specify the location on the local server.
 - 13 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
 - 14 Click the *Transfer* button when ready to move the target file to the specified location.
Repeat the process as necessary to move each desired log file to the specified location.
 - 15 Click the *Abort* button to terminate the transfer before completion. The abort option is helpful if certificate credentials prove problematic in the transfer process.
 - 16 Click the *Close* button to exit the screen after a transfer. There are no changes to save or apply.

Configuring Enhanced Beacons and Probes

The controller can be configured to detect and locate rogue APs and MUs. Refer to ["Editing AP Settings" on page 212](#) to enable an AP to forward beacons and association information for AP radios to detect a rogue. An AP can also be configured to forward MU probe requests to the controller to help locate a rogue MU.



NOTE

Currently, only AP4600 Series Access Ports support enhanced beacons and probes request forward configuration.

Use the Enhanced Beacons/Probe screen to configure enhanced beacons/probes and their output reports. The Enhanced Probes and Beacons screens displays four tabs supporting the following configuration activities:

- [Configuring the Beacon Table on page 524](#)
- [Configuring the Probe Table on page 526](#)
- [Reviewing Found Beacons on page 528](#)

- [Reviewing Found Probes on page 529](#)

Configuring the Beacon Table

The Beacon Table is used to detect rogue APs. An AP4600 transmits beacons and MUs send a probe request to the AP for association. The AP4600 (on receipt of the probe request) sends a probe response and forms an AP-MU association.

When enabling an Enhanced Beacon, the controller allows adopted Access Ports to periodically scan for rogue APs on different channels without disassociating MUs. The beacons collected in the scan are passed on to the controller so required information is gathered to locate a particular rogue AP. Refer to [“Editing AP Settings” on page 212](#) to enable an AP to forward beacons and association information for AP radios to detect a rouge.

The controller is provided with a set of 802.11a and 802.11bg radio specific channels. The controller radio scans scan each channel to detect the potential existence or rogues operating on the configured channel. On completion of a scan, the controller moves the AP back to its original channel.

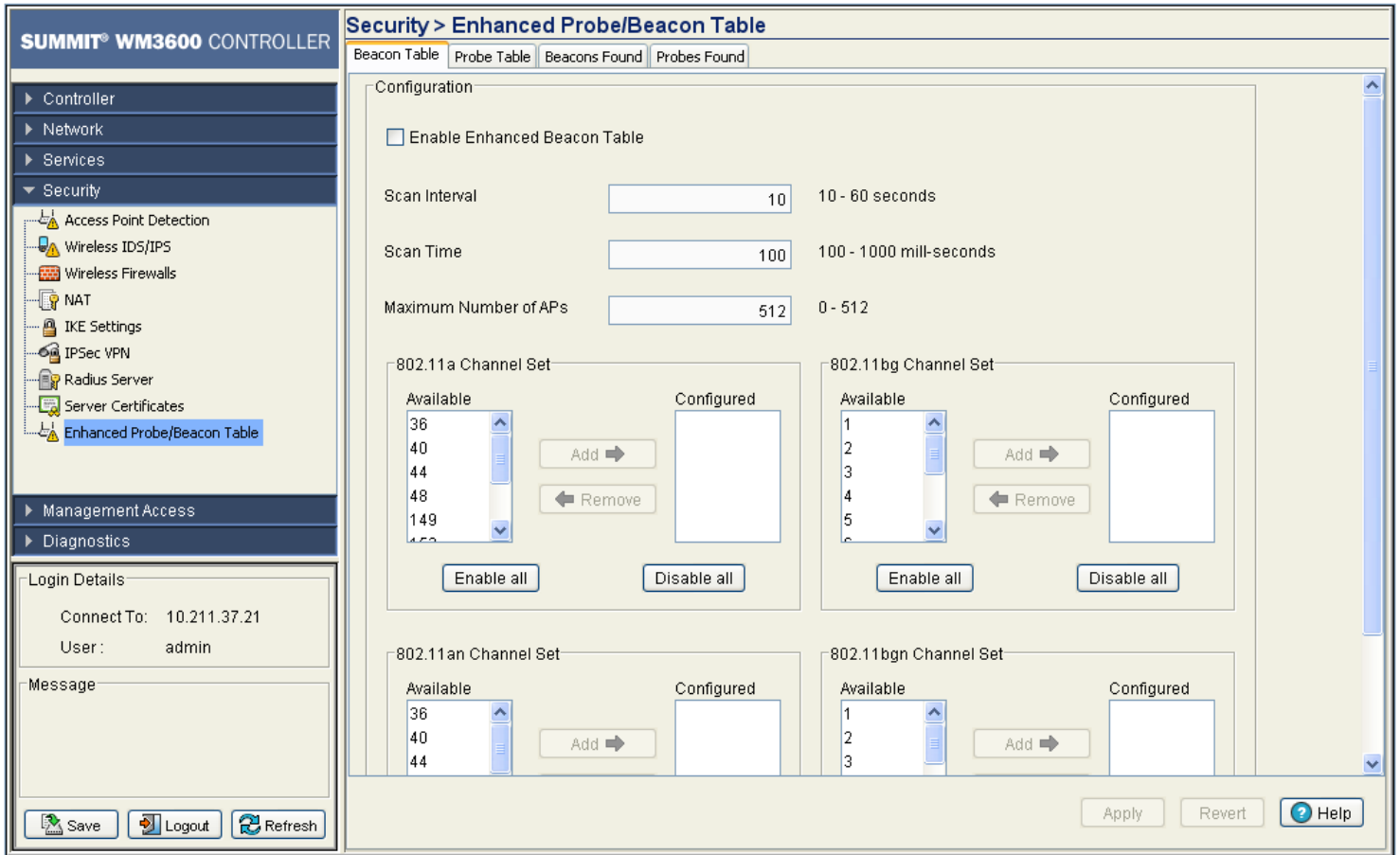
If, during the scan, an AP is detected on a different channel (due to a leaked signal), this channel is also added to the channel set. The AP sends this information to the controller, which maintains a table with the following information:

- MAC address of the detected rogue AP
- AP MAC address
- Signal strength of the detected rogue AP
- Channel on which the AP was detected
- Time when the AP was detected.

This information is used by the Extreme Networks WMS to locate the rogue AP. Extreme Networks WMS uses this information to physically locate the position of rogues and authorized devices within a site map representative of the physical dimensions of the actual device deployment area.

To configure enhanced beacons:

- 1 Select *Security > Enhanced Probe/Beacon Table* from the main menu tree.
- 2 Select the *Beacon Table* tab.



- 3 Select the *Enable Enhanced Beacon Table* checkbox to allow the AP to receive beacons and association information.
- 4 Use *Scan Interval* value to enter the interval used by the radio between scans. The radio scans each channel for the defined interval. The default value is 10 seconds.
- 5 Use the *Scan Time* value to enter the duration of the scan. The radio scans each channel for the defined interval. The default value is 100 milliseconds.
- 6 Define a *Max Number of APs* value to set the number of detected APs displayed in the Beacon Found table. The available range is from 0 to 512.
- 7 Refer to *802.11a Channel Set* field to select channels for the 802.11a transmission band. The channel information is provided to the controller, which then makes an 802.11a radio scan for the configured channels.

Available	Displays the channels available to the AP. The channel list is country specific and differs from country to country.
Add ->	Select a channel frequency and click the <i>Add -></i> button to include the channel to the <i>Configured</i> list box. You can select multiple channels and add them to the <i>Configured</i> list box. Press the Ctrl button and use the mouse to select multiple channels. The controller uses an 802.11a radio to scan the selected channels to detect any rogue APs.

- | | |
|-------------|---|
| <- Remove | Select the channel's frequency from the Configured list box and click <- <i>Remove</i> to remove a channel from the list of channels provided to the controller. |
| Configured | Displays the channels provided to the controller. The controller makes all the 802.11a radios move to the selected channel and scan (one at a time), for a configurable interval. |
| Enable all | Select the <i>Enable all</i> button (within the 802.11a Radios field) to enable all 802.11a radios from receive beacons. |
| Disable all | Select the <i>Disable all</i> button (within the 802.11a Radios field) to disable all 802.11a radios from receiving beacons. |
- 8 Refer to *802.11bg Channel Set* field to select channels for the 802.11bg transmission band. The channel information is provided to the controller, which conducts an 802.11bg scan for each channel.
- | | |
|-------------|---|
| Available | Displays all the channels available to the AP. The channel list is country specific and differs from country to country. |
| Add -> | Select a channel frequency and click the <i>Add -></i> button to include the channel to the <i>Configured</i> list box. Select multiple channels and add them to the <i>Configured</i> list box. Press the Ctrl button and use the mouse to select multiple channels. The controller uses an 802.11a radio to scan the selected channels to detect any non-adopted or rogue APs. |
| <- Remove | Select the channel's frequency from the Configured list box and click <- <i>Remove</i> to remove a channel from the list of channels provided to the controller. |
| Configured | Displays the channels provided to the controller. The controller makes all the 802.11bg radios move to a channel from this channel-set and scan these channels, one at a time, for a configurable duration. |
| Enable all | Select the <i>Enable</i> button (within the 802.11bg Radios field) to enable all the 802.11bg radios receive enhanced beacons. |
| Disable all | Select the <i>Disable</i> button (within the 802.11bg Radios field) to disable all the 802.11bg radios from receiving enhanced beacons. |
- 9 Click *Apply* to save changes to the screen. Navigating away from the screen without clicking the *Apply* button results in changes being discarded.
- 10 Click *Revert* to undo the changes to the screen and revert to the last saved configuration.

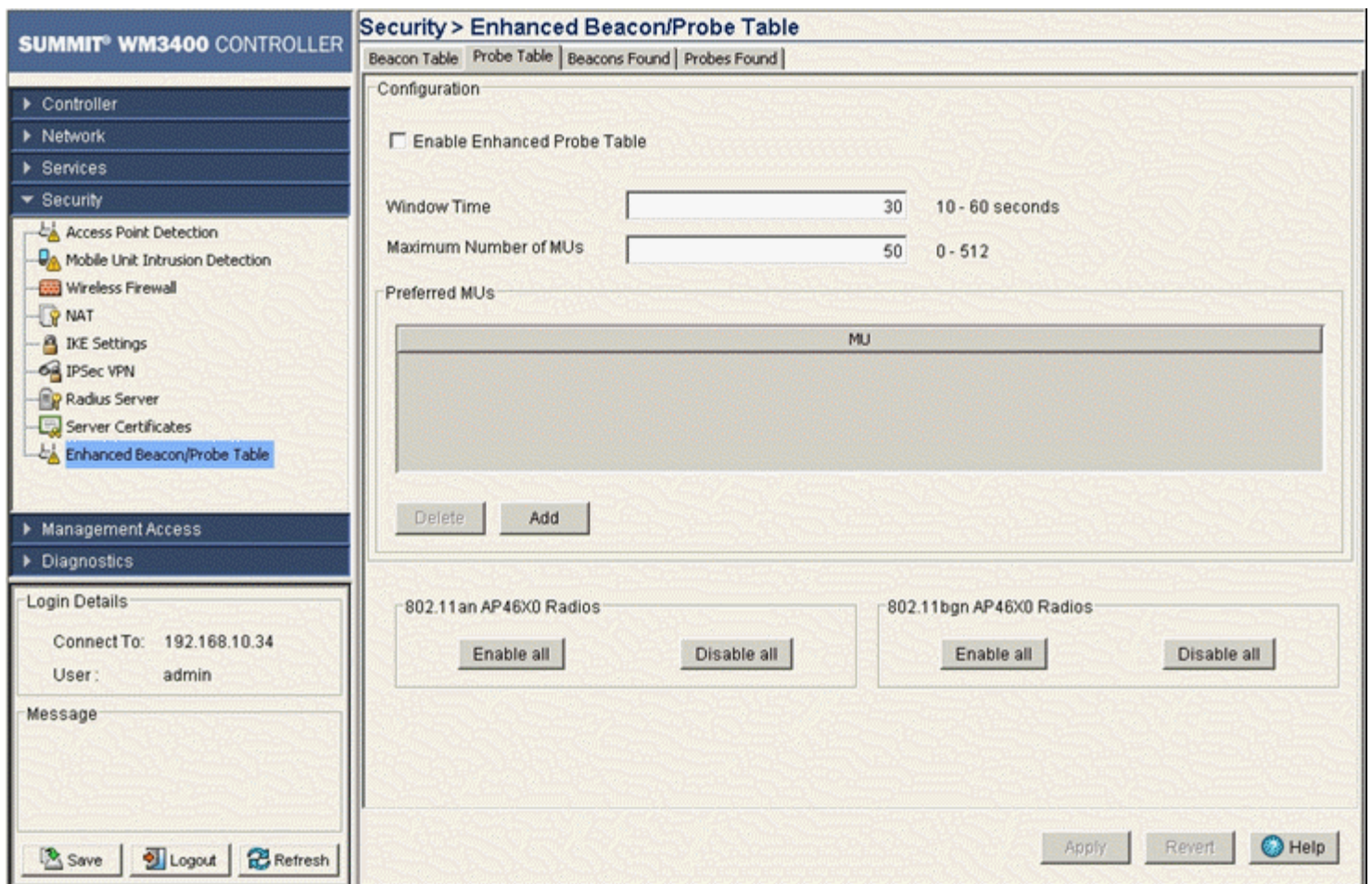
Configuring the Probe Table

Define enhanced probes to detect rogue MUs within the network. An AP4600 transmits beacons and the MUs sends a probe request to the AP for association. An AP4600 (on receipt of the probe request) sends a probe response and associates to the MU.

When using an enhanced probe, an AP4600 sends a probe response to the MU to associate. At the same time, the AP forwards the MU's probe request information to the controller. The controller maintains a table of the probe requests the AP4600 receives from MUs. In conjunction with the Extreme Networks WMS application, the AP locates the rogue MU and displays its location within An Extreme Networks WMS maintained site map.

To configure enhanced beacons:

- 1 Select *Security > Enhanced Probe/Beacon Table* from the main menu tree.
- 2 Select the *Probe Table* tab.



- 3 Select the *Enable Enhanced Probe Table* checkbox to allow an AP to forward MU probe requests to the controller.
- 4 Define a *Window Time* (from 10 to 60 seconds) to set an interval used by the AP to record MU probe requests. The MU radio probe entry with the highest signal strength during the window period is recorded in the table.
- 5 Set a *Maximum Numbers of MUs* (from 0 to 512) to define the number of MUs configured in the controller table. The default is 50 MUs.
- 6 The *Preferred MUs* table lists the MAC Addresses for all preferred MUs.
- 7 Select an MU from the Preferred MUs table and click the *Delete* button to remove the MU from the table.
- 8 Click the *Add* button to open a dialogue and add the MAC Address of a preferred MU to the table.
- 9 *802.11a Radios*: Click the *Enable All* button to allow an AP's 802.11a radio to receive MU probe requests and forward them to the controller.
- 10 *802.11a Radios*: Click the *Disable* button to stop the AP's 802.11a radios from forwarding MU probe requests to the controller.

- 11 *802.11bg Radios*: Click the *Enable* button to allow the AP's 802.11bg radios to receive MU probe requests and forward them to the controller.
- 12 *802.11bg Radios*: Click the *Disable* button to stop the AP's 802.11bg radios from forwarding MU probe requests to the controller.
- 13 Click *Apply* to save any changes. Navigating away from the screen without clicking the *Apply* button results in all the changes on the screen being discarded.
- 14 Click *Revert* to undo the changes to the screen and revert to the last saved configuration.

Reviewing Found Beacons

Select the *Beacons Found* tab to view the enhanced beacons report created by the controller. The table displays beacon information collected during the AP's channel scan. The table contains at least 5 entries for each AP radio (channel) scan. The information displayed within the Beacons Found tab is read-only with no user configurable parameters.

To view the enhanced beacons report:

- 1 Select *Security > Enhanced Probe/Beacon Table* from the main menu tree.
- 2 Select the *Beacons Found* tab.

The screenshot shows the Summit WM3600 Controller web interface. The left sidebar contains a navigation tree with 'Security' expanded to show 'Enhanced Probe/Beacon Table'. The main content area has a breadcrumb 'Security > Enhanced Probe/Beacon Table' and four tabs: 'Beacon Table', 'Probe Table', 'Beacons Found', and 'Probes Found'. The 'Beacons Found' tab is active, displaying a table with the following headers: 'Portal MAC', 'Rogue AP MAC', 'Signal Strength (dBm)', 'Heard Channel', and 'Heard Time'. The table body is currently empty. Below the table is a 'Clear Report' button. At the bottom of the interface are buttons for 'Save', 'Logout', 'Refresh', and 'Help'.

- 3 Refer to the following information as displayed within the *Beacons Found* tab.

Portal MAC	Displays the MAC address of the unadopted AP detected by the enhanced beacon supported AP.
Rogue AP MAC	Displays the MAC address of the enhanced beacon supported AP.
Signal Strength (dBm)	Displays the signal strength when the unadopted AP was detected.
Heard Channel	Displays the channel frequency when the unadopted AP was detected.
Heard Time	Displays the time when the unadopted AP was detected.

- 4 Select the *Clear Report* button to clear the statistic counters and begin a new data calculation.

Reviewing Found Probes

Refer to the *Probes Found* tab to view the enhanced Probe report created by the controller. The table displays probe information collected during the AP's channel scan. The information displayed within the *Probes Found* tab is read-only with no user configurable parameters.

To view the enhanced beacons table report:

- 1 Select *Security > Enhanced Probe/Beacon Table* from the main menu tree.
- 2 Select the *Probes Found* tab.

The screenshot displays the Summit WM3600 Controller web interface. The main content area is titled "Security > Enhanced Probe/Beacon Table" and contains four tabs: "Beacon Table", "Probe Table", "Beacons Found", and "Probes Found". The "Probes Found" tab is selected, showing a table with the following columns: "Portal MAC", "MU MAC", "Signal Strength (dBm)", "Heard Channel", and "Heard Time". The table is currently empty. Below the table is a "Clear Report" button. The left sidebar shows the navigation menu with "Enhanced Probe/Beacon Table" selected. The bottom of the page has "Save", "Logout", and "Refresh" buttons, and a "Help" button in the bottom right corner.

- 3 Refer to the following information as displayed within the *Probes Found* tab.

Portal MAC	Displays the MAC address of the unadopted MU picked detected by the Enhanced Probes enabled AP.
MU MAC	Displays the MAC address of the Enhanced Probe detected MU.
Signal Strength (dBm)	Displays the signal strength when the unadopted MU was detected.
Heard Channel	Displays the channel frequency used when the unadopted MU was detected.
Heard Time	Displays the time the unadopted MU was detected.

- 4 Select the *Clear Report* button to clear the statistic counters and begin a new data calculation.

8

CHAPTER

Controller Management

This chapter describes the Management Access main menu items used to configure the controller. This chapter consists of the following controller management activities:

- [Displaying the Management Access Interface on page 531](#)
- [Configuring Access Control on page 533](#)
- [Configuring SNMP Access on page 535](#)
- [Message Parameters on page 541](#)
- [Configuring SNMP Trap Receivers on page 550](#)
- [Configuring Management Users on page 553](#)



NOTE

HTTPS must be enabled to access the controller applet. Ensure HTTPS access has been enabled before using the login screen to access the controller applet.

Displaying the Management Access Interface

Refer to the main Management Access interface for a high-level overview of the current controller firmware version and the current controller log output configuration. Use this information to discern whether a controller firmware upgrade is required (by checking the website for a newer version) and if the controller is outputting log data appropriately.

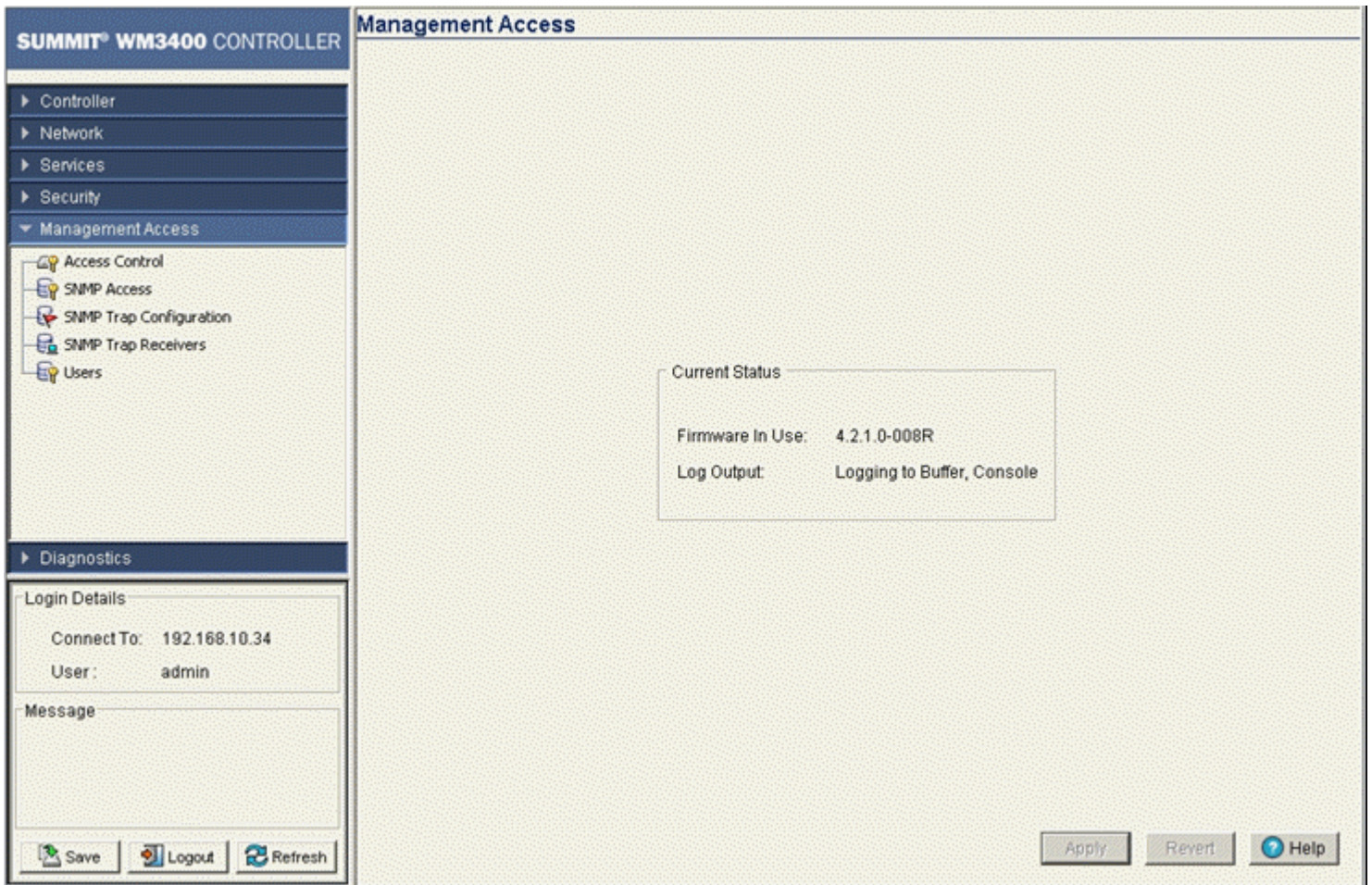


NOTE

When the controller's configuration is successfully updated (using the Web UI), the affected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the affected screen's Status field and the screen remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

To display the main Management screen:

- 1 Select *Management Access* from the main menu tree.



- 2 Refer to the *Current Status* field to review the following read-only information:

Firmware In Use	The <i>Firmware In Use</i> value displays the software version currently running on the controller. Use this information to assess whether a firmware update would improve the controller feature set and functionality.
Log Output	The Log Output value displays the target location for log files output by the controller.



NOTE

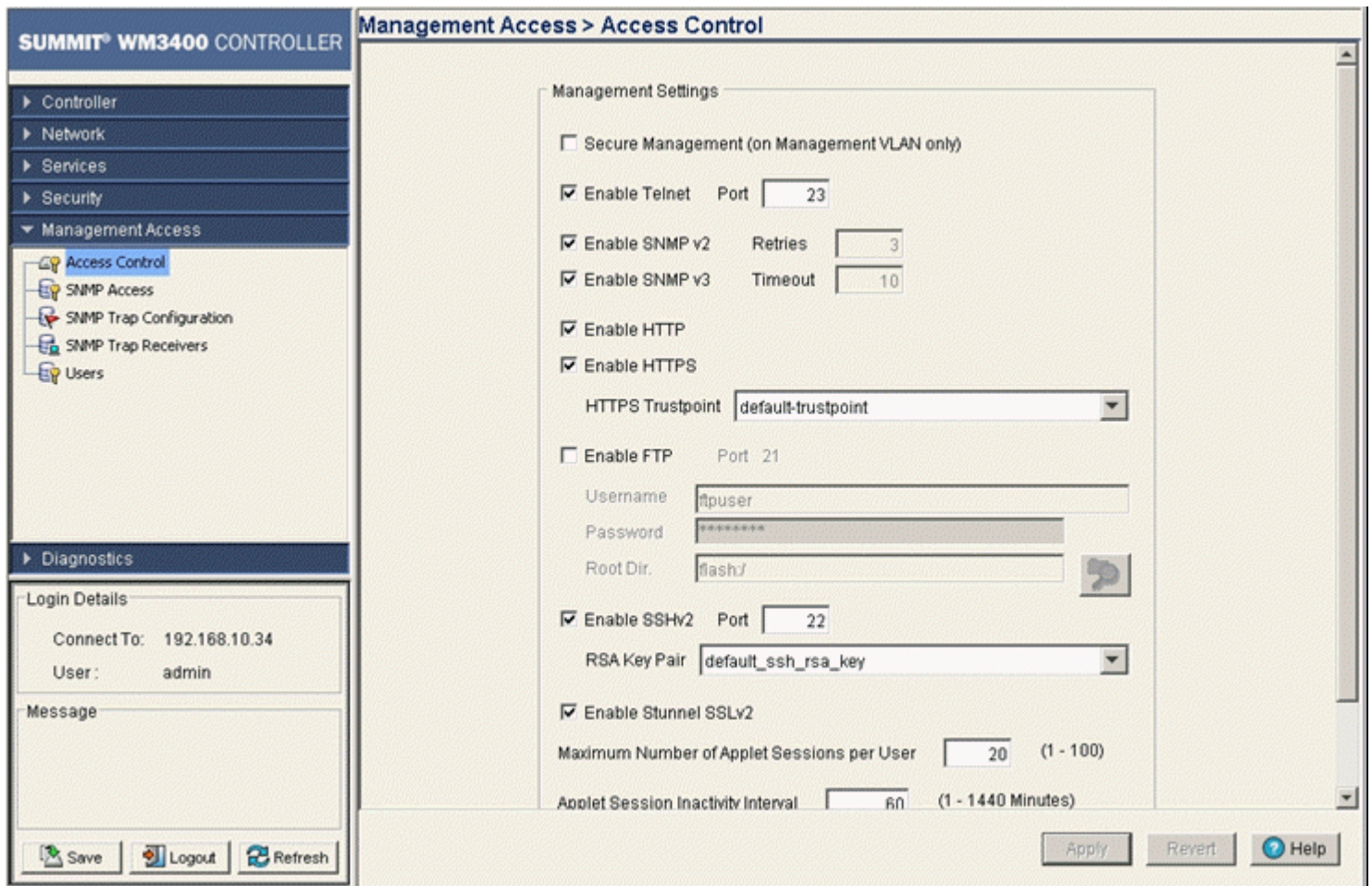
The Apply and Revert functions are grayed out within the Management Access screen, as this screen is has no configurable parameters for the user to update and save.

Configuring Access Control

Refer to the *Access Control* screen to allow/deny management access to the controller using the different protocols (HTTP, HTTPS, Telnet, SSH or SNMP) available to users. Access options are either enabled or disabled as required. The Access Control screen is not meant to function as an ACL (in routers or other firewalls), where you can specify and customize specific IPs to access specific interfaces.

To configure access control settings:

- 1 Select *Management Access > Access Control* from the main menu tree.



- 2 Refer to the *Management Settings* field to enable or disable the following controller interfaces:

Secure Management (on Management VLAN only)	Select this checkbox to allow management VLAN access to controller resources. The management VLAN is used to establish an IP connection to the controller from a workstation connected to a port in the VLAN. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN. Only one management VLAN can be active at a time. This option is disabled (not selected) by default.
Enable Telnet	Select this checkbox to allow the controller to use a Telnet session for communicating over the network. This setting is enabled by default.
Port	Define the port number used for the Telnet session with the controller. This field is enabled as long as the Enable Telnet option remains enabled. The default port is port 23.

Enable SNMP v2	Select this checkbox to enable SNMPv2 access to the controller over the SNMPv2 interface. This setting is enabled by default.
Enable SNMP v3	Select this checkbox to enable SNMPv3 access to the controller over the SNMPv3 interface. This setting is enabled by default.
Retries	Define the number of retries the controller uses to connect to the SNMP interface if the first attempt fails. The default value is 3 retry attempts.
Timeout	When the provided interval is exceeded, the user is logged out of the SNMP session and forced re-initiate their connection. The default value is 10 minutes.
Enable HTTP	Select this checkbox to enable HTTP access to the controller. The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This setting is enabled by default.
Enable HTTPS	Select this checkbox to enable HTTPS access to the controller. This setting is enabled by default.
HTTPS Trustpoint	Use the Trustpoint drop-down menu to select the local or default trustpoint used with a HTTPS session with the controller. For information on creating a new certificate, see “Creating Server Certificates” on page 509 .
Enable FTP	Select this checkbox to enable FTP access to the controller. <i>File Transfer Protocol (FTP)</i> is the language used for file transfers across the Web. This setting is disabled by default.
Port	Displays the port number used for the FTP session with the controller (if using FTP).
Username	Displays the read-only name of the user whose credentials are used for the FTP session.
Password	If FTP is enabled, a password is required (for the user specified in the <i>Username</i> field) to use the controller with the FTP interface.
Root Dir.	Define the root directory where the FTP server is located (if using FTP). Click the Magnifying Glass icon to display a <i>Select Directory File</i> screen useful in selecting the root directory. If necessary a new directory folder can be created.
Enable SSHv2	Select this checkbox to enable SSH version 2 access to the controller. <i>Secure Shell (SSH)</i> is a program designed to perform a number of functions, such as file transfer between computers, command execution or logging on to a computer over a network. It is intended to do these tasks with greater security than programs such as Telnet or FTP. This setting is enabled by default.
Port	Define the port number used for the SSH session with the controller.
RSA Key Pair	Use the <i>RSA Key Pair</i> drop-down menu to select a public/private key pair used for RSA authentication. The default setting is “deflorations”

**NOTE**

You cannot establish an SSH session with the controller when an RSA Key with a length of 360 is associated with the SSH-Server.

- 3 Click the *Apply* button to save changes made to the screen since the last saved configuration.
- 4 Click the *Revert* button to revert the screen back to its last saved configuration. Changes made since the contents of the screen were last applied are discarded.

Configuring SNMP Access

Use the SNMP Access menu to view and configure existing SNMP v1/v2 and SNMP v3 values and their current access control settings. You can also view the SNMP v2/v3 events and their current values. The SNMP Access window consists of the following tabs:

- [Configuring SNMP v1/v2 Access on page 535](#)
- [Configuring SNMP V3 Access on page 537](#)
- [Accessing SNMP v2/v3 Statistics on page 540](#)
- [Message Parameters on page 541](#)



CAUTION

Your system must be running Sun JRE version 1.5.x (or higher) or Mozilla for the controller Web UI to be used with the SNMP interface.



NOTE

The SNMP facility cannot retrieve a configuration file directly from its SNMP interface. First deposit the configuration file to a computer, then FTP the file to the controller.



NOTE

When accessing the controller via a SNMP client ensure that UDP traffic is allowed on port 161 for the network being used for the controller and the SNMP client.

Configuring SNMP v1/v2 Access

SNMP version 2 (SNMPv2) is an evolution of SNMPv1. The Get, GetNext, and Set operations used in SNMPv1 are exactly the same as those used in SNMPv2. However, SNMPv2 adds and enhances some protocol operations. The SNMPv2 Trap operation, for example, serves the same function used in SNMPv1, but uses a different message format and is designed to replace a SNMPv1 Trap.

Refer to the v1/v2c screen for information on existing SNMP v1/v2 community names and their current access control settings. Community names can be modified by selecting a community name and clicking the *Edit* button.



NOTE

The SNMP undo feature is not supported.

To review existing SNMP v1/v2 definitions:

- 1 Select *Management Access > SNMP Access > v1/v2* from the main menu tree.

Community Name	Access Control
public	Read Only
private	Read Write

- 2 Refer to the *Community Name* and *Access Control* parameters for the following information:

- Community Name** Displays the read-only or read-write name used to associate a site-appropriate name for the community. The name is required to match the name used within the remote network management software. Click the *Edit* button to modify an existing Community Name. The string length is <0-11>.
- Access Control** The Access Control field specifies a read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve information, while read/write access allows a remote device to modify settings. Click the *Edit* button to modify an existing Access Control permission.

- 3 Highlight an existing entry and click the *Edit* button to modify the properties of an existing SNMP v1/v2 community and access control definition. For more information, see [“Editing an Existing SNMP v1/v2 Community Name”](#) on page 536.

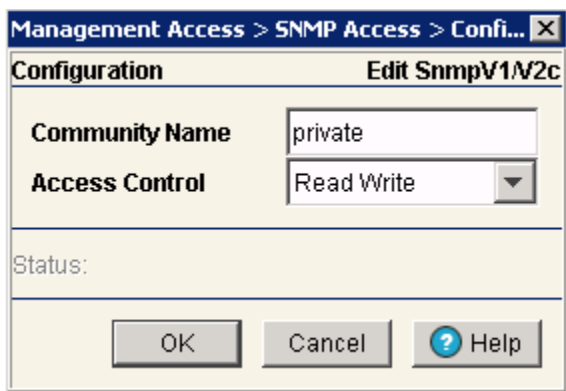
Editing an Existing SNMP v1/v2 Community Name

The *Edit* screen allows the user to modify a community name and change its read-only or read/write designation. Since the community name is required to match the name used within the remote network

management software, it is recommended the name be changed appropriately to match a new naming (and user) requirement used by the management software.

To modify an existing SNMP v1/v2 Community Name and Access Control setting:

- 1 Select *Management Access > SNMP Access > v1/v2* from the main menu tree.
- 2 Select an existing Community Name from those listed and click the *Edit* button.



- 3 Modify the *Community Name* used to associate a site-appropriate name for the community. The name revised from the original entry is required to match the name used within the remote network management software.
- 4 Modify the existing read-only (R) *access* or read/write (RW) *access* for the community. Read-only access allows a remote device to retrieve information, while read/write access allows a remote device to modify settings.
- 5 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 6 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller
- 7 Click *Cancel* to return back to the SNMP v1/v2 screen without implementing changes.

Configuring SNMP V3 Access

SNMP Version 3 (SNMPv3) adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *User-based Security Model (USM)* for message security and the *View-based Access Control Model (VACM)* for access control. The architecture supports the concurrent use of different security, access control, and message processing techniques.

Refer to the *v3* screen to review the current SNMP v3 configuration. An Existing User Name can be selected and edited, enabled or disabled.

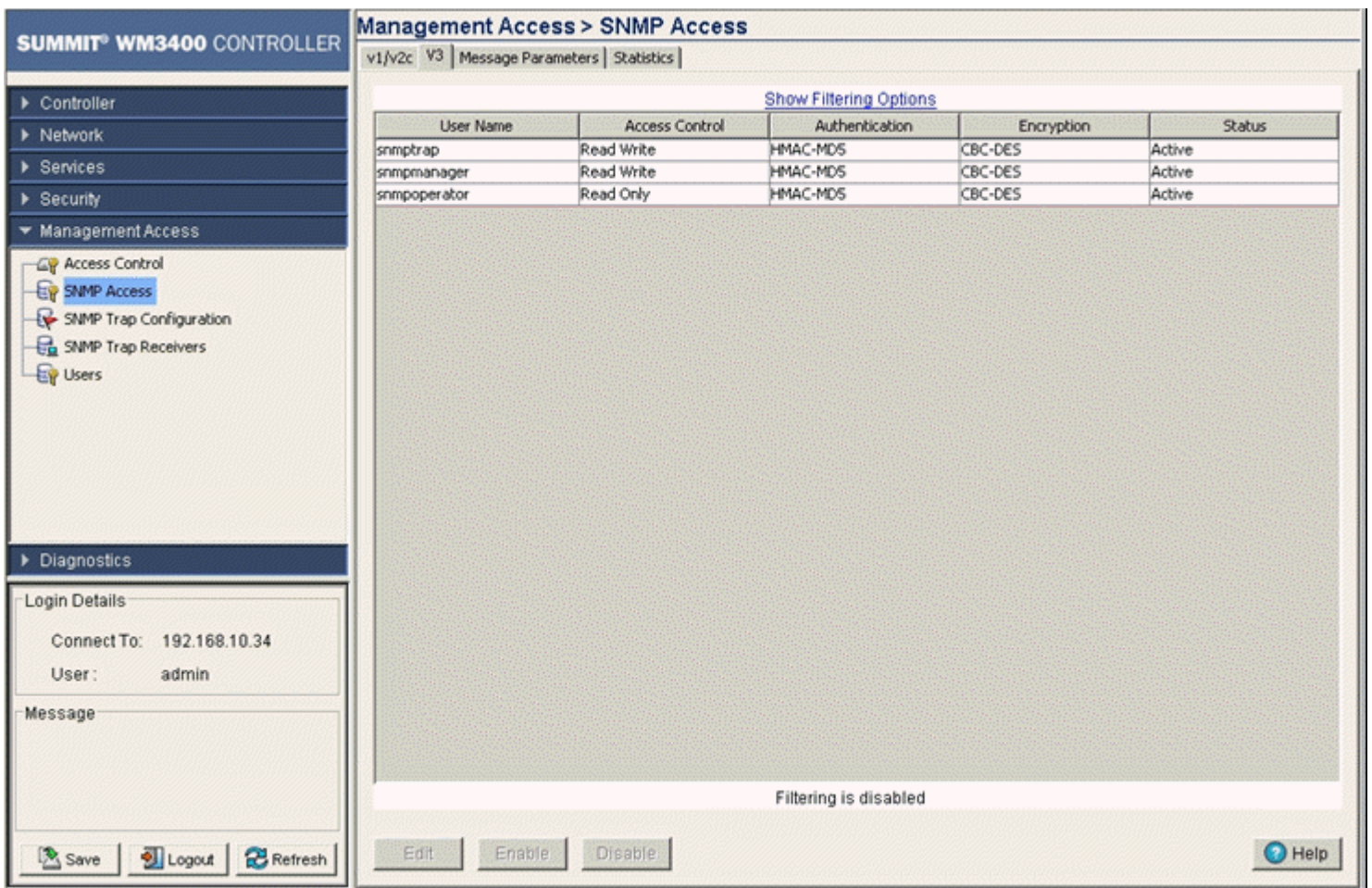


NOTE

The SNMP undo feature is not supported in this product.

To review existing SNMP v3 definitions:

- 1 Select *Management Access > SNMP Access* from the main menu tree.
- 2 Select the *V3* tab from within the SNMP Access screen.



- 3 Refer to the fields within the V3 screen for the following information:

User Name	Displays a read-only SNMP v3 username of operator or Admin. An operator typically has an Access Control of read-only and an Admin typically has an Access Control of read/write. The username string length is <0-3>.
Access Control	Displays a <i>read-only</i> (R) access or <i>read/write</i> (RW) access for the v3 user. Read-only access allows the user (when active) to retrieve information, while read/write access grants the user modification privileges.
Authentication	Displays the current authorization scheme used by this user for v3 access to the controller. Click the <i>Edit</i> button to modify the password required to change authentication keys.
Encryption	Displays the current Encryption Standard (DES) protocol the user must satisfy for SNMP v3 access to the controller. Click the <i>Edit</i> button to modify the password required to change encryption keys.
Status	Displays whether this specific SNMP v3 User Name is active on the controller. For more information, see “Accessing SNMP v2/v3 Statistics” on page 540.

- 4 Highlight an existing v3 entry and click the *Edit* button to modify the password for the Auth Protocol and Priv Protocol.
For additional information, see “Editing an Existing SNMP v1/v2 Community Name” on page 536
- 5 Highlight an existing SNMP v3 User Name and click the *Enable* button to enable the log-in for the specified user. When selected the status of the user is defined as active.
- 6 Highlight an existing SNMP v3 User Name and click the *Disable* button to disable the log-in for the specified user. When selected the status of the user is defined as inactive.

Editing an SNMP v3 Authentication and Privacy Password

The *Edit* screen enables the user to modify the password required to change the authentication keys. Updating the password requires logging off of the system. Updating the existing password creates new authentication and encryption keys. To edit an SNMP v3 user profile:

- 1 Select *Management Access > SNMP Access* from the main menu tree.
- 2 Select the *v3* tab from within the SNMP Access screen.
- 3 Highlight an existing SNMP v3 User Name and click the *Edit* button.

The *Authentication Protocol* is the existing protocol for the User Profile. The *Authentication Protocol* is not an editable option. The *Privacy Protocol* is the existing protocol for the User Profile. The *Privacy Protocol* is also not an editable option.

- 4 Enter the *Old Password* used to grant *Authentication Protocol* and *Privacy Protocol* permissions for the User Profile.
- 5 Enter the *New Password*, then verify the new password within the *Confirm New Password* area.
- 6 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 7 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Accessing SNMP v2/v3 Statistics

Refer to the *Statistics* screen for a read-only overview of SNMP V2/V3 events and their current values. The screen also displays Usm Statistics (SNMP V3 specific events specific to the User-based Security Model) and their values.

To edit an SNMP V3 user profile:

- 1 Select *Management Access > SNMP Access* from the main menu tree.
- 2 Select the *Statistics* tab from within the SNMP Access screen.

SUMMIT® WM3400 CONTROLLER Management Access > SNMP Access

v1/v2c | V3 | Message Parameters | Statistics

V2/V3 Metrics	Values
Total Snmp Packets in	
Total Snmp Packets out	
Total GET Objects requested	
Total SET Objects altered	
Total GET Requests processed	
Total GETNEXT Requests processed	
Total SET Requests processed	
Total GET Responses generated	
Total Traps generated	
Total unsupported SNMP version Errors received	
Total bad community name Errors received	
Total bad community user Errors received	
Total ASN.1 or BER Parse Errors received	
Total Too Big Errors received	
Total No Such Name Errors received	
Total Bad Values Errors received	
Total Read Only Errors received	
Total General Errors received	
Total Too Big Errors generated	
Total No Such Name Errors generated	
Total Bad Values Errors generated	
Total General Errors generated	

Usm Statistics	Values
Total Unsupported Security Levels Errors	
Total Not InTime Windows Errors	
Total Unknown User Names Errors	
Total Unknown Engine ID Errors	
Total Wrong Digests Errors	
Total Decryption Errors	

Login Details
Connect To: 192.168.10.34
User: admin

Message

Save Logout Refresh Help

- 3 Refer to the following read-only statistics displayed within the SNMP Access Statistics screen:

- V2/V3 Metrics** Displays the individual SNMP Access events capable of having a value tracked for them. The metrics range from general SNMP events (such as the number of SNMP packets in and out) to specific error types that can be used for troubleshooting SNMP events (such as Bad Value and Read-Only errors).
- Values** Displays the current numerical value for the SNMP V2/V3 Metric described on the left-hand side of the screen. The value equals the number of times the target event has occurred. This data is helpful in troubleshooting SNMP related problems within the network.

Usm Statistics

Displays SNMP v3 events specific to Usm. The *User-based Security Model (USM)* decrypts incoming messages. The module then verifies authentication data. For outgoing messages, the USM module encrypts PDUs and generates authentication data. The module then passes the PDUs to the message processor, which then invokes the dispatcher.

The USM module's implementation of the SNMP-USER-BASED-SM-MIB enables SNMP to issue commands to manage users and security keys. The MIB also enables the agent to ensure a requesting user exists and has the proper authentication information. When authentication is done, the request is carried out by the agent.

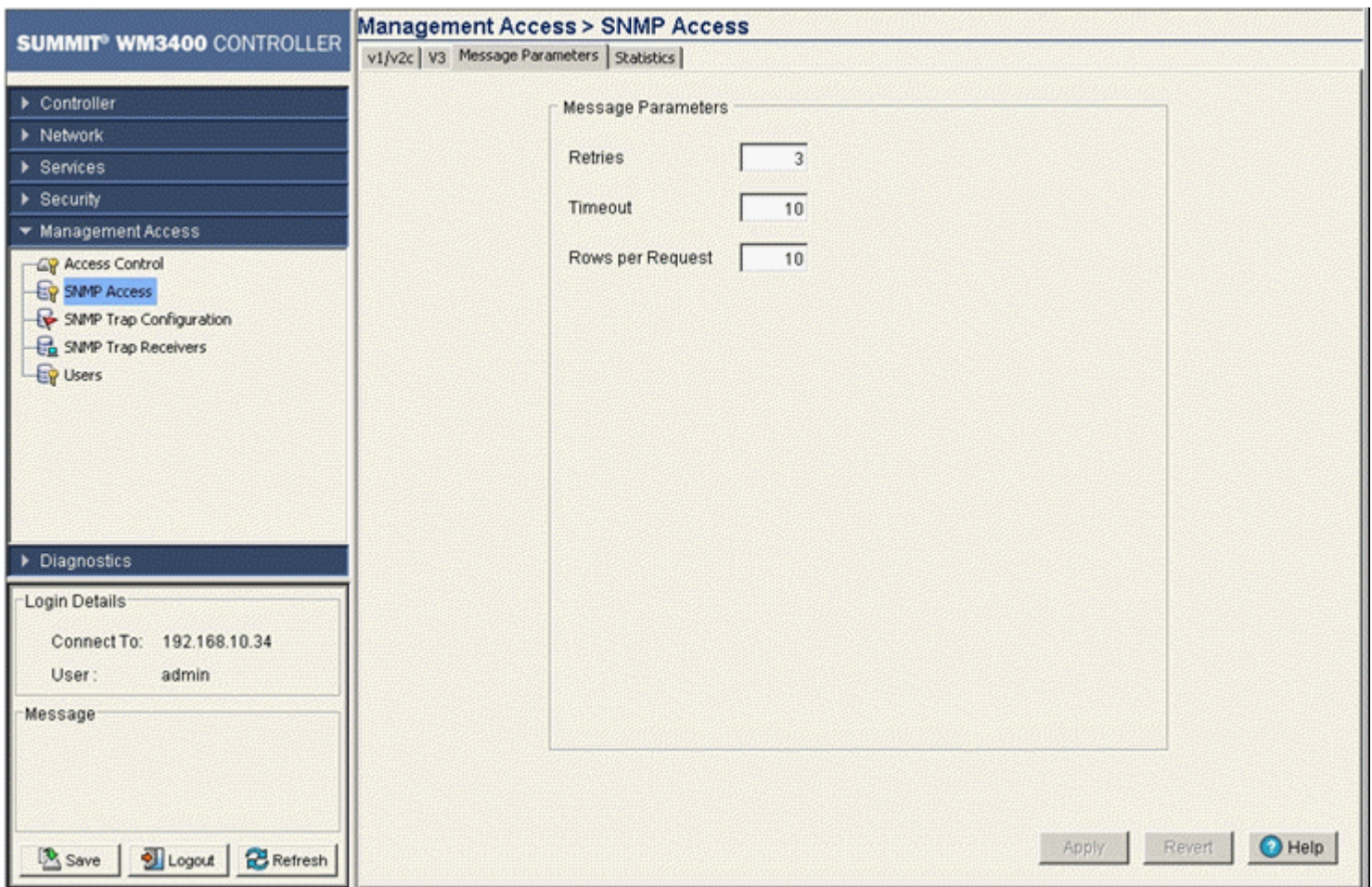
Values

Displays the current numerical value for the Usm Metric described on the left-hand side of the screen. The value equals the number of times the target event occurred. This data is helpful in troubleshooting Usm (Authentication and Encryption) related problems within the network.

Message Parameters

To view Message Parameters:

- 1 Select *Management Access > SNMP Access* from the main menu tree.
- 2 Select the *Message Parameters* tab from within the SNMP Access screen.



3 Refer to the following parameters displayed with in Message Parameters screen.

Retries	Displays the number of retries permitted
Timeout	Displays the timeout in seconds
Rows per Request	Displays the number of rows per request

4 The *Apply* and *Revert* buttons are grayed out within this screen, as there is no data to be configured or saved.

5 Highlight an existing message parameter and edit the value. Click the *Apply* button to save the changes made.

6 Highlight an existing message parameter and click the *Revert* button to remove the changes made.

Configuring SNMP Traps

Use the SNMP Trap Configuration screen to enable or disable individual traps or by functional trap groups. It is also used for modifying the existing threshold conditions values for individual trap descriptions. Refer to the tabs within the SNMP Trap Configuration screen to conduct the following configuration activities:

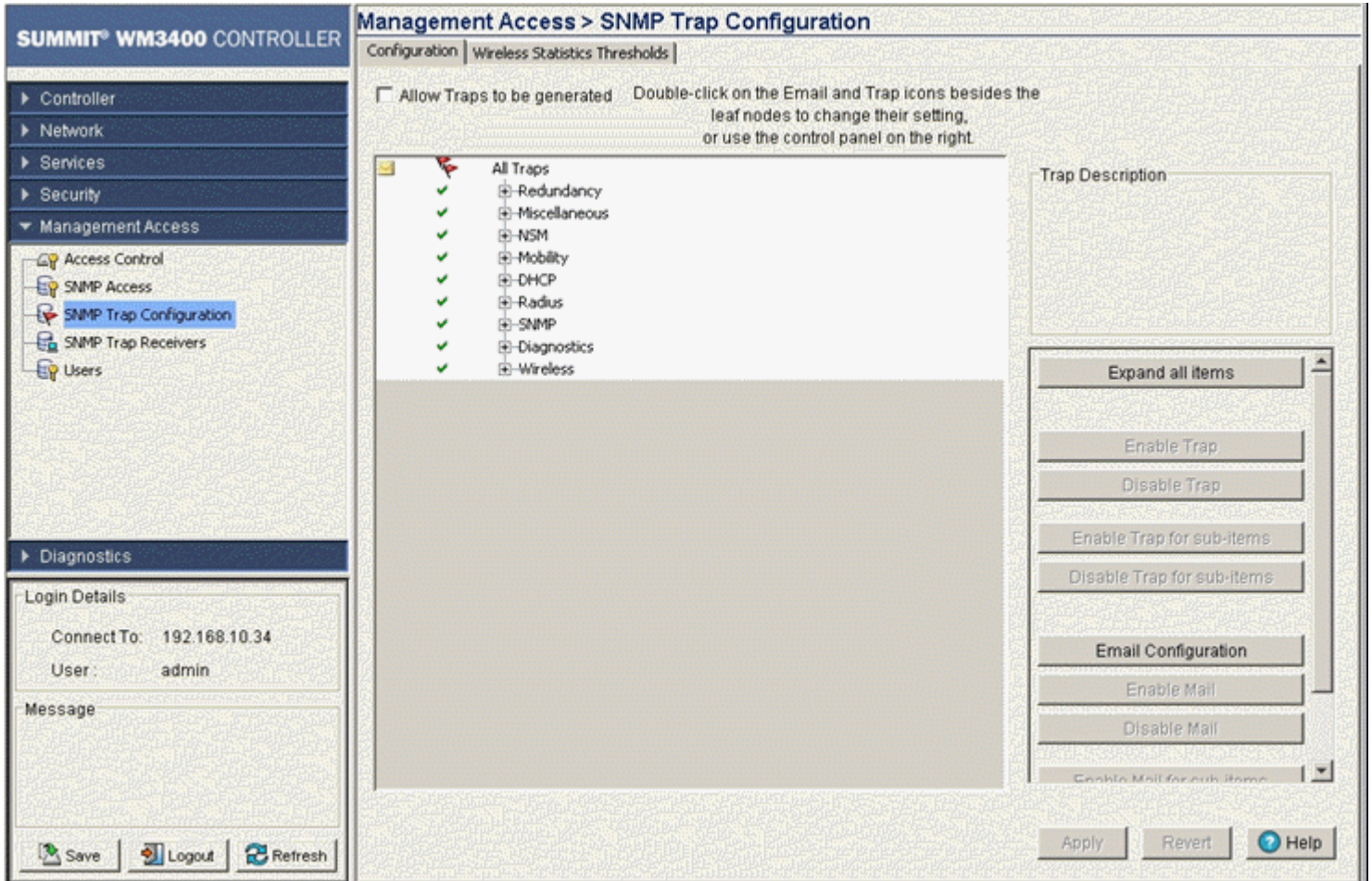
- [Enabling Trap Configuration on page 542](#)
- [Configuring Trap Thresholds on page 546](#)

Enabling Trap Configuration

If unsure whether to enable a specific trap, select it and view a brief description that may help your decision. Use *Expand all items* to explode each trap category and view all the traps that can be enabled. Traps can either be enabled by group or as individual traps within each parent category.

To configure SNMP trap definitions:

- 1 Select *Management Access > SNMP Trap Configuration* from the main menu tree.



- 2 Select the *Allow Traps to be generated* checkbox to enable the selection (and employment) of all the traps within the screen. Leaving the checkbox unselected means traps must be enabled by category or individually.
- 3 Refer to trap categories within the Configuration screen to determine whether traps should be enabled by group or individually enabled within parent groups.
- 4 Select an individual trap, by expanding the node in the tree view, to view a high-level description of this specific trap within the *Trap Description* field. You can also select a trap family category heading (such as “Redundancy” or “NSM”) to view a high-level description of the traps within that trap category.

Redundancy	Displays a list of sub-items (trap options) specific to the Redundancy (clustering) configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the Cluster category.
Miscellaneous	Displays a list of sub-items (trap options) specific to the Miscellaneous configuration option (traps that do not fit in any other existing category). Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the Miscellaneous trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the Miscellaneous category.

NSM	Displays a list of sub-items (trap options) specific to the NSM configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the NSM trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the NSM category.
Mobility	Displays a list of sub-items (trap options) specific to the Mobility configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the Mobility trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the Mobility category.
DHCP	Displays a list of sub-items (trap options) specific to the DHCP configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the DHCP trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the DHCP category.
Radius	Displays a list of sub-items (trap options) specific to the RADIUS configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the RADIUS trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the RADIUS category.
SNMP	Displays a list of sub-items (trap options) specific to the SNMP configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the SNMP trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the SNMP category.
Diagnostics	Displays a list of sub-items (trap options) specific to the Diagnostics configuration option. Select an individual trap within this subsection and click the <i>Enable</i> button to enable this specific trap or highlight the Diagnostics trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the Diagnostics category.
Wireless	Displays the list of sub-items (trap options) specific to Wireless configuration. These include traps specific to wireless interoperability between the controller and its associated devices. Select an individual trap and click the <i>Enable</i> button to enable a specific trap or highlight the Wireless trap family parent item and click <i>Enable all sub-items</i> to enable all traps within the Wireless category.

- Click the *Expand All Items* button to display the sub-items within each trap category. Use this item to display every trap that can be enabled.

Once expanded, traps can then be enabled by trap category or individually within each trap category.

- Highlight a specific trap and click the *Enable* button to enable this specific trap as an active SNMP trap.

The items previously disabled (with an "X" to the left) now display with a check to the left of it.

- Highlight a specific trap and click the *Disable* button to disable the item as an active SNMP trap.

The items previously enabled (with a check to the left) now display with an "X" to the left of it.

- Highlight a sub-menu header (such as Redundancy or Update Server) and click the *Enable all sub-items* button to enable the item as an active SNMP trap.

Those sub-items previously disabled (with an "X" to the left) now display with a check to the left of them. Once the *Apply* button is clicked, the selected items are now active SNMP traps on the system.

- Highlight a sub-menu header (such as Redundancy or SNMP) and click the *Disable all sub-items* button to disable the item as an active SNMP trap.

Those sub-items previously enabled (with a check to the left) now display with an "X" to the left of them.

- 10 Click *Apply* to save the trap configurations enabled using the Enable or Enable all sub-items options.
- 11 Click *Revert* to discard any updates and revert back to its last saved configuration.

Configuring Email Notifications

To enable email notification:

- 1 Select *Management Access > SNMP Trap Configuration* from the main menu tree.
- 2 Click the *Email Configuration* button to launch a dialogue where you can configure outgoing email servers and addresses for alerts.

- 3 Check the *Enable SMTP* box to enable the outgoing mail server on the controller. In order to use email notification on the controller, this box must be checked.

Configure the SMTP mail server properties as follows:

Name	Enter the hostname of your outgoing SMTP mail server. This is the server that is used to deliver outgoing mail.
Port	Specify the port number used by your outgoing SMTP server. In many cases this is port 25.
User Name	Enter the username for the user which will be sending outgoing mail through the SMTP server.
Password	Enter the password associated with the above username.
Enable Authentication	Check the Enable Authentication box to enable support for SMTP Authentication which is required for certain outgoing SMTP servers.

4 Configure the mail-to section of the page as follows:

To Address(es)	Specify an email address or addresses that notifications will be sent to. To add an email address to the list, enter the email address in the To Address(es) field and click the Add button. There is a maximum of 4 email addresses allowed on the list.
Add	Click the Add button to add an email address that is in the To Address(es) field to the list below.
Remove	Select an email address from the list and click the Remove button to delete that address from the list.
From Address	Enter an email address that will serve as the From address for the notifications sent by the controller.
Subject Prefix	Enter a short subject line that will prepend the subject line in each outgoing notification email.

5 Click *OK* to save and add the changes to the running configuration and close the dialog.

6 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Trap Thresholds

Use the *Wireless Statistics Thresholds* screen to modify existing threshold conditions values for individual trap descriptions. Refer to the greater than, less than and worse than conditions to interpret how the values should be defined. Additionally, the Unit of Threshold Values increment should be referenced to interpret the unit of measurement used.

To configure SNMP trap threshold values:

- 1 Select *Management Access > SNMP Trap Configuration* from the main menu tree.
- 2 Click the *Wireless Statistics Thresholds* tab.

Management Access > SNMP Trap Configuration

Configuration Wireless Statistics Thresholds

To edit threshold values, please click inside the corresponding cell.

Threshold Name (Description)	Threshold Conditions	Threshold Values for				Unit of Threshold Values
		MU	AP	WLAN	Controller	
Packets Per Second	greater than	0	0	0	0	Pps
Throughput	greater than	0	0	0	0	Mbps
Average Bit Speed	less than	0	0	0	0	Mbps
Average MU Signal	worse than	0	0	0	0	dBm
Non-Unicast Packets	greater than	0	0	0	0	%
Transmitted Packet Dropped	greater than	0	0	0	0	%
Transmitted Packet Average Retries	greater than	0	0	0	0	Retries
Undecrypt Received Packets	greater than	0	0	0	0	%
Total MUs	greater than		0	0	0	
Average Noise Level	worse than			0		dBm

Minimum Packets

Minimum number of packets required to send a trap (1-65535)

- 3 Refer to the following information for thresholds descriptions, conditions, editable threshold values and units of measurement.

Threshold Name (Description)	Displays the target metric for the data displayed to the right of the item. It defines a performance criteria used as a target for trap configuration.
Threshold Conditions	Displays the criteria used for generating a trap for the specific event. The Threshold conditions appear as greater than, less than or worse than and define a baseline for trap generation.
Threshold values for: MU	Displays a threshold value for associated MUs. Use the <i>Threshold Name</i> and <i>Threshold Conditions</i> as input criteria to define an appropriate Threshold Value unique to the MUs within the network. For information on specific values, see “Wireless Trap Threshold Values” on page 549 .
Threshold values for: AP	Set a threshold value for adopted APs. Use the <i>Threshold Name</i> and <i>Threshold Conditions</i> as input criteria to define an appropriate Threshold Value unique to the APs within the network. For information on specific values, see “Wireless Trap Threshold Values” on page 549 .
Threshold values for: WLAN	Use the <i>Threshold Name</i> and <i>Threshold Conditions</i> as input criteria to define an appropriate Threshold Value unique to the controller. For information on specific values, see “Wireless Trap Threshold Values” on page 549 .

Threshold values for: Controller	Use the <i>Threshold Name</i> and <i>Threshold Conditions</i> as input criteria to define an appropriate Threshold Value unique to the controller. For information on specific values, see “Wireless Trap Threshold Values” on page 549 .
Unit of Threshold Values	Displays the measurement value used to define whether a threshold value has been exceeded. Typical values include Mbps, retries and %. For information on specific values, see “Wireless Trap Threshold Values” on page 549 .

- 4 Select a threshold and click the *Edit* button to display a screen wherein threshold settings for the MU, AP and WLAN can be modified.

EDIT		Throughput
Throughput (Mbps)		greater than
MU	<input type="text" value="0.0"/>	(0.0 - 100000.0)
AP	<input type="text" value="0.0"/>	(0.0 - 100000.0)
WLAN	<input type="text" value="0.0"/>	(0.0 - 100000.0)
Controller	<input type="text" value="0.0"/>	(0.0 - 100000.0)

Status:

OK Cancel ? Help

Adjust the values as needed (between 0 -100) to initiate a trap when the value is exceeded for the MU, AP or WLAN. Ensure the value set is realistic, in respect to the number of MUs and APs supporting WLANs within the controller managed network.

- 5 Use the *Maximum Number of Packets to Send a Trap* field (at the bottom of the screen) to enter a value used as the minimum number of data packets required for a trap to be generated for a target event. Ensure the value is realistic, as setting it to low could generate traps unnecessarily. Refer to [“Wireless Trap Threshold Values” on page 549](#) for additional information.
- 6 Click the *Apply* button to save changes made to the screen since the last saved configuration.
- 7 Click the *Revert* button to revert the screen back to its last saved configuration. Changes made since the contents of the screen were last applied are discarded.

Wireless Trap Threshold Values

Table 4 lists the Wireless Trap threshold values for the controller.

Table 4: Wireless Trap Threshold Values

	Threshold Name	Condition	Station Range	Radio Range	WLAN Range	Wireless Service Range	
1	Packets per Second	Greater than	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	Pps
2	Throughput	Greater than	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	A decimal number greater than 0.00 and less than or equal to 100000.00	Mbps
3	Average Bit Speed	Less than	A decimal number greater than 0.00 and less than or equal to 54.00	A decimal number greater than 0.00 and less than or equal to 54.00	A decimal number greater than 0.00 and less than or equal to 54.00	N/A	Mbps
4	Average MU Signal	Worse than	A decimal number less than -0.00 and greater than or equal to -120.00	A decimal number less than -0.00 and greater than or equal to -120.00	A decimal number less than -0.00 and greater than or equal to -120.00	N/A	dBm
5	Non Unicast Packets	Greater than	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	N/A	%
6	Transmitted Packet dropped	Greater than	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	N/A	%

Table 4: Wireless Trap Threshold Values (Continued)

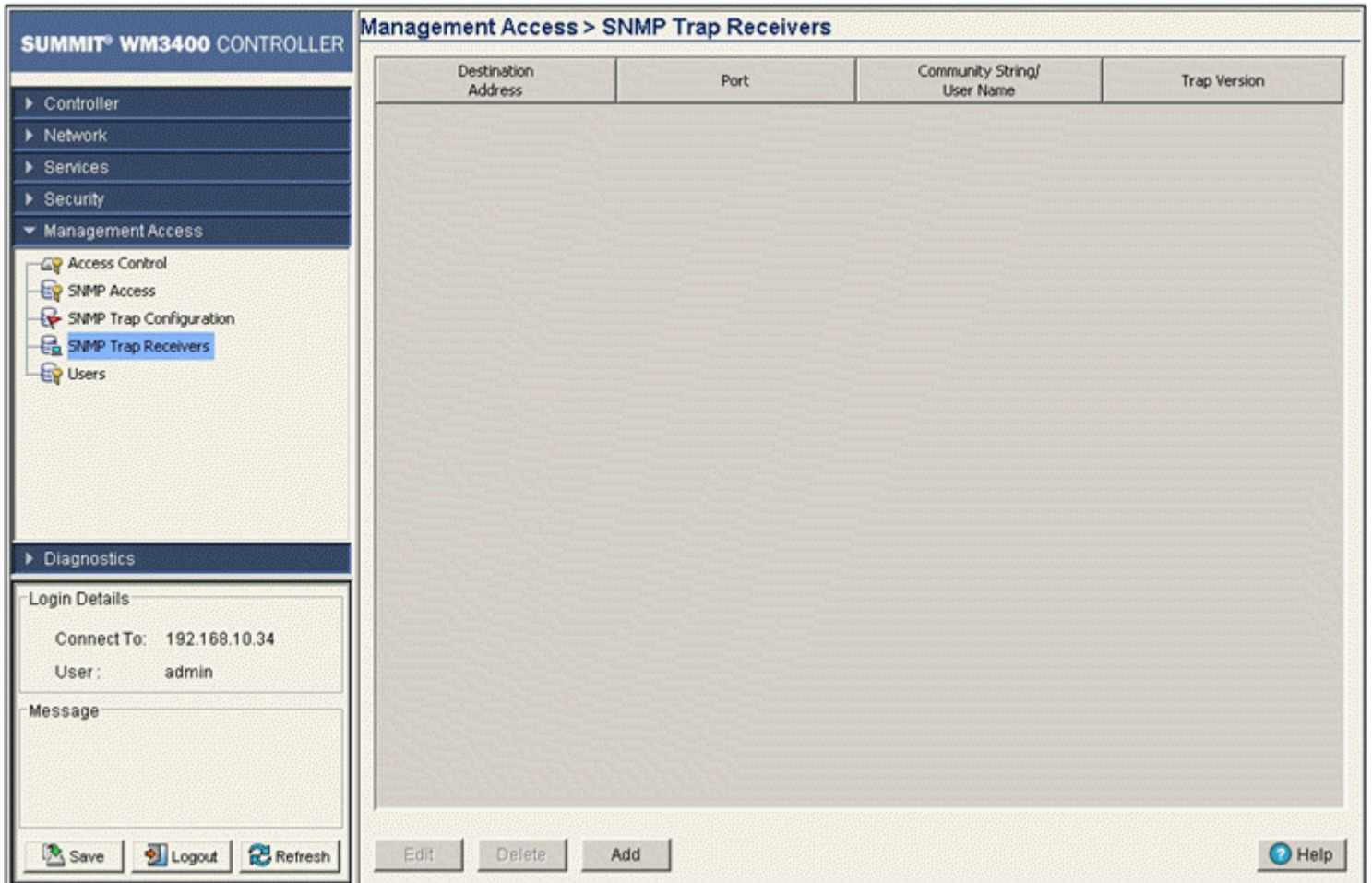
	Threshold Name	Condition	Station Range	Radio Range	WLAN Range	Wireless Service Range	
7	Transmitted Packet Average retries	Greater than	A decimal number greater than 0.00 and less than or equal to 16.00	A decimal number greater than 0.00 and less than or equal to 16.00	A decimal number greater than 0.00 and less than or equal to 16.00	N/A	Retries
8	Undecrypted received packets	Greater than	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	A decimal number greater than 0.00 and less than or equal to 100.00	N/A	%
9	Total MUs	Greater than	N/A	N/A A decimal N/A in the range <1-1000>	N/A A decimal N/A in the range <1-1000>	A decimal number in the range <1-1000>	Count

Configuring SNMP Trap Receivers

Refer to the *Trap Receivers* screen to review the attributes of existing SNMP trap receivers (including destination address, port, community and trap version). A new v2c or v3 trap receiver can be added to the existing list by clicking the *Add* button.

To configure the attributes of SNMP trap receivers:

- 1 Select *Management Access > SNMP Trap Receivers* from the main menu tree.



- 2 Refer to the following SNMP trap receiver data to assess whether modifications are required.

Destination Address	Defines the numerical (non DNS name) destination IP address for receiving traps sent by the SNMP agent.
Port	Specifies a destination User Datagram Protocol (UDP) receiving traps.
Community String/ User Name	Displays the Community String and User Name specific to the SNMP-capable client that receives the traps. The community name is public.
Trap Version	Defines the trap version (v1/2 or v3) defined by the SNMP-capable client receiving the trap. A trap designation cannot be modified.

- 3 Highlight an existing Trap Receiver and click the *Edit* button to display a sub-screen used to modify the v2c or v3 Trap Receiver.

Edit Trap Receivers as needed if existing trap receiver information is insufficient. You can only modify the IP address, port and v2c or v3 trap designation within the Edit screen. For more information, see [“Editing SNMP Trap Receivers” on page 552](#).

- 4 Highlight an existing Trap Receiver and click the *Delete* button to remove the Trap Receiver from the list of available destinations available to receive SNMP trap information.

Remove Trap Receivers as needed if the destination address information is no longer available on the system.

- Click the *Add* button to display a sub-screen used to assign a new Trap Receiver IP Address, Port Number and v2c or v3 designation to the new trap.

Add trap receivers as needed if the existing trap receiver information is insufficient. For more information, see [“Adding SNMP Trap Receivers” on page 552](#).

Editing SNMP Trap Receivers

Use the *Edit* screen to modify the trap receiver’s IP Address, Port Number and v2c or v3 designation. Consider adding a new receiver before editing an existing one or risk overwriting a valid receiver. Edit existing destination trap receivers as required to suit the various traps enabled and their function in supporting the controller managed network.

To edit an existing SNMP trap receiver:

- Select *Management Access > SNMP Trap Receivers* from the main menu tree.
- Select (highlight) an existing SNMP trap receiver and click the *Edit* button.

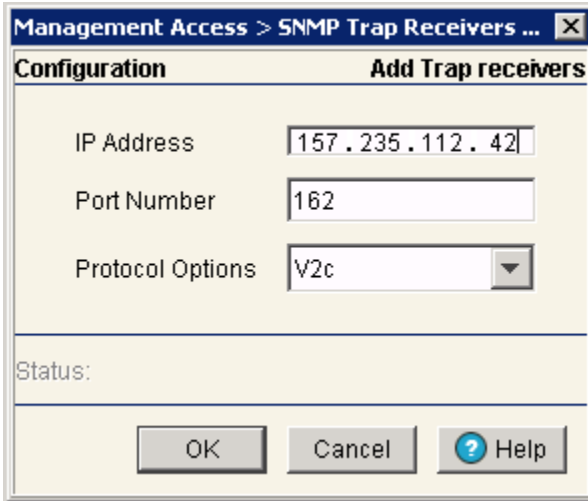
- Modify the existing IP address if it is no longer a valid address.
If it is still a valid IP address, consider clicking the *Add* button from within the SNMP Trap Receivers screen to add a new address without overwriting this existing one.
- Define a *Port Number* for the trap receiver.
- Use the *Protocol Options* drop-down menu to specify the trap receiver as either a SNMP v2c or v3 receiver.
- Click *OK* to save and add the changes to the running configuration and close the dialog.
- Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- Click *Cancel* to close the dialog without committing updates to the running configuration.

Adding SNMP Trap Receivers

The SNMP *Add* screen is designed to create a new SNMP trap receiver. Use the Add screen to create a new trap receiver IP Address, Port Number and v2c or v3 designation. Add new destination trap receivers as required to suit the various traps enabled and their function in supporting the controller managed network.

To add a new SNMP trap receiver:

- 1 Select *Management Access > SNMP Trap Receivers* from the main menu tree.
- 2 Click the *Add* button at the bottom of the screen.



- 3 Create a new (non DNS name) destination IP address for the new trap receiver to be used for receiving the traps sent by the SNMP agent.
- 4 Define a *Port Number* for the trap receiver.
- 5 Use the *Protocol Options* drop-down menu to specify the trap receiver as either a SNMP v2c or v3 receiver.
- 6 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 7 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *Cancel* to close the dialog without committing updates to the running configuration.

Configuring Management Users

Refer to the *Users* screen to view the administrative privileges assigned to different controller users. You can modify the roles and access modes assigned to each user. The *Users* screen also allows you to configure the authentication methods used by the controller. Use this screen for the following permission configuration activities:

- [Configuring Local Users on page 553](#)
- [Configuring Controller Authentication on page 560](#)

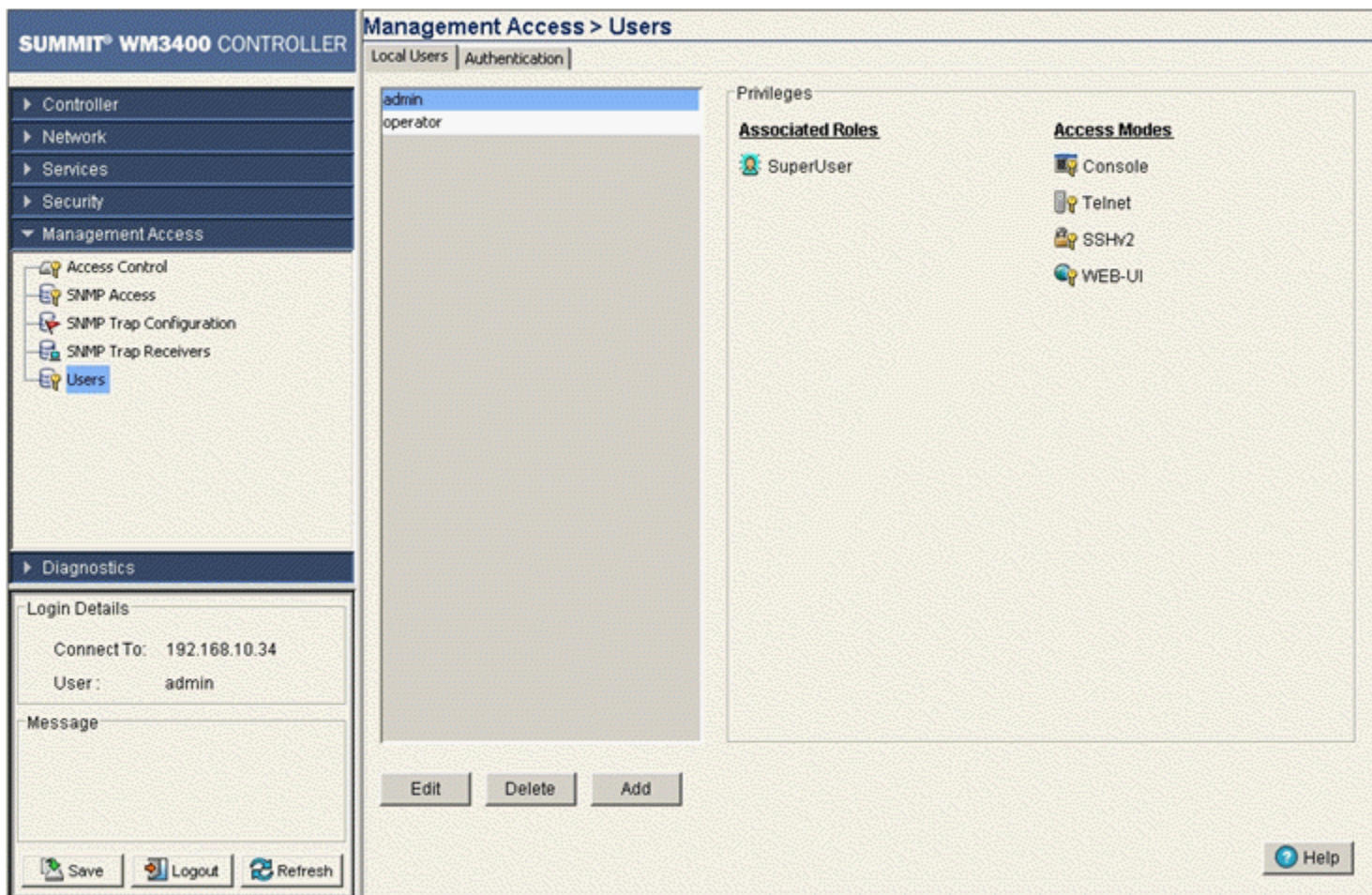
Additionally, the controller Web UI has the facility for creating guest administrators for creating guest users with defined login periods to specific guest groups. For more information, see [“Creating a Guest Admin and Guest User” on page 558](#).

Configuring Local Users

Refer to the *Local Users* tab to view the administrative privileges assigned to users, create a new user and configure the associated roles and access modes assigned to each user.

To configure the attributes of Local User Details:

- 1 Select *Management Access > Users* from the main menu tree.
- 2 Click the *Local Users* tab.



The Local User window consists of 2 fields:

- *Users*—Displays the users currently authorized to use the controller. By default, the controller has two default user types, Admin and Operator.
 - *Privileges*—This frame displays the privileges assigned to different type of user.
- 3 Select the user (Admin, Operator or user defined) from the *Users* frame. The *Privilege* frame displays the rights authorized to the user.
 - 4 Click the *Edit* button to modify the associated roles and access modes of the selected user. By default, the controller has two default users—Admin and Operator. Admin’s role is that of a superuser. An operator has read only access.
 - 5 Click *Add* button to add and assign rights to a new user.
 - 6 Click *Delete* button to delete the selected user from the Users frame.

Creating a New Local User

Local users are those users connected directly into the controller and do not require any sort of configurable remote connection.

To create a new local user:

- 1 Select *Management Access > Users* from the main menu tree.
- 2 Click the *Add* button within the Local Users tab.

Management Access > Users > Configuration

Configuration Add User

User Name

Password

Confirm Password

Associated Roles

Monitor HelpDesk Manager

Network Administrator System Administrator

WebUser Administrator SuperUser

Access Modes

Console Telnet

SSHv2 WEB-UI

Status:

OK Cancel Help

- 3 Enter the login name for the user in the *Username* field. Ensure this name is practical and identifiable to the user.
- 4 Enter the authentication password for the new user in the *Password* field and reconfirm the same again in the *Confirm Password* field.
- 5 Select the role you want to assign to the new user from the options provided in the *Associated Roles* panel. Select one or more of the following options:

Monitor	Select <i>Monitor</i> to assign regular user permissions without any administrative rights. The Monitor option provides <i>read-only</i> permissions.
Help Desk Manager	Assign this role to someone who typically troubleshoots and debugs problems reported by the customer. The Help Desk Manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the controller.
Network Administrator	The <i>Network Administrator</i> has privileges to configure all wired and wireless parameters like IP config, VLANs, Layer 2/Layer 3 security, WLANs, radios, IDS and hotspot.

System Administrator	Select <i>System Administrator</i> to allow the user to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access.
Web User Administrator	Assign <i>Web User Administrator</i> privileges to add users for Web authentication (hotspot).
Super User	Select <i>Super User</i> to assign complete administrative rights.



NOTE

There are some basic operations/CLI commands (exit, logout and help) available to all user roles. All the roles except Monitor can perform Help Desk role operations.



NOTE

By default, the controller is HTTPS enabled with a self signed certificate. This is required since the Web UI uses HTTPS for user authentication.

- 6 Select the access modes to assign to the new user from the options provided in the *Access Modes* panel. Select one or more of the following options:

Console	Provides the new user access to the controller using the console.
SSH	Provides the new user access to the controller using SSH.
Telnet	Provides the new user access to the controller using a Telnet session.
Applet	Provides the new user access to the controller through the Web UI (applet).



NOTE

When establishing a connection to the controller using SSH, ensure that traffic can pass on TCP port 22 between the client and the controller.



NOTE

When establishing a connection to the controller using Telnet, ensure that traffic can pass on TCP port 23 between the client and the controller.



NOTE

When establishing a connection to the controller's applet, ensure that traffic can pass on TCP port 80 for HTTP access and TCP port 443 for HTTPS between the client and the controller.

- 7 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to create the new user.
- 9 Click *Cancel* to revert back to the last saved configuration without saving any of your changes.

Modifying an Existing Local User

To create a new local user:

- 1 Select *Management Access > Users* from the main menu tree.
- 2 Select a user from the Users list and click the *Edit* button.
- 3 The *Username* field is read-only field and displays the login name of the user.
- 4 Enter the new authentication password for the user in the *Password* field and reconfirm within the *Confirm Password* field.
- 5 Select the user role from the options provided in the *Associated Roles* field. Select one or more of the following options:

Monitor	If necessary, modify user permissions without any administrative rights. The Monitor option provides <i>read-only</i> permissions.
Help Desk Manager	Optionally assign this role to someone who typically troubleshoots and debugs problems reported by the customer. the Help Desk Manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the controller.
Network Administrator	The <i>Network Administrator</i> provides configures all wired and wireless parameters like IP config, VLANs, Layer 2/Layer 3 security, WLANs, radios, IDS and hotspot.
System Administrator	Select <i>System Administrator</i> (if necessary) to allow the user to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access.
Web User Administrator	Assign <i>Web User Administrator</i> privileges (if necessary) to add users for Web authentication (hotspot).
Super User	Select <i>Super User</i> (if necessary) to assign complete administrative rights.



NOTE

By default, the controller is HTTPS enabled with a self signed certificate. This is required since the applet uses HTTPS for user authentication.



NOTE

There are some basic operations/CLI commands like exit, logout and help available to all user roles. All roles except Monitor can perform Help Desk role operations.

- 6 Select the access modes you want to assign to the user from the options provided in the *Access Modes* panel. Select one or more of the following options:

Console	Provides the new user access to the controller using the console (applet)
SSH	Provides the new user access to the controller using SSH.
Telnet	Provides the new user access to the controller using Telnet
Applet	Provides the new user access to the controller using the Web UI (applet)



NOTE

When establishing a connection to the controller using SSH, ensure that traffic can pass on TCP port 22 between the client and the controller.



NOTE

When establishing a connection to the controller using Telnet, ensure that traffic can pass on TCP port 23 between the client and the controller.



NOTE

When establishing a connection to the controller's applet, ensure that traffic can pass on TCP port 80 for HTTP access and TCP port 443 for HTTPS between the client and the controller.

- 7 Refer to the *Status* field for an indication of any problems that may have arisen.
The Status is the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 8 Click *OK* to complete the modification of the users privileges.
- 9 Click *Cancel* to revert back to the last saved configuration without saving any of your changes.

Creating a Guest Admin and Guest User

Optionally, create a guest administrator for creating guest users with specific usernames, start and expiry times and passwords. Each guest user can be assigned access to specific user groups to ensure they are limited to just the group information they need, and nothing additional.



NOTE

A guest user added from controller Web UI will be 5 minutes ahead of the controller's current time.

To create a guest administrator:

- 1 Select *Management Access > Users* from the main menu tree.
- 2 Click the *Add* button within the *Local Users* tab.

Management Access > Users > Configuration

Configuration Add User

User Name

Password

Confirm Password

Associated Roles

Monitor HelpDesk Manager

Network Administrator System Administrator

WebUser Administrator SuperUser

Access Modes

Console Telnet

SSHv2 WEB-UI

Status:

OK Cancel Help

- 3 Enter the new guest-admin login name for the user in the *Username* field.
- 4 Enter the authentication password for the guest-admin in the *Password* field and reconfirm the same again in the *Confirm Password* field.
- 5 Assign the guest-admin *WebUser Administrator* access.



NOTE

To create guest users, a guest administrator must be assigned a *WebUser Administrator* access mode. None of the other modes launch the required *Guest User Configuration* screen upon login.

When the guest-admin user logs in, they are redirected to a *Guest User Configuration* screen, wherein start and end user permissions can be defined in respect to specific users.

- 6 Add guest users by name, start date and time, expiry date and time and user group.
- 7 Optionally, click the *Generate* button to automatically create a username and password for each guest user.

- Repeat this process as necessary until all required guest users have been created with relevant passwords and start/end guest group permissions.

Configuring Controller Authentication

The controller provides the capability to proxy authenticate requests to a remote RADIUS server. Refer to the *Authentication* tab to view and configure the RADIUS Server used by the local user to log into the controller.



NOTE

The RADIUS configuration described in this section is independent of other RADIUS Server configuration activities performed using other parts of the controller.

- Select *Management Access > Users* from the main menu tree.
- Select the *Authentication* tab.

SUMMIT® WM3400 CONTROLLER

Management Access > Users

Local Users | Authentication

Authentication methods

Preferred method: local

Alternate method: none

If authentication services are unavailable, allow read-only access

Apply Revert

Radius Servers configured in order of priority:

Index	IP Address	Port	Shared secret	Retries	Timeout

Edit Delete Add

Help

Login Details

Connect To: 192.168.10.34

User: admin

Message

Save Logout Refresh

3 Refer to the *Authentication methods* field for the following:

Preferred Method	Select the preferred method for authentication. Options include: <ul style="list-style-type: none">• <i>None</i>—No authentication• <i>Local</i>—The user employs a local user authentication resource. This is the default setting.• <i>Radius</i>—Uses an external RADIUS Server.
Alternate Method	Select an alternate method for authentication. This drop-down menu will not list the option already selected as the preferred method. Select any of the remaining authentication methods as an alternate method.

If *authentication services are not available*, due to technical reasons, then select the option provided in the panel to avail read-only access.

- 4 Click the *Apply* button to commit the authentication method for the controller.
- 5 Click the *Revert* button to rollback to the previous authentication configuration.
- 6 Refer to the bottom half of the Authentication screen to view the RADIUS Servers configured for controller authentication. The servers are listed in order of their priority.

Index	Displays a numerical <i>Index</i> for the RADIUS Server to help distinguish this RADIUS Server from other servers with a similar configuration. The maximum number that can be assigned is 32.
IP Address	Displays the IP address of the external RADIUS server. Ensure this address is a valid IP address and not a DNS name.
Port	Displays the TCP/IP port number for the RADIUS Server. The port range available for assignment is from 1–65535.
Shared Secret	Displays the shared secret used to verify RADIUS messages (with the exception of the Access-Request message) are sent by a RADIUS-enabled device configured with the same shared secret. The shared secret is a case-sensitive string (password) that can include letters, numbers, or symbols. Ensure the shared secret is at least 22 characters long to protect the RADIUS server from brute-force attacks.
Retries	Displays the maximum number of times the controller can retransmit a RADIUS Server frame before it times out of the authentication session.
Timeout	Displays the maximum time (in seconds) the controller waits for the RADIUS Server's acknowledgment of authentication request packets before the controller times out of the session.

- 7 Select a RADIUS server from the table and click the *Edit* button to modify how the authentication method is used. For more information, see [“Modifying the Properties of an Existing RADIUS Server” on page 561](#).
- 8 Highlight a RADIUS Server from those listed and click the *Delete* button to remove the server from the list of available servers.
- 9 Click the *Add* button at the bottom of the screen to display a sub-screen used to add a RADIUS Server to the list of servers available to the controller. For more information, see [“Adding an External RADIUS Server” on page 563](#).

Modifying the Properties of an Existing RADIUS Server

Some of the attributes of an existing RADIUS Server can be modified by the controller to better reflect the RADIUS Server's existing connection with the controller.

To modify the attributes of an existing RADIUS Server:

- 1 Select *Management Access > Users* from the main menu tree.

The Users screen displays.

- 2 Click the *Authentication* tab.

- 3 Select an existing RADIUS Server from those listed and click the *Edit* button at the bottom of the screen.

- 4 Modify the following RADIUS Server attributes as necessary:

Radius Server Index	Displays the read-only numerical <i>Index</i> value for the RADIUS Server to help distinguish this server from other servers with a similar configuration (if necessary). The maximum number that can be assigned is 32.
Radius Server IP Address	Modify the IP address of the external RADIUS server (if necessary). Ensure this address is a valid IP address and not a DNS name.
Radius Server Port	Change the TCP/IP port number for the RADIUS Server (if necessary). The port range available for assignment is from 1–65535.
Number of retries to communicate with Radius Server	Revise (if necessary) the maximum number of times the controller retransmits a RADIUS Server frame before it times out of the authentication session. The available range is between 0–100.
Time to wait for Radius Server to reply	Revise (if necessary) the maximum time (in seconds) the controller waits for the RADIUS Server's acknowledgment of authentication request packets before the controller times out of the session. The configurable range is between 1–1000 seconds.
Encryption key shared with Radius Server	Enter the encryption key the controller and RADIUS Server share and must validate before the user authentication scheme provided by the RADIUS Server can be initiated.

- 5 Refer to the *Status* field for the current state of the requests made from applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.

- 6 Click *OK* to complete the modification of the RADIUS Server.
- 7 Click *Cancel* to revert back to the last saved configuration without saving any of your changes.

Adding an External RADIUS Server

The attributes of a new RADIUS Server can be defined by the controller to provide a new user authentication server. Once the server is configured and added, it displays within the *Authentication* tab as an option available to the controller.

To define the attributes of a new RADIUS Server:

- 1 Select *Management Access > Users* from the main menu tree.
The Users screen displays.
- 2 Select the *Authentication* tab.
- 3 Click the *Add* button at the bottom of the screen.

Configuration		Add Radius Server	
Radius Server IP Address	<input type="text" value="192 . 122 . 255 . 22"/>		
Radius Server Port	<input type="text" value="153"/>	(0 - 65535)	
Number of retries to communicate with Radius Server	<input type="text" value="5"/>	(0 - 100)	
Time to wait for Radius Server to reply	<input type="text" value="10"/>	(1 - 1000 seconds)	
Encryption key shared with Radius Server	<input type="text" value="12345"/>		
Status:			
		<input type="button" value="OK"/>	<input type="button" value="Cancel"/> <input type="button" value="Help"/>

- 4 Configure the following RADIUS Server attributes:

Radius Server IP Address	Provide the IP address of the external RADIUS server. Ensure this address is a valid IP address and not a DNS name.
Radius Server Port	Enter the TCP/IP port number for the RADIUS Server. The port range available for assignment is from 1–65535.
Number of retries to communicate with Radius Server	Enter the maximum number of times for the controller to retransmit a RADIUS Server frame before it times out the authentication session. The available range is between 0–100.
Time to wait for Radius Server to reply	Enter the maximum number of times the controller can retransmit a RADIUS Server frame before it times out of the authentication session. The available range is between 0–100.
Encryption key shared with Radius Server	Enter the encryption key the controller and RADIUS Server share and must validate before the user based authentication provided by the RADIUS Server can be initiated.

- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *OK* to complete the addition of the RADIUS Server.
- 7 Click *Cancel* to revert back to the last saved configuration without saving any of your changes.

External RADIUS Server Settings

When using an external RADIUS Server with the controller, ensure that the following values are configured on your server to ensure maximum compatability with the controller.

Vendor ID.

Vendor ID The Extreme Networks vendor ID is 1916.

RADIUS VSAs.

There are two RADIUS VSAs used for management user authentication:

VSA Name	Attribute Number	Type	Values
Extreme-Service-Type	1	Integer (Decimal)	<ul style="list-style-type: none"> • Monitor Role: Value is 1. (read-only access to the controller) • Helpdesk Role: Value is 2. (helpdesk/support access to the controller) • Nwadmin Role: Value is 4. (all wired and wireless access to the controller) • Sysadmin Role: Value is 8. (System administrator access) • WebAdmin Role: Value is 16. (Guest user application access) • Superuser Role: Value is 32768. (grants full read/write access to the controller) <p>To configure multiple roles this value may be configured multiple times with different values for each role.</p>
Extreme-Login-Service	100	Integer (Decimal)	<ul style="list-style-type: none"> • Console Access: Value is 128. (user is allowed to login only from console) • Telnet Access: Value is 64. (use is allowed to login only from telnet session) • SSH Access: Value is 32. (user is allowed to login only from ssh session) • Web Access: Value is 16. (user is allowed to login only from web/applet) <p>To configure multiple access methods this value can be set multiple times with different access values, or the desired values can be added together and entered as a single value.</p>

9 Diagnostics

CHAPTER

This chapter describes the various diagnostic features available for monitoring controller performance. This chapter consists of the following controller diagnostic activities:

- [Displaying the Main Diagnostic Interface on page 565](#)
- [Configuring System Logging on page 573](#)
- [Reviewing Core Snapshots on page 580](#)
- [Reviewing Panic Snapshots on page 582](#)
- [Debugging the Applet on page 585](#)
- [Configuring a Ping on page 586](#)



NOTE

HTTPS must be enabled to access the controller applet. Ensure HTTPS access has been enabled before using the login screen to access the controller applet.



NOTE

The Extreme Networks Wireless Management Suite (WMS) is a recommended utility to plan the deployment of the controller and view its configuration once operational. Extreme Networks WMS can help optimize the positioning and configuration of a controller and assist in the troubleshooting of performance issues as they are encountered in the field.

Displaying the Main Diagnostic Interface

The main diagnostic screen contains tabs assessing the performance of the following diagnostics:

- [Controller Environment on page 566](#)
- [CPU Performance on page 567](#)
- [Controller Memory Allocation on page 569](#)
- [Controller Disk Allocation on page 570](#)
- [Controller Memory Processes on page 571](#)
- [Other Controller Resources on page 572](#)



NOTE

When the controller's configuration is successfully updated (using the Web UI), the affected screen is closed without informing the user their change was successful. However, if an error were to occur, the error displays within the affected screen's Status field and the screen remains displayed. In the case of file transfer operations, the transfer screen remains open during the transfer operation and remains open upon completion (with status displayed within the Status field).

Controller Environment

Use the *Environment* tab to view and modify the controller diagnostic interval, temperature sensors and fan speeds.

- 1 Select *Diagnostics* from the main tree menu.
- 2 Select the *Environment* tab (opened by default).

Summit WM3400 CONTROLLER

Environment | CPU | Memory | Disk | Processes | Other Resources

Settings

Enable Diagnostics Monitoring Interval: (100 - 30000 millisecs)

Temperature Sensors Number of sensors : 6

Name	Current Temperature	High Limit	Critical Limit	Hysteresis (°C)
exhaust fan	39.0	70.0	95.0	5.0
inlet near PCI 0	29.0	70.0	95.0	5.0
inboard of PCI 1	29.0	70.0	95.0	5.0
between CPU/BCMS3115	39.0	70.0	95.0	5.0
leeward of BCMS3115	37.0	70.0	95.0	5.0
cons/USB/PCIe	38.0	70.0	95.0	5.0

Fans Number of fans : 1

Name	Current Speed (rpm)	Low Speed Limit (rpm)	Hysteresis (rpm)
exhaust	3480	3000	250

Apply Revert Help

-
- 3 The Environment displays the following fields:
 - Settings
 - Temperature Sensors
 - Fans
 - 4 In the Settings field, select the *Enable Diagnostics* checkbox to enable/disable diagnostics and set the monitoring interval. The monitoring interval is the interval the controller uses to update the information displayed within the CPU, Memory, Disk, Processes and Other Resources tabs. Keep the monitoring interval at a shorter time increment when periods of heavy wireless traffic are anticipated.



NOTE

Enabling controller diagnostics is recommended, as the diagnostics facilities provide detailed information on the physical performance of the controller and may provide indicators in advance of actual problems. Enabling diagnostics also assists in troubleshooting problems associated with data transfers and the monitoring of network traffic.

- 5 Use the Temperature Sensors field to monitor the CPU and system temperatures. This information is extremely useful in assessing if the controller exceeds its critical limits.



NOTE

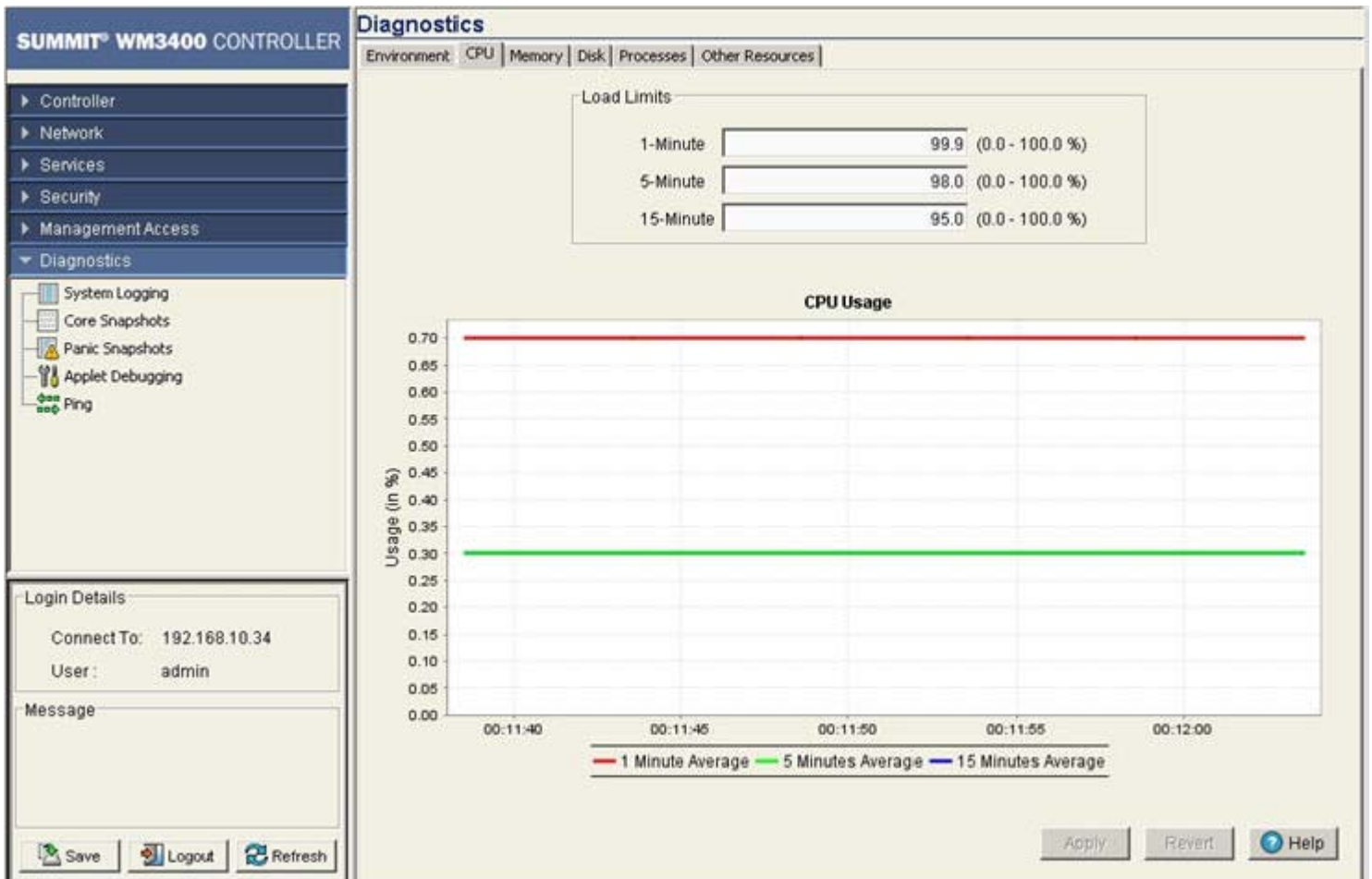
A Summit WM3700 Controller has six sensors.

- 6 Refer to the *Fans* field to monitor the CPU and system fan speeds.
- 7 Click the *Apply* button to commit and apply the changes.
- 8 Click the *Revert* button to revert back to the last saved configuration.

CPU Performance

Use the *CPU* tab to view and define the CPU's load statistics. Load limits can be assessed for the last one minute, five minutes and 15 minutes to better gauge controller loads over differing periods of network activity.

- 1 Select *Diagnostics* from the main tree menu.
- 2 Select the *CPU* tab.



- 3 The *CPU* screen consists of 2 fields:
 - Load Limits
 - CPU Usage
- 4 The *Load Limits* field displays the maximum CPU load limits for the last 1, 5, and 15 minutes. The limits displayed coincide with periods of increased or decreased controller activity. The maximum CPU load threshold can be manually configured.
- 5 The *CPU Usage* field displays real time CPU consumption values. Use this information to periodically determine if performance is negatively impacted by the overuse of controller CPU resources. If CPU usage is substantial during periods of low network activity, then perhaps, the situation requires troubleshooting.
- 6 Click the *Apply* button to commit and apply the changes.
- 7 Click the *Revert* button to revert back to the last saved configuration.

Controller Memory Allocation

Use the *Memory* tab to periodically assess the controller's memory load.

- 1 Select *Diagnostics* from the main tree menu.
- 2 Select the *Memory* tab.

SUMMIT™ WM3400 CONTROLLER

Diagnostics

Environment | CPU | **Memory** | Disk | Processes | Other Resources

RAM

Free Limit: (0.0 - 25.0 %)

81% Free

Free=124 MB Available=204 MB

Buffers

Name	Usage	Limit
Buffer32	3202	32768
Buffer64	3885	8192
Buffer128	1584	4096
Buffer256	704	4096
Buffer512	632	8192
Buffer1k(1024)	80	8192
Buffer2k(2048)	99	16384
Buffer4k(4096)	36	16384
Buffer8k(8192)	10	1024
Buffer16k(16384)	84	512
Buffer32k(32768)	3	256
Buffer64k(65536)	2	64

Login Details

Connect To: 192.168.10.34

User: admin

Message

Save Logout Refresh

Apply Revert Help

The Memory tab is partitioned into the following two fields:

- RAM
- Buffer

- 3 Refer to the *RAM* field to view the percentage of CPU memory in use (in a pie chart format).
- 4 Refer to the *Free Limit* value to change the CPU's memory allocation limits. Free Limit should be configured in respect to high bandwidth and increased load anticipated over the controller managed network.
- 5 The *Buffers* field displays buffer usage information. The Buffers field consists of the following information:

Name	The name of the buffer
Usage	Buffer's current usage
Limit	The buffer limit

- 6 Click the *Apply* button to commit and apply the changes.

- Click the *Revert* button to revert back to the last saved configuration.

Controller Disk Allocation

The *Disk* tab contains parameters related to the various disk partitions on the controller. It also displays available space in the external drives (compact flash etc).

- Select *Diagnostics* from the main tree menu.
- Select the *Disk* tab.

SUMMIT® WM3400 CONTROLLER

Diagnostics

Environment | CPU | Memory | **Disk** | Processes | Other Resources

flash:

Free Space Limit (0.0 - 100.0 %)

98% Free

Free=83,932 KB Total=86,016 KB

nvram:

Free Space Limit (0.0 - 100.0 %)

97% Free

Free=63,808 KB Total=65,536 KB

system:

Free Space Limit (0.0 - 100.0 %)

Free INodes 98.4 %

Free INode Limit (0.0 - 10.0 %)

96% Free

Free=19,668 KB Total=20,480 KB

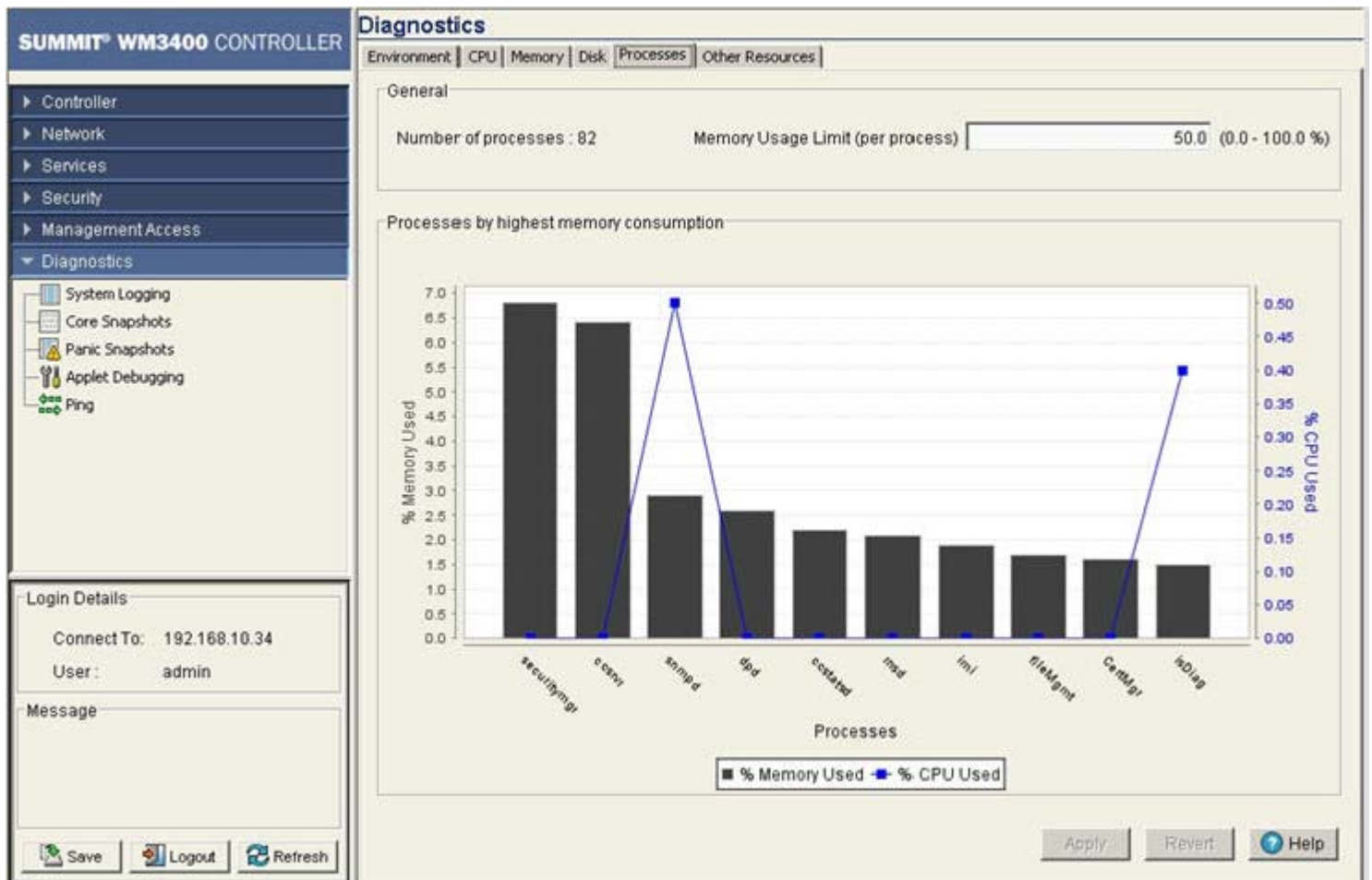
Save Logout Refresh Apply Revert Help

- This *Disk* tab displays the status of the controller flash, nvram and system disk resources. Each field displays the following:
 - Free Space Limit
 - Free INodes
 - Free INode Limit
- Define the *Free Space Limit* variable carefully, as disk space may be required during periods of high bandwidth traffic and file transfers.
- Click the *Apply* button to commit and apply the changes.
- Click the *Revert* button to revert back to the last saved configuration.

Controller Memory Processes

The *Processes* tab displays the number of processes in use and percentage of memory usage limit per process.

- 1 Select *Diagnostics* from the main tree menu.
- 2 Select the *Processes* tab



- 3 The *Processes* tab has 2 fields:
 - General
 - Processes by highest memory consumption
- 4 Refer to the *General* field to review the number of processes in use and percentage of memory usage per process. The value defined is the maximum limit per process during periods of increased and network activity and is negotiated among the other process as needed during normal periods of controller activity.
- 5 *Processes by highest memory consumption* displays a graph of the top ten controller processes based on memory consumption. Use this information to determine if a spike in consumption with the controller priorities in processing data traffic within the controller managed network.
- 6 Click the *Apply* button to commit and apply any changes to the memory usage limit.
- 7 Click the *Revert* button to revert back to the last saved configuration.

Other Controller Resources

The *Other Resources* tab displays the memory allocation of Packet Buffer, IP Route Cache and File Descriptors.

- 1 Select *Diagnostics* from the main tree menu.
- 2 Select the *Other Resources* tab.

SUMMIT WM3400 CONTROLLER

Diagnostics

Environment | CPU | Memory | Disk | Processes | **Other Resources**

Packet Buffers

4% In Use

Maximum Limit (0 - 65535)

In Use=390 Allocated=11,000

IP Route Cache

2% In Use

Maximum Limit (0 - 65535)

In Use=17 Allocated=1,000

File Descriptors

6% In Use

Maximum Limit (0 - 32767)

In Use=1,632 High Water Mark=25,500

Login Details

Connect To: 192.168.10.34

User: admin

Message

Save Logout Refresh Apply Revert Help

Keep the Cache allocation in line with cache expectations required within the controller managed network.

- 3 Define the maximum limit for each resource accordingly as you expect these resources to be utilized within the controller managed network.
- 4 Click the *Apply* button to commit and apply any changes to any of the resources maximum limit.
- 5 Click the *Revert* button to revert back to the last saved configuration

Configuring System Logging

Use the *System Logging* screen for logging system events. It is important to log individual controller events to discern an overall pattern that may be negatively impacting controller performance. The System Logging screen consists of the following tabs:

- [Log Options on page 573](#)
- [File Management on page 574](#)

Log Options

Use the Log Options tab to enable logging and define the medium used to capture system events and append them to the log file. Ensure the correct destination server address is supplied.

To view the Log options available to the controller:

- 1 Select *Diagnostics > System Logging* from the main menu tree.
- 2 Select the *Log Options* tab.

The screenshot displays the 'Diagnostics > System Logging' configuration page for a Summit WM3400 Controller. The 'Log Options' tab is active. The configuration includes:

- Enable Logging Module
- Enable logging to Buffer (Log Level: 4: Warning)
- Enable logging to Console (Log Level: 4: Warning)
- Enable logging to Syslog Server (Log Level: 6: Info)
- Server Facility: Facility: local7
- Server 1 (IP Address): 0 . 0 . 0 . 0
- Server 2 (IP Address): 0 . 0 . 0 . 0
- Server 3 (IP Address): 0 . 0 . 0 . 0
- Logging aggregation time: 0 (0 - 60 secs)

At the bottom, there are buttons for 'Apply', 'Revert', and 'Help'. The left sidebar shows the navigation menu with 'System Logging' selected under 'Diagnostics'. The bottom left corner shows 'Login Details' (Connect To: 192.168.10.34, User: admin) and a 'Message' field.

- 3 Select the *Enable Logging Module* checkbox to enable the controller to log system events to a user defined log file or a syslog server.
- 4 Select the *Enable Logging to Buffer* checkbox to enable the controller to log system events to a buffer.

The log levels are categorized by their severity. The default level is 3, (errors detected by the controller). However, more granular log levels can be selected for system level information detected by the controller that may be useful in assessing overall controller performance or troubleshooting.

- 5 Select the *Enable Logging to Console* checkbox to enable the controller to log system events to the system console.

Use the drop-down menu to select the desired log level for tracking system events to a local log file. This setting logs warning events (and those more severe) by default.

- 6 Select the *Enable Logging to Syslog Server* checkbox to enable the controller to log system events send them to an external syslog server. Selecting this option also enables the Server Facility feature. Use the drop-down menu to select the desired log level for tracking system events to a local log file.
 - a Use the *Server Facility* drop-down menu to specify the local server facility (if used) for the transfer.
 - b Specify the numerical (non DNS name) IP address for the first choice syslog server to log system events (within the *Server 1* field).
 - c Optionally, use the *Server 2* parameter to specify the numerical (non DNS name) IP address of an alternative syslog server if the first syslog server is unavailable.
 - d Optionally, use the *Server 3* parameter to specify the numerical (non DNS name) IP address of a third syslog server to log system events if the first two syslog servers are unavailable.

**NOTE**

255.255.255.255 is accepted as a valid entry for the IP address of a logging server.

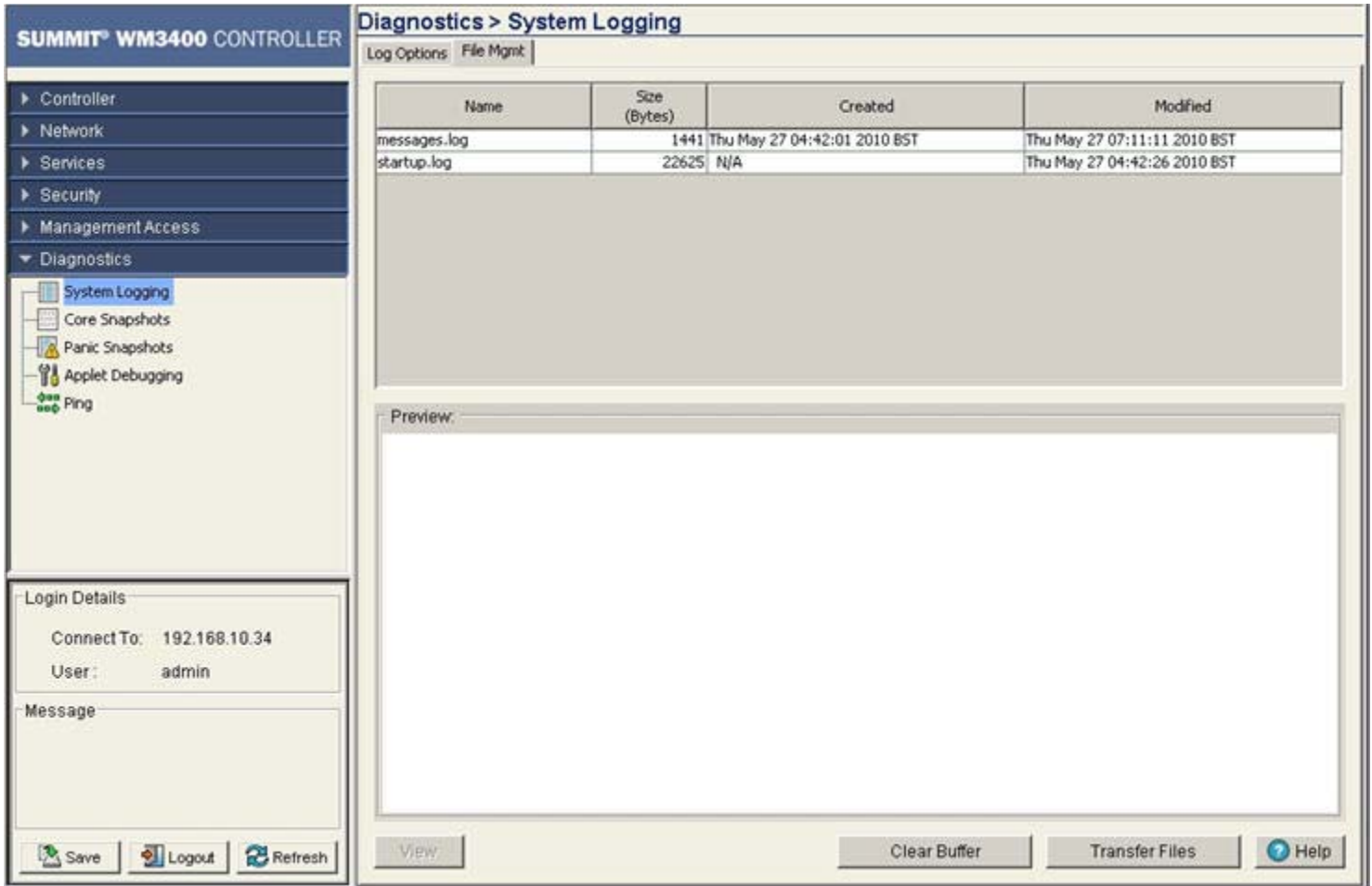
- 7 Use the *Logging aggregation time* parameter to define the increment (or interval) system events are logged (0-60 seconds). The shorter the interval, the sooner the event is logged.
- 8 Click *Apply* to save the changes made to the screen. This will overwrite the previous configuration.
- 9 Click *Revert* to move the display back to the last saved configuration.

File Management

Use the *File Mgt* tab to view existing system logs. Select a file to display its details in the *Preview* field. Click the *View* button to display the file's entire contents. Once viewed, the user has the option of clearing the file or transferring the file to a user-defined location.

To view the Log options:

- 1 Select *Diagnostics > System Logging* from the main menu tree.
- 2 Select the *File Mgmt* tab.



3 The *File Mgmt* tab displays existing log files. Refer to the following for log file details:

Name	Displays a read-only list of the log files (by name) created since the last time the display was cleared. To define the type of log files created, click the <i>Log Options</i> tab to enable logging and define the log level.
Size	Displays the log file size in bytes. This is the current size of the file, if modifications were made, they have been accounted for.
Created	Displays the date, year and time of day the log file was initially created. This value only states the time the file was initiated, not the time it was modified or appended.
Modified	Displays the date, year and time of day the log file was modified since its initial creation date.

4 Highlight an existing log file to display the file's first page within the *Preview* field. Once a file is selected, its name is appended within the preview field, and its contents are displayed.

The time, module, severity, mnemonic and description of the file are displayed.

5 Highlight a file from the list of log files available within the *File Mgmt* tab and click the *View* button to display a detailed description of the entire contents of the log file.

To view the entire content of an individual log file, see [“Viewing the Entire Contents of Individual Log Files”](#) on page 576.

- 6 Click the *Clear Buffer* button to remove the contents of the File Mgmt tab. This is only recommended if you consider the contents of this file obsolete and wish to begin gathering new log file data.

When the button is selected, a confirmation prompt displays verifying whether the contents of the log files is cleared.

- 7 Click the *Transfer Files* button to display a sub-screen wherein log files can be sent to an external location (defined by you) using a user-defined file transfer medium.



NOTE

On the Summit WM3700 users can also transfer log files using USB or Compact Flash. On the Summit WM3600 users can also transfer log files using USB. On Summit WM3400 users can also transfer log files using USB or PCI Express card.



NOTE

When a PCI Express storage device and a standard USB storage device are both connected to the controller, the device that is connected to the controller first will be listed as USB1 and the device connected second will be listed as USB2.

Transferring files is recommended when the log file is frequently cleared, but an archive of the log files is required in a safe location. For more information on transferring individual log files, see [“Transferring Log Files”](#) on page 578.

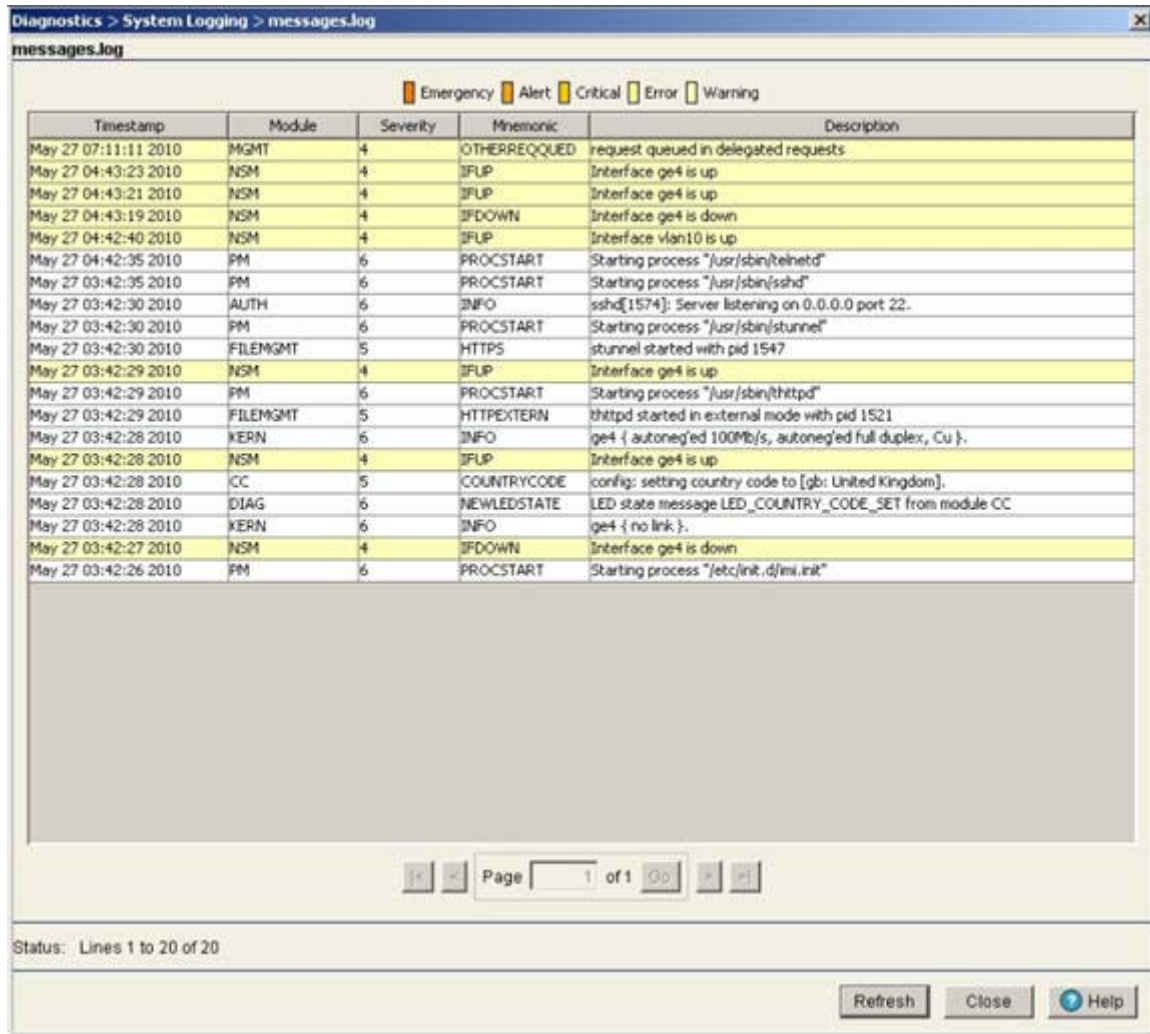
Viewing the Entire Contents of Individual Log Files

Extreme Networks recommends the entire contents of a log file be viewed to make an informed decision whether to transfer the file or clear the buffer. The *View* screen provides additional details about a target file by allowing the entire contents of a log file to be reviewed.

To display the entire contents of a log file:

- 1 Select *Diagnostics > System Logging* from the main menu tree.
- 2 Select the *File Mgmt* tab.

- 3 Select an individual log file whose properties you wish to display in detail and click the *View* button.



- 4 Refer to the following for information on the elements that can be viewed within a log file:

Timestamp	Displays the date, year and time of day the log file was initially created. This value only states the time the file was initiated, not the time it was modified or appended.
Module	Displays the name of the controller logging the target event. This metric is important for troubleshooting issues of a more serious priority, as it helps isolate the controller resource detecting the problem.

Severity	<p>The Severity level coincides with the logging levels defined within the Log Options tab. Use these numeric identifiers to assess the criticality of the displayed event. The severity levels include:</p> <ul style="list-style-type: none">• 0—Emergency• 1—Alert• 2—Critical• 3—Errors• 4—Warning• 5—Notice• 6—Info• 7—Debug
Mnemonic	<p>Use the <i>Mnemonic</i> as a text version of the severity code information. A mnemonic is convention for the classification, organization, storage and recollection of controller information.</p>
Description	<p>Displays a high-level overview of the event, and (when applicable) message type, error or completion codes for further clarification of the event. Use this information for troubleshooting or for data collection.</p>

- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click the *Refresh* button to update the contents of the screen to the latest values.
- 7 Click the *Close* button to exit the screen. Clicking Close does not lose any data, as there are no values configured within this screen (it is view-only).

Transferring Log Files

If a system log contains data that may require archiving, consider using the *Transfer Files* screen to export the log file to an external location (that you designate) where there is no risk of deleting the contents of the log.

To transfer a log file to a user specified location:

- 1 Select *Diagnostics > System Logging* from the main menu tree.
- 2 Select the *File Mgmt* tab.

- 3 Select a target log file to transfer and click the *Transfer File* button.

The screenshot shows a web-based 'Transfer' dialog box. The title bar reads 'Diagnostics > System Logging > Transfer'. The dialog is split into two panes. The left pane, labeled 'Source', contains a 'From' dropdown menu with 'Controller' selected and a 'File' dropdown menu with 'messages.log' selected. The right pane, labeled 'Target', contains a 'To' dropdown menu with 'Server' selected, a 'File' text input field, a 'Using' dropdown menu with 'FTP' selected, a 'Port' text input field with '21', an 'IP Address' text input field with three dots, a 'User ID' text input field, a 'Password' text input field, and a 'Path' text input field. A 'Status:' label is positioned below the 'Source' pane. At the bottom of the dialog are four buttons: 'Transfer', 'Abort', 'Close', and 'Help'.

- 4 Use the *From* drop-down menu (within the Source field) to specify the location from which the log file is sent. If only the applet is available as a transfer location, use the default controller option.
- 5 Select a target file for transfer from the *File* drop-down menu. The drop-down menu contains the log files listed within the *File-Mgmt* screen.
- 6 Use the *To* drop-down menu (within the Target field) to define whether the target log file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
- 7 Provide the name of the file to be transferred within the *File* parameter. Ensure the file name is correct or the transfer will not take place.
- 8 If Server has been selected as the source, use the *Using* drop down-menu to configure whether the log file transfer is conducted using FTP or TFTP.
- 9 If Server has been selected as the source, enter the *IP Address* of the destination server or system receiving the log file. Ensure the IP address is valid or risk jeopardizing the success of the log file transfer.
- 10 If Server has been selected as the source, enter the *User ID* credentials required to send the log file to the target location.
- 11 If Server has been selected as the source, use the *Password* parameter to enter the password required to send the log file to the target location.
- 12 Specify the appropriate *Path* name to the target directory on the local system disk or server as configured using the *To* parameter. If the local disk is selected, a browse button is available.
- 13 Click the *Transfer* button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired log file to the specified location.
- 14 If a problem condition is discovered during the file transfer, click the *Abort* button to terminate the transfer.
- 15 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 16 Click the *Close* button to exit the screen. No values need to be saved once the transfer has been made.

Reviewing Core Snapshots

Use the *Core Snapshots* screen to view the core snapshots (system events and process failures with a .core extension) logged by the system. Core snapshots are issues impacting controller core (or distribution layer). Once reviewed, core files can be deleted or transferred for archive.

To view core snapshots available on the controller:

- 1 Select *Diagnostics > Core Snapshots* from the main menu tree.

The screenshot displays the 'Diagnostics > Core Snapshots' interface. On the left, a navigation tree includes 'System Logging', 'Core Snapshots' (highlighted), 'Panic Snapshots', 'Applet Debugging', and 'Ping'. Below the tree is a 'Login Details' section with 'Connect To: 192.168.10.34' and 'User: admin'. The main content area features a table with the following structure:

Name	Size (Bytes)	Created
(Table is currently empty)		

At the bottom of the interface, there are buttons for 'Save', 'Logout', 'Refresh', 'Delete', 'Transfer Files', and 'Help'.

- 2 Refer to the following table headings within the Core Snapshots screen:

Name	Displays the title of the process, process ID (pid) and build number separated by underscores. The file extension is always .core for core files.
Size (Bytes)	Displays the size of the core file in bytes.
Created	Displays the date and time the core file was generated. This information may be useful in troubleshooting issues.

- 3 Select a target file and click the *Delete* button to remove the selected file. This option is not recommended until the severity of the core snapshot has been assessed.

- 4 Click the *Transfer Files* button to open the transfer dialogue to enable a file to be copied to another location. For more information on transferring core snapshots, see [“Transferring Core Snapshots” on page 581](#).

Transferring Core Snapshots

Use the *Transfer* screen to define a source for transferring core snapshot files to a secure location for potential archive.

To transfer core snapshots to a user defined location:

- 1 Select *Diagnostics > Core Snapshots* from the main menu tree.
- 2 Select a target file, and select the *Transfer Files* button.

The screenshot shows a 'Transfer' dialog box with the following fields and controls:

- Source:**
 - From:** A dropdown menu currently showing 'Controller'.
 - File:** A dropdown menu for selecting a file.
- Target:**
 - To:** A dropdown menu currently showing 'Server'.
 - File:** A text input field for the target file name.
 - Using:** A dropdown menu currently showing 'FTP'.
 - Port:** A text input field currently showing '21'.
 - IP Address:** A text input field with three dots as a placeholder.
 - User ID:** A text input field.
 - Password:** A text input field.
 - Path:** A text input field.
- Buttons:** 'Transfer', 'Abort', 'Close', and 'Help'.

- 3 Use the *From* drop-down menu to specify the location from which the log file is sent. If only the applet is available as a transfer location, use the default controller option.
- 4 Select a target file for the file transfer from the *File* drop-down menu. The drop-down menu contains the core files listed within the File-Mgmt screen.
- 5 Use the *To* drop-down menu (within the Target field) to define whether the target log file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
- 6 Provide the name of the file to be transferred to the location specified within the *File* field.
- 7 If Server has been selected as the source, use the *Using* drop down-menu to configure whether the log file transfer is sent using FTP or TFTP.
- 8 If Server has been selected as the source, enter the *IP Address* of destination server or system receiving the target log file.
- 9 If Server has been selected as the source, enter the *User ID* credentials required to send the file to the target location. Use the user ID for FTP transfers only.
- 10 If Server has been selected as the source, enter the *Password* required to send the file to the target location using FTP.
- 11 Specify the appropriate *Path* to the target directory on the local system disk or server as configured using the *To* parameter. If the local disk option is selected, use the browse button to specify the location on the local disk.

- 12 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 13 Click the *Transfer* button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired log file to the specified location.
- 14 If a problem condition is discovered during the file transfer, click the *Abort* button to terminate the transfer.
- 15 Click the *Close* button to exit the screen after a transfer. There are no changes to save or apply.

Reviewing Panic Snapshots

Refer to the *Panic Snapshots* screen for an overview of the panic files available. Typically, panic files refer to controller events interpreted as critical conditions (and thus requiring prompt attention). Use the information displayed within the screen to make informed decisions whether a target file should be discarded or transferred to a secure location for permanent archive.

To review the current panic snapshots on the controller:

- 1 Select *Diagnostics > Panic Snapshots* from the main menu.

The screenshot displays the Summit WM3400 Controller web interface. The left-hand navigation menu is expanded to show the 'Diagnostics' section, with 'Panic Snapshots' selected. The main content area is titled 'Diagnostics > Panic Snapshots' and features a table with the following headers: 'Name', 'Size (Bytes)', and 'Created'. Below the table is a 'Preview:' section. At the bottom of the interface, there is a toolbar with buttons for 'View', 'Delete', 'Transfer Files', and 'Help'. The 'Login Details' section on the left shows 'Connect To: 192.168.10.34' and 'User: admin'. The 'Message' section is currently empty.

2 Refer to the following table headings within the Panic Snapshots screen:

Name	Displays the title of the panic file. Panic files are named n.panic where n is in the range 0-9. 0 is always the oldest saved panic file and the highest number is the most recent. If the system experiences a panic, there are ten existing panics, the oldest is deleted and the remaining nine are renamed so the newest can be saved as 9.
Size	Displays the size of the panic file in bytes.
Created	Displays the date and time the panic file was created. The panic file is created after the system reboots, however the panic information within the file contains the date and time the panic actually occurred.

3 Refer to the *Preview* field for panic information in ASCII text. When a panic file is selected, the corresponding text is displayed in the preview screen and the name of the file displays. Use this information as a high-level overview of the panic.

4 Select a target panic file and click the *Delete* button to remove the file.

5 Select a target panic file and click the *View* button to open a separate viewing screen to display the panic information in greater detail. For more information, see [“Viewing Panic Details” on page 583](#).

6 Click the *Transfer Files* button to open the transfer dialogue to transfer the file to another location. For more information, see [“Transferring Panic Files” on page 583](#).

Viewing Panic Details

Use the *View* facility to review the entire contents of a panic snapshot before transferring or deleting the file. The view screen enables you to display the entire file.

To review Panic Snapshots:

1 Select *Diagnostics > Panic Snapshots* from the main menu.

2 Select a panic from those available and click the *View* button.

3 Refer to the following information to review the severity of the panic file:

Main	The <i>Main</i> parameter displays detailed panic information for the selected file.
Page	Panic information may be spread across multiple pages. The Page value allows the user to view complete information on the panic. Use the < and > options to navigate through the contents of the file.
Refresh	Click the <i>Refresh</i> button to update the data displayed within the screen to the latest values.
Close	Click the <i>Close</i> button to exit the screen.

Transferring Panic Files

It is recommended that panic snapshots files be kept in a safe location off the system used to create the initial files. Use the *Transfer Files* screen to specify a location where files can be archived without the risk of them being lost or corrupted.

For information on transferring panic files:

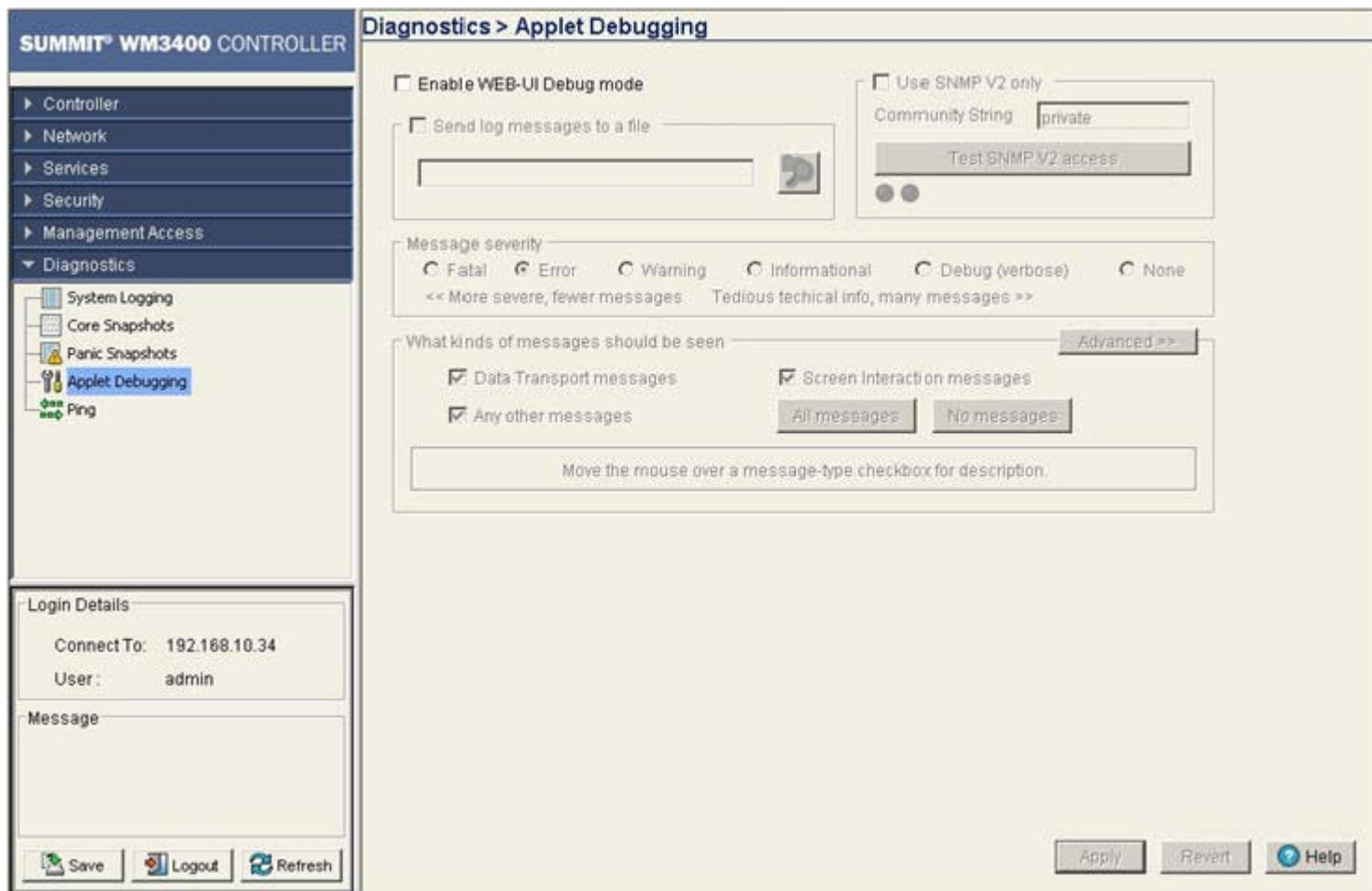
- 1 Select *Diagnostics > Panic Snapshots* from the main menu.
- 2 Select a record from those available and click the *Transfer* button.

- 3 Use the *From* drop-down menu to specify the location from which the file is sent. If only the applet is available as a transfer location, use the default controller option.
- 4 Select a file for the file transfer from the *File* drop-down menu. The drop-down menu contains the panic files listed within the File-Mgmt screen.
- 5 Use the *To* drop-down menu (within the Target field) to define whether the target panic file is to be sent to the system's local disk (Local Disk) or to an external server (Server).
- 6 Provide the name of the file to be transferred to the location specified within the *File* field.
- 7 If Server has been selected as the source, use the *Using* drop down-menu to configure whether the panic file transfer will be sent using FTP or TFTP.
- 8 If Server has been selected as the source, enter the *IP Address* of the destination server or system receiving the target panic file.
- 9 If Server has been selected as the source, enter the *User ID* credentials required to send the file to the target location. The User ID is required for FTP transfers only.
- 10 If Server has been selected as the source, enter the *Password* required (for FTP transfers) to send the file to the target location.
- 11 Specify the appropriate path name to the target directory on the local system disk or server as configured using the "To" parameter. If local server is selected, use the Browse button to specify a location on your local machine.
- 12 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 13 Click the *Transfer* button when ready to move the target file to the specified location. Repeat the process as necessary to move each desired log file to the specified location.
- 14 If a problem condition is discovered during the file transfer, click the *Abort* button to terminate the transfer.
- 15 Click the *Close* button to exit the dialogue and abandon the transfer.

Debugging the Applet

Refer to the *Applet Debugging* screen to debug the applet. This screen allows you to view and debug system events by a criticality level you define.

- 1 Select *Diagnostics > Applet Debugging* from the main menu.



- 2 To use this window, select the *Enable Web-UI Debug Mode* checkbox.
The Applet Debugging field is partitioned into the following editable fields:
 - Send log message to a file
 - Use SNMP V2 only
 - Message Severity
 - What kinds of message should be seen
- 3 Select the *Send log message to a file* checkbox if you wish to store the log message.
Enabling this checkbox allows you to select the file location where you wish to store the log message.
- 4 Select the *Use SNMP V2 only* checkbox to use SNMP V2 to debug the applet.
Check whether you have access to SNMP V2 by clicking on the *Test SNMP V2 access* button. If SNMP V2 access is available, the test icon will change from gray to green, indicating the SNMP V2 interface is viable on the controller.

- 5 Select the severity of the message you wish to store in the log file.

The *Message Severity* section allows you to report a bug and log it per the following severity levels:

- *Fatal*—loss of data or controller functionality
- *Error*—controller data compilation problem, could result in data loss
- *Warning*—potential data loss of configuration corruption
- *Informational*—data that may be useful in assessing a potential error
- *Debug*—information relevant to troubleshooting
- *None*—no impact.

- 6 Select the message deployed when a bug is raised.

The *What Kind of message should be seen* field allows you to select a range of parameters for returned messages while debugging. Move your mouse pointer over a message checkbox for a message description.

- a Click the *Advanced* button to display the entire list of message categories when bugs are raised. Select the checkboxes corresponding to the message types you would like to receive.

Each message category is enabled by default. Click the *Simple* button to minimize this area and hide the available message categories.

- b Click the *All Messages* button to select all the message categories.

- c Click the *No Messages* button if you do not want to select any of the message categories.

- 7 Click the *Apply* button to save the changes you have applied within this screen.

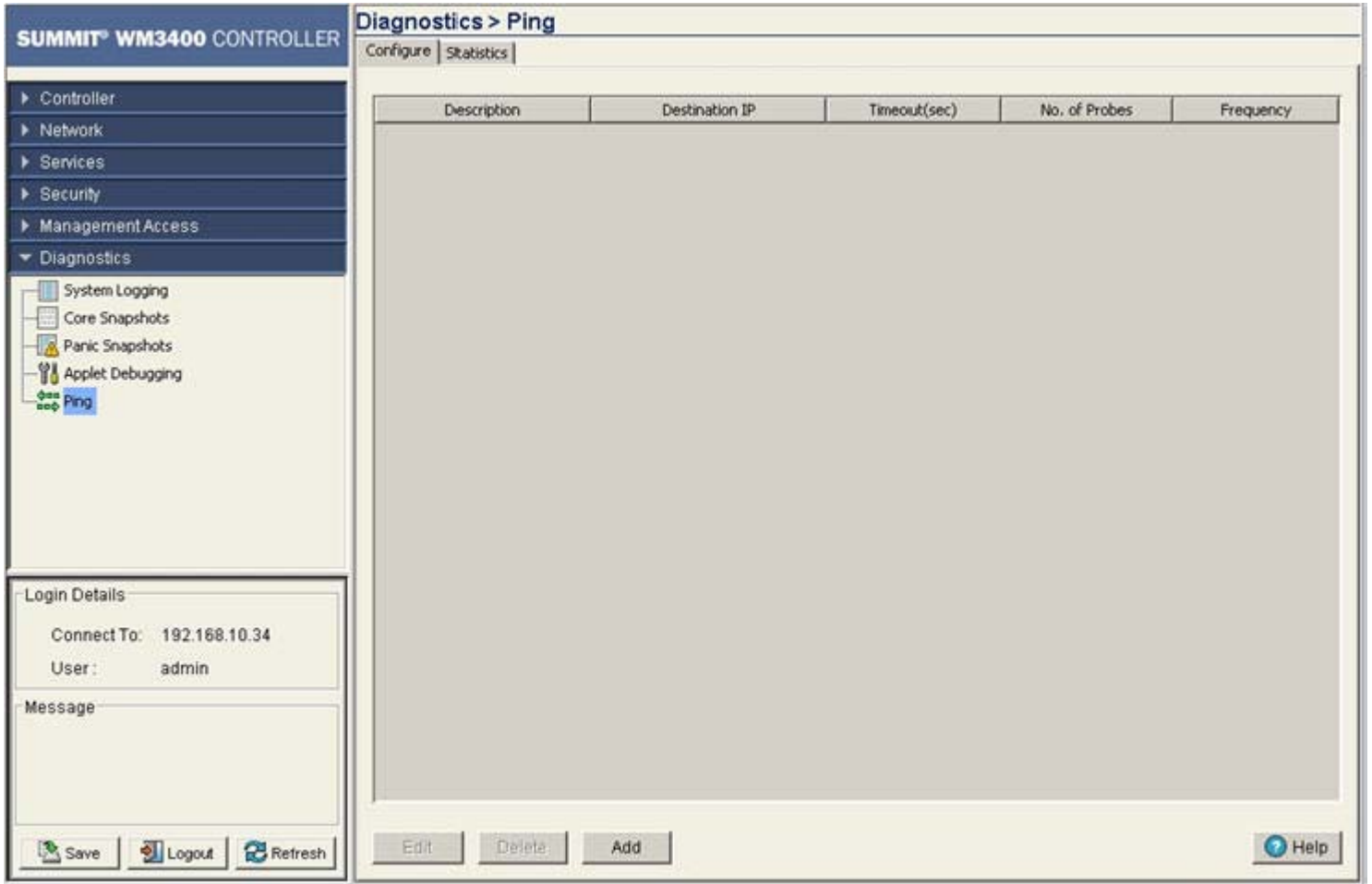
- 8 Click the *Revert* button to revert back to the last saved configuration.

Configuring a Ping

The controller can verify its link with other controllers and associated MUs by sending ping packets to the associated device. Use a ping to test the connection between the controller and IP destinations you specify. For each ping packet transmitted, statistics are gathered for the round-trip time (RTT) between the controller and its destination. The RTT is the time (in milliseconds) for a ping packet to travel from the controller to its target destination and back again. This number can vary significantly due to the random nature of packet routings and random loads on the controller and its destination.

To view the controller's existing ping configuration:

- 1 Select *Diagnostics > Ping* from the main menu.



- 2 Refer to the following information displayed within the Configuration tab:

Description	Displays the user assigned description of the ping test. The name is read-only. Use this title to determine whether this test can be used as is or if a new ping test is required.
Destination IP	Displays the IP address of the target device. This is the numeric destination for the device sent the ping packets. If this address does not accurately reflect the ping destination target, the ping test will not be successful.
Timeout (sec)	Displays the timeout value (in seconds) used to timeout the ping test if a round trip packet is not received from the target device.
No. of Probes	Displays the number of packets transmitted to the target IP address to discern the round trip time between the controller and its connected device.
Frequency	Define the interval (in seconds) between ping packet transmissions. Define a longer interval if high levels of network congestion are anticipated between the controller and its target device. Use a value of 0 to execute a single ping test or stop a currently executing ping test.

- 3 To edit the properties of an existing ping test, select a ping based on the description listed and click the *Edit* button. For more information, see [“Modifying the Configuration of an Existing Ping Test” on page 588](#).
- 4 Select an existing ping test from those displayed within the Configure tab and click the *Delete* button to remove the ping test from those displayed.
- 5 Click the *Add* button to display a screen used to define the attributes of a new ping test. For more information, see [“Adding a New Ping Test” on page 589](#).

Modifying the Configuration of an Existing Ping Test

The properties of an existing ping test can be modified to ping an existing (known) device whose network address attributes may have changed and require modification to connect (ping) to it.

To modify the attributes of an existing ping test:

- 1 Select *Diagnostics > Ping* from the main menu.
- 2 Highlight an existing ping test within the Configuration tab and select the *Edit* button.

- 3 Modify the following information (as needed) to edit the existing ping test:

Description	If necessary, modify the description for the ping test. Ensure this description is representative of the test, as this is the description displaying within the Configuration tab.
Destination IP	If necessary, modify the IP address of the target device. This is the numeric (non DNS address) destination for the device transmitted the ping packets.
No. of Probes	If necessary, modify the number of packets transmitted to the target IP address to discern the round trip time between the controller and its connected device.

Timeout(sec)	If necessary, modify the timeout value (in seconds) used to timeout the ping test if a round trip packet is not received by the controller from its target device. Ensure this interval is long enough to account for network congestion between the controller and its target device.
Frequency	If necessary, modify the interval (in seconds) between ping packet transmissions. Define a longer interval if high levels of network congestion are anticipated between the controller and its target device. Use a value of 0 to execute a single ping or stop a currently executing ping test.

- 4 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller.
- 6 Click *Cancel* to return to the Configuration tab without implementing changes.

Adding a New Ping Test

If the attributes of an existing ping test do not satisfy the requirements of a new connection test, and you do not want to modify an existing test, a new test can be created and added to the list of existing ping tests displayed within the Configuration tab.

To create a new ping test and add it to the list of existing tests:

- 1 Select *Diagnostics > Ping* from the main menu.
- 2 Click the *Add* button at the bottom of the Configuration tab.

3 Enter the following information to define the properties of the new ping test:

Test Name	Enter a short name for the ping test to describe either the target destination of the ping packet or the ping test's expected result. Use the name provided in combination with the ping test description to convey the overall function of the test.
Description	Ensure the description is representative of the test, as this is the description displaying within the Configuration tab.
Destination IP	Enter the IP address of the target device. This is the numeric (non DNS address) destination for the device transmitted the ping packets.
No. of Probes	Define the number of ping packets transmitted to the target device. This value represents the number of packets transmitted to the target IP address to discern the round trip time between the controller and its connected device.
Timeout(sec)	Configure the timeout value (in seconds) used to timeout the ping test if a round trip packet is not received from the target device. Ensure this interval is long enough to account for network congestion between the controller and its target device.
Frequency	Define the interval (in seconds) between ping packet transmissions. Define a longer interval if high levels of network congestion are anticipated between the controller and its target device. Use a value of 0 to execute a single ping test or stop a currently running ping test.

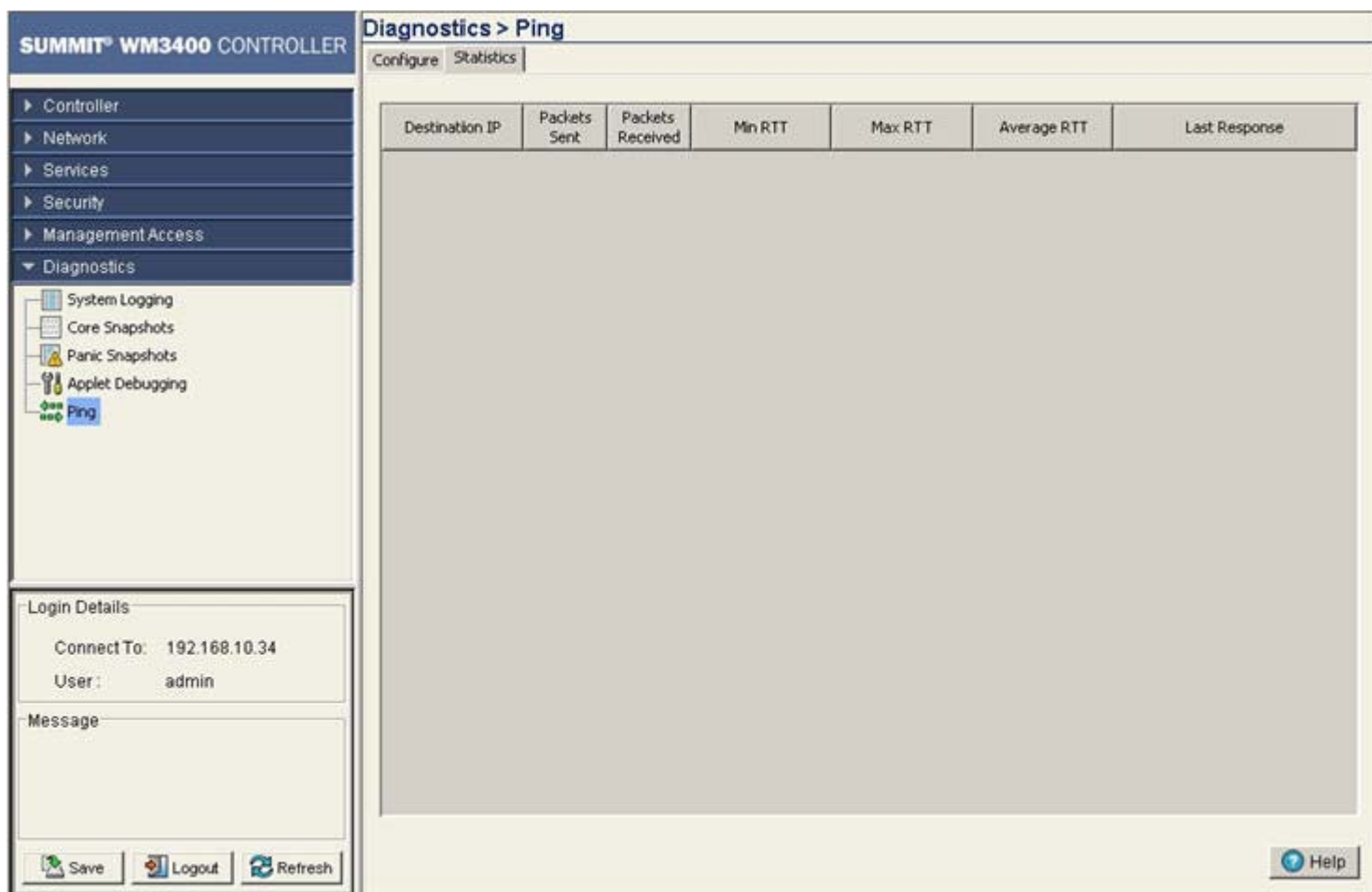
- 4 Click *OK* to save and add the changes to the running configuration and close the dialog.
- 5 Refer to the *Status* field for the current state of the requests made from the applet. This field displays error messages if something goes wrong in the transaction between the applet and the controller
- 6 Click *Cancel* to return back to the Configuration tab without implementing changes.

Viewing Ping Statistics

Refer to the Statistics tab for an overview of the overall success of the ping test with the destination IP addresses displayed within the screen. Use this information to determine whether the destination IP represents a device offering the controller a viable connection to either extend the controller's existing radio coverage area or provide support for additional MUs within an existing network segment.

To view ping test statistics:

- 1 Select *Diagnostics > Ping* from the main menu.
- 2 Select the *Statistics* tab.



- 3 Refer to the following content within the Statistics tab to assess the connection with the target device:

Destination IP	Displays the numeric (non DNS address) destination for the device transmitted the ping packets.
Packets Sent	Displays the number of packets transmitted to the target device IP address. Compare this value with the number of packets received to assess the connection quality with the target device.
Packets Received	Displays the number of packets received from the target device. If this number is significantly lower than the number sent to the target device, consider removing this device from consideration for permanent connection with the controller.
Min RTT	Displays the quickest round trip time for ping packets transmitted from the controller to its destination IP address. This may reflect the time when data traffic was at its lowest for the two devices.
Max RTT	Displays the longest round trip time for ping packets transmitted from the controller to its destination IP address. This may reflect the time when data traffic was at its most congested for the two devices.

Average RTT	Displays the average round trip time for ping packets transmitted between the controller and its destination IP address. Use this value as a general baseline (along with packets sent vs packets received) for the overall connection and association potential between the controller and target device.
Last Response	Displays the time (in seconds) the controller last “heard” the destination IP address over the controller managed network. Use this time (in contention with the RTT values displayed) to determine whether this device warrants a permanent controller connection.

A

APPENDIX

Customer Support



NOTE

Services can be purchased from Extreme Networks or through one of its channel partners. If you are an end-user who has purchased service through an Extreme Networks channel partner, please contact your partner first for support.

Extreme Networks Technical Assistance Centers (TAC) provide 24x7x365 worldwide coverage. These centers are the focal point of contact for post-sales technical and network-related questions or issues. TAC will create a Service Request (SR) number and manage all aspects of the SR until it is resolved. For a complete guide to customer support, see the *Technical Assistance Center User Guide* at:

www.extremenetworks.com/go/TACUserGuide

The Extreme Networks eSupport website provides the latest information on Extreme Networks products, including the latest Release Notes, troubleshooting, downloadable updates or patches as appropriate, and other useful information and resources. Directions for contacting the Extreme Networks Technical Assistance Centers are also available from the eSupport website at:

<https://esupport.extremenetworks.com>

Registration

If you have not already registered with Extreme Networks using a registration card supplied with your product, you can register on the Extreme Networks website at:

<http://www.extremenetworks.com/go/productregistration>.

Documentation

Check for the latest versions of documentation on the Extreme Networks documentation website at:

<http://www.extremenetworks.com/go/documentation>



Adaptive AP Overview

Adaptive AP Overview

An *adaptive AP* (AAP) is an AP3510, AP3550 or AP4700 Series Access Point that can adopt like an AP4600 Series device (Layer 3). The management of an AAP is conducted by the controller, once the Access Point connects to an Extreme Networks Summit WM3400, Summit WM3600 or Summit WM3700 model controller and receives its AAP configuration.

An AAP provides:

- local 802.11 traffic termination
- local encryption/decryption
- local traffic bridging
- the tunneling of centralized traffic to the wireless controller

An AAP's controller connection can be secured using IP/UDP or IPSec depending on whether a secure WAN link from a remote site to the central site already exists.

The controller can be discovered using one of the following mechanisms:

- DHCP
- Controller *fully qualified domain name* (FQDN)
- Static IP addresses

The benefits of an AAP deployment include:

- *Centralized Configuration Management & Compliance*—Wireless configurations across distributed sites can be centrally managed by the wireless controller or cluster.
- *WAN Survivability*—Local WLAN services at a remote sites are unaffected in the case of a WAN outage.
- *Securely extend corporate WLANs to stores for corporate visitors*—Small home or office deployments can utilize the feature set of a corporate WLAN from their remote location.
- *Maintain local WLANs for branch office applications*—WLANs created and supported locally can be concurrently supported with your existing infrastructure.

Where to Go From Here

Refer to the following for a further understanding of AAP operation:

- [Adaptive AP Management on page 596](#)
- [Licensing on page 596](#)
- [Controller Discovery on page 596](#)
- [Securing a Configuration Channel Between Controller and AP on page 598](#)
- [Adaptive AP WLAN Topology on page 598](#)
- [Configuration Updates on page 598](#)
- [Securing Data Tunnels between the Controller and AAP on page 599](#)
- [Adaptive AP Controller Failure on page 599](#)
- [Remote Site Survivability \(RSS\) on page 599](#)
- [Adaptive Mesh Support on page 599](#)

For an understanding of how AAP support should be configured for the Access Point and its connected controller, see [“How the AP Receives its Adaptive Configuration” on page 604](#).

For an overview of how to configure both the Access Point and controller for basic AAP connectivity and operation, see [“Establishing Basic Adaptive AP Connectivity” on page 605](#).

Adaptive AP Management

An AAP can be adopted, configured and managed like a thin Access Port from the wireless controller.



NOTE

Configuration changes made on the access point will not be updated on the controller. To change the AAP configuration for the access point, make the changes using the controller's interface.

Once an access point connects to a controller and receives its AAP configuration, its WLAN and radio configuration is similar to a thin access port. An AAP's radio mesh configuration can also be configured from the controller. However, non-wireless features (DHCP, NAT, Firewall etc.) cannot be configured from the controller and must be defined using the Access Point's resident interfaces before its conversion to an AAP.

Licensing

An AAP uses the same licensing scheme as a thin Access Port. This implies an existing license purchased with a controller can be used for an AAP deployment. Regardless of how many AP4600 Series Access Ports and/or AAPs are deployed, you must ensure the license used by the controller supports the number of radio ports (both AP4600 Series Access Ports and AAPs) you intend to adopt.

Controller Discovery

For an access point to function as an AAP (regardless of mode), it needs to connect to a controller to receive its configuration. There are two methods of controller discovery:

- [Auto Discovery using DHCP on page 597](#)

- [Manual Adoption Configuration on page 598](#)

Auto Discovery using DHCP

Extended Global Options 189, 190, 191, 192 can be used or Embedded Option 43—Vendor Specific options can be embedded in Option 43 using the vendor class identifier.

Table 5: Vendor-Specific Options

	Code	Data Type
List of Controller IP addresses (<i>separate by comma, semi-colon, or space delimited</i>)	189	String
Controller FQDN	190	String
AP35xx Encryption IPsec Passphrase (Hashed)**	191	String
AP35xx controller discovery mode 1 = auto discovery enable 2 = auto discover enabled (using IPsec)	192	String

** The Access Point uses an encryption key to hash passphrases and security keys. To obtain the encryption passphrase, configure an Access Point with the passphrase and export the configuration file

```

/
enc-admin-passwd d2
/
// System Configuration
/
system
set name AP-35x0
set loc \0
set email \0
set cc us
/
system
aap-setup
// Adaptive AP menu
set auto-discovery disable
set interface lan1
set name \0
set port 24576
delete all
set enc-passphrase bf0819993a702c39
set ac-keepalive 5
set tunnel-to-switch enable
/
// System-Access menu
system
access
set applet lan 1 enable
set applet slan 1 enable
set cli lan 1 enable
set ssh lan 1 enable
set snmp lan 1 enable
set applet lan 2 enable
set applet slan 2 enable
set cli lan 2 enable
set ssh lan 2 enable
set snmp lan 2 enable
set admin-auth radius
set applet wan enable

```

Encrypted Passphrase to be used in DHCP Option

Manual Adoption Configuration

A manual controller adoption of an AAP can be conducted using:

- *Static FQDN*—A controller fully qualified domain name can be specified to perform a DNS lookup and controller discovery.
- *Static IP addresses*—Up to 12 controller IP addresses can be manually specified in an ordered list the AP can choose from. When providing a list, the AAP tries to adopt based on the order in which they are listed (from 1-12).



NOTE

An AAP can use its LAN or WAN Ethernet interface to adopt. The LAN is PoE and DHCP enabled by default.

The WAN has no PoE support and has a default static AP address of 10.1.1.1/8.

Securing a Configuration Channel Between Controller and AP

Once an Access Point obtains a list of available controllers, it begins connecting to each. The controller can be either on the LAN or WAN side of the Access Point to provide flexibility in the deployment of the network. If the controller is on the Access Point's LAN, ensure the LAN subnet is on a secure channel. The AP will connect to the controller and request a configuration.

Adaptive AP WLAN Topology

An AAP can be deployed in the following WLAN topologies:

- *Extended WLANs*—Extended WLANs are the centralized WLANs created on the controller
- *Independent WLANs*—Independent WLANs are local to an AAP and can be configured from the controller. You must specify a WLAN as independent to stop traffic from being forwarded to the controller. Independent WLANs behave like WLANs on a standalone Access Point.
- *Both*—Extended and independent WLANs are configured from the controller and operate simultaneously.



NOTE

For a review of some important considerations impacting the use of extended and independent WLANs within an AAP deployment, see [Adaptive AP Deployment Considerations](#).

Configuration Updates

An AAP receives its configuration from the controller initially as part of its adoption sequence. Subsequent configuration changes on the controller are reflected on an AAP when applicable.

An AAP applies the configuration changes it receives from the controller after 30 seconds from the last received controller configuration message. When the configuration is applied on the AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds) forcing associated MUs to be deauthenticated. MUs are quickly able to associate.

Securing Data Tunnels between the Controller and AAP

If a secure link (site-to-site VPN) from a remote site to the central location already exists, the AAP does not require IPsec to be configured for adoption.

For sites with no secure link to the central location, an AAP can be configured to use an IPsec tunnel (with AES 256 encryption) for adoption. The tunnel configuration is automatic on the AAP side and requires no manual VPN policy to be configured. On the controller side, configuration updates are required to adopt the AAP using an IPsec tunnel.

To review a sample AAP configuration, see *“Sample Controller Configuration File for IPsec and Independent WLAN” on page 612*.

Adaptive AP Controller Failure

In the event of a controller failure, an AAP's independent WLAN continues to operate without disruption. The AAP attempts to connect to other controllers (if available) in background. Extended WLANs are disabled once controller adoption is lost. When a new controller is discovered and a connection is secured, an extended WLAN can be enabled.

If a new controller is located, the AAP synchronizes its configuration with the located controller once adopted. If *Remote Site Survivability (RSS)* is disabled, the independent WLAN is also disabled in the event of a controller failure.

Remote Site Survivability (RSS)

RSS can be used to turn off RF activity on an AAP if it loses adoption (connection) to the controller.

Table 6: RF Activity Options

RSS State	Independent WLANs	Extended WLANs
RSS Enabled	WLAN continues beaconing	WLAN continues beaconing but AP does not allow clients to associate on that WLAN
RSS Disabled	WLAN stops beaconing	WLAN stops beaconing

Adaptive Mesh Support

An AAP can extend an Access Point's existing mesh functionality to a controller managed network. All mesh APs are configured and managed through the wireless controller. APs without a wired connection form a mesh backhaul to a repeater or a wired mesh node and then get adopted to the controller. Mesh nodes with existing wired access get adopted to the controller like a wired AAP.

Mesh AAPs apply configuration changes 180 seconds after the last received controller configuration message. When the configuration is applied on the Mesh AAP, the radios shutdown and re-initialize (this process takes less than 2 seconds), forcing associated MUs to be deauthenticated and the Mesh link will go down. MUs are able to quickly associate, but the Mesh link will need to be re-established before MUs can pass traffic. This typically takes about 90 to 180 seconds depending on the size of the mesh topology.



NOTE

When mesh is used with AAPs, the "ap-timeout" value needs to be set to a higher value (for example, 180 seconds) so Mesh AAPs remain adopted to the controller during the period when the configuration is applied and mesh links are re-established.

Configuring Adaptive AP Mesh. To configure mesh support for Adaptive AP:

- 1 Go to Network > Access Point Radios and click the Global Settings button.

Network > Wireless LANs > Global WLAN Settings

Global WLAN Settings

Global

MU Proxy ARP handling

Shared-Key Authentication

Manual mapping of WLANs

Enable WLAN Bandwidth Settings

MU Rate Limiting UP (0, 100 - 1000000) kbps

MU Rate Limiting Down (0, 100 - 1000000) kbps

MU Load Balance Mode Count By Throughput

Status:

OK Cancel Help

- 2 Uncheck the Adopt Unconfigured Radios Automatically option to prevent the controller from automatically adopting new APs when they are connected to the controller.
- 3 Configure the client bridge back haul WLAN, base bridge and client bridge radios on the controller using the Command Line Interface (CLI) commands listed below.

Client Bridge Back Haul WLAN Configuration:

```
WMController(config-wireless)#wlan 1 enable
WMController(config-wireless)#wlan 1 ssid meshWlan
WMController(config-wireless)#wlan 1 independent
WMController(config-wireless)#wlan 1 client-bridge-backhaul enable
```

Base Bridge Radio Configuration: (AP35xx that is wired to the controller)

```
WMController(config-wireless)#radio add 1 "base bridge radio mac" 11bg ap35xx
WMController(config-wireless)#radio add 2 "base bridge radio mac" 11a ap35xx
WMController(config-wireless)#radio 1 base-bridge enable
WMController(config-wireless)#radio 1 bss 1 1
(map the mesh WLAN if manual mapping is enabled, not needed otherwise)
```

Client Bridge Radios Configuration: (AP35xx's that are wirelessly connected)

```
WMController(config-wireless)#radio add 3 "client bridge radio mac" 11bg ap35xx
WMController(config-wireless)#radio add 4 "client bridge radio mac" 11a ap35xx
WMController(config-wireless)#radio 3 client-bridge enable
WMController(config-wireless)#radio 3 client-bridge ssid meshWlan
WMController(config-wireless)#radio 3 bss 1 1
(map the mesh WLAN if manual mapping is enabled, not needed otherwise)
```

- 4 Configure Adaptive AP support on the Access Point by adopting the APs base bridge as well as client bridge. The client-bridge radios must be wired directly wired to the controller during this configuration step.
- 5 Once all APs are adopted, wait for 3 minutes. After 3 minutes disconnect the client-bridge Access Points from the network. The client bridge Access Points will continue to be adopted.

AAP RADIUS Proxy Support

When an Adaptive AP is adopted to a central controller over a WAN Link, the controller configures the Adaptive AP for a WLAN with RADIUS authentication from a RADIUS server residing at the central site. When the Adaptive AP gets a RADIUS MU associated, it sends the RADIUS packets on the wired side with its own IP Address as the source IP of the request and the Destination IP Address of the RADIUS Server. In a local network implementation, the Adaptive APs, controller and RADIUS Servers are all on the same LAN and the routing works fine. However, when the Adaptive AP is adopted over a WAN link, the RADIUS Server IP Address will be an internal address which is non-routable over the Internet.

To access the RADIUS server's non-routable IP address over the WAN, you have the option to configure Adaptive AP RADIUS Proxying for the WLAN. When this flag is enabled, the Adaptive AP is reconfigured to send all RADIUS traffic to the controller and the controller does the proxying to the real RADIUS server to handle authentication. The controller automates the process of handling RADIUS proxy configuration and client configurations. The controller supports only one real RADIUS server configuration without the presence of realm information. To support multiple RADIUS servers, a realm has to be associated with the real RADIUS server.

When AAP RADIUS proxying is enabled without specifying a realm, the controller can no longer process requests on the on-board RADIUS server. You cannot authenticate using the on-board RADIUS server any longer because all authentications done by users without a realm are forwarded to the external RADIUS server, as configured for the WLAN with Adaptive AP RADIUS Proxy.



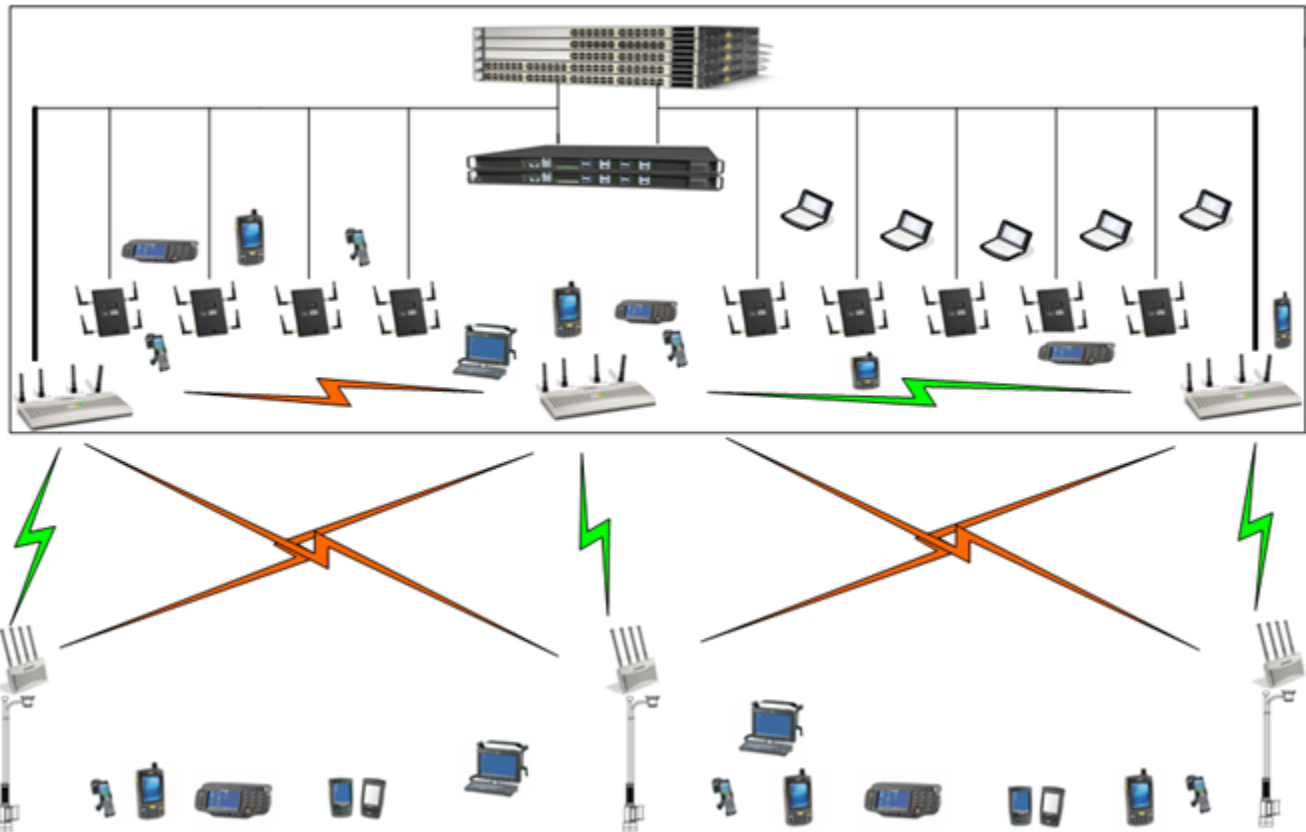
NOTE

The Extreme Networks wireless LAN controllers support Adaptive AP RADIUS proxy without specifying realm information. If AP Proxy RADIUS is enabled without specifying realm information, the internal RADIUS server can no longer be used to authenticate users. If Proxy RADIUS is enabled for a WLAN with realm configured, then the internal RADIUS server can perform as usual.



NOTE

If AAP Proxy RADIUS is configured, the onboard RADIUS server has to be enabled. By default the onboard RADIUS server is disabled. To enable the onboard RADIUS server use the Web UI or issue the "service RADIUS" command in the CLI.



Supported Adaptive AP Topologies

The following AAP topologies are supported:

- [Extended WLANs Only on page 603](#)
- [Independent WLANs Only on page 603](#)
- [Extended WLANs with Independent WLANs on page 603](#)
- [Extended VLAN with Mesh Networking on page 603](#)

Topology Deployment Considerations

When reviewing the AAP topologies described in the section, be cognizant of the following considerations to optimize the effectiveness of the deployment:

- An AAP firmware upgrade will not be performed at the time of adoption from the wireless controller. Instead, the firmware is upgraded using the AP-51x1's firmware update procedure (manually or using the DHCP Auto Update feature).
- An AAP can use its LAN1 interface or WAN interface for adoption. The default gateway interface is set to LAN1. If the WAN Interface is used, explicitly configure WAN as the default gateway interface.
- Extreme Networks recommends using the LAN1 interface for adoption in multi-cell deployments.

-
- If you have multiple independent WLANs mapped to different VLANs, the AAP's LAN1 interface requires trunking be enabled with the correct management and native VLAN IDs configured. Additionally, the AAP needs to be connected to a 802.1q trunk port on the wired controller.
 - Be aware IPSec Mode supports NAT Traversal (NAT-T).

Extended WLANs Only

An extended WLAN configuration forces all MU traffic through the controller. No wireless traffic is locally bridged by the AAP.

Each extended WLAN is mapped to the Access Point's virtual LAN2 subnet. By default, the Access Point's LAN2 is not enabled and the default configuration is set to static with IP addresses defined as all zeros. If the extended VLAN option is configured on the controller, the following configuration updates are made automatically:

- The AAP's LAN2 subnet becomes enabled.
- All extended VLANs are mapped to LAN2.



NOTE

MUs on the same WLAN associated to the AAP can communicate locally at the AP Level without going through the controller. If this scenario is undesirable, the Access Point's MU-to-MU disallow option should be enabled.

Independent WLANs Only

An independent WLAN configuration forces all MU traffic to be bridged locally by the AAP. No wireless traffic is tunneled back to the controller. Each extended WLAN is mapped to the Access Point's LAN1 interface. The only traffic between the controller and the AAP are control messages (for example, heartbeats, statistics and configuration updates).

Extended WLANs with Independent WLANs

An AAP can have both extended WLANs and independent WLANs operating in conjunction. When used together, MU traffic from extended WLANs go back to the controller and traffic from independent WLANs is bridged locally by the AP.

All local WLANs are mapped to LAN1, and all extended WLANs are mapped to LAN2.

Extended VLAN with Mesh Networking

Mesh networking is an extension of the existing wired network. There is no special configuration required, with the exception of setting the mesh and using it within one of the two extended VLAN configurations.

**NOTE**

The mesh backhaul WLAN must be an independent WLAN mapped to LAN2. The controller enforces the WLAN be defined as an independent WLAN by automatically setting the WLAN to independent when backhaul is selected. The AP ensures the backhaul WLAN be put on LAN1.

How the AP Receives its Adaptive Configuration

An AAP does not require a separate "local" or "running" configuration. Once enabled as an AAP, the AP obtains its configuration from the controller. If the AP's WAN link fails, it continues to operate using the last valid configuration until its link is re-established and a new configuration is pushed down from the controller. There is no separate file-based configuration stored on the controller.

Only WLAN, VLAN extension and radio configuration items are defined for the AAP by its connected controller. None of the other Access Point configuration items (RADIUS, DHCP, NAT, Firewall etc.) are configurable from the connected controller.

After the AP downloads a configuration file from the controller, it obtains the version number of the image it should be running. The controller does not have the capacity to hold the Access Point's firmware image and configuration. The Access Point image must be downloaded using a means outside the controller. If there is still an image version mismatch between what the controller expects and what the AAP is running, the controller will deny adoption.

**NOTE**

When configuring wireless settings for Adaptive APs all configuration must be done through the controller and not from the AP management console. Making changes directly in the AP management console can lead to unstable operation of the Adaptive AP.

Adaptive AP Prerequisites

Converting an Access Point into an AAP requires:

- A version 2.0 or higher firmware running on the Access Point.
- An Extreme Networks wireless LAN controller.
- The appropriate controller licenses providing AAP functionality on the controller.
- The correct password to authenticate and connect the adaptive to the controller.

Configuring the Adaptive AP for Adoption by the Controller

An AAP needs to find and connect to the controller. To ensure this connection:

- Configure the controller's IP address on the AAP
 - Provide the controller IP address using DHCP option 189 on a DHCP server. The IP address is a comma delimited string of IP addresses. For example "157.235.94.91, 10.10.10.19". There can be a maximum of 12 IP addresses.
 - Configure the controller's FQDN on the AAP. The AAP can use this to resolve the IP address of the controller.
- 6 Use the controller's secret password on the AAP for the controller to authenticate it.
- To avoid a lengthy broken connection with the controller, Extreme Networks recommends generating an SNMP trap when the AAP loses adoption with the controller.



NOTE

For additional information (in greater detail) on the AP configuration activities described above, see ["Adaptive AP Configuration" on page 606](#).

Configuring the Controller for Adaptive AP Adoption

The tasks described below are configured on an Extreme Networks wireless LAN controller. For information on configuring the controller for AAP support, see <https://esupport.extremenetworks.com>

To adopt an AAP on a controller:

- 1 Ensure enough licenses are available on the controller to adopt the required number of AAPs.
- 2 As soon as the AAP displays in the adopted list:
Adjust each AAP's radio configuration as required. This includes WLAN-radio mappings and radio parameters. WLAN-VLAN mappings and WLAN parameters are global and cannot be defined on a per radio basis. WLANs can be assigned to a radio as done today for an AP4600 Series Access Port. Optionally, configure WLANs as independent and assign to AAPs as needed.
- 3 Configure each VPN tunnel with the VLANs to be extended to it.
If you do not attach the target VLAN, no data will be forwarded to the AAP, only control traffic required to adopt and configure the AP.



NOTE

For additional information (in greater detail) on the controller configuration activities described above, see [Controller Configuration](#).

Establishing Basic Adaptive AP Connectivity

This section defines the activities required to configure basic AAP connectivity with the controller. In establishing a basic AAP connection, both the Access Point and controller require modifications to their respective default configurations. For more information, see:

- [Adaptive AP Configuration on page 606](#)

-
- [Controller Configuration on page 609](#)



NOTE

Refer to [Adaptive AP Deployment Considerations](#) for usage and deployment caveats that should be considered before defining the AAP configuration. Refer to [Sample Controller Configuration File for IPSec and Independent WLAN](#) if planning to deploy an AAP configuration using IPSec VPN and an extended WLAN.

Adaptive AP Configuration

An AAP can be manually adopted by the controller, adopted using a configuration file (consisting of the adaptive parameters) pushed to the Access Point or adopted using DHCP options. Each of these adoption techniques is described in the sections that follow.

Adopting an Adaptive AP Manually

There are two methods to manually enable the Access Point's controller discovery for adoption: Access Point CLI and Access Point web GUI. The AP CLI is available to APs and the AP web GUI is currently unavailable on APs with AP firmware v2.4.

Using Access Point CLI.

The following script shows an example with basic steps for setting up the AAP discovery for controller adoption:

```
*****
ADP-35xx Access Point 2.4.1.0-008R

(none) login: admin
Password:

admin>system
admin(system)>aap
admin(system.aap-setup)>set auto-discovery enable(enable controller discovery)
admin(system.aap-setup)>set interface lan1(lan1 or lan2 of the access point WLAN port)
admin(system.aap-setup)>set ipadr 1 10.255.108.37(the 1st controller IP address. up to
12 controllers may be listed.
admin(system.aap-setup)>save
admin(system.aap-setup)>show(show ap adoption status)

Auto Discovery Mode           : enable
Controller Interface          : lan1
Controller Name               :
Static IP Port                : 24576
Static IP Addresses:
IP Address 1                  : 10.255.108.37
IP Address 2                  : 0.0.0.0
IP Address 3                  : 0.0.0.0
IP Address 4                  : 0.0.0.0
IP Address 5                  : 0.0.0.0
IP Address 6                  : 0.0.0.0
IP Address 7                  : 0.0.0.0
IP Address 8                  : 0.0.0.0
```

```

IP Address 9           : 0.0.0.0
IP Address 10          : 0.0.0.0
IP Address 11          : 0.0.0.0
IP Address 12          : 0.0.0.0

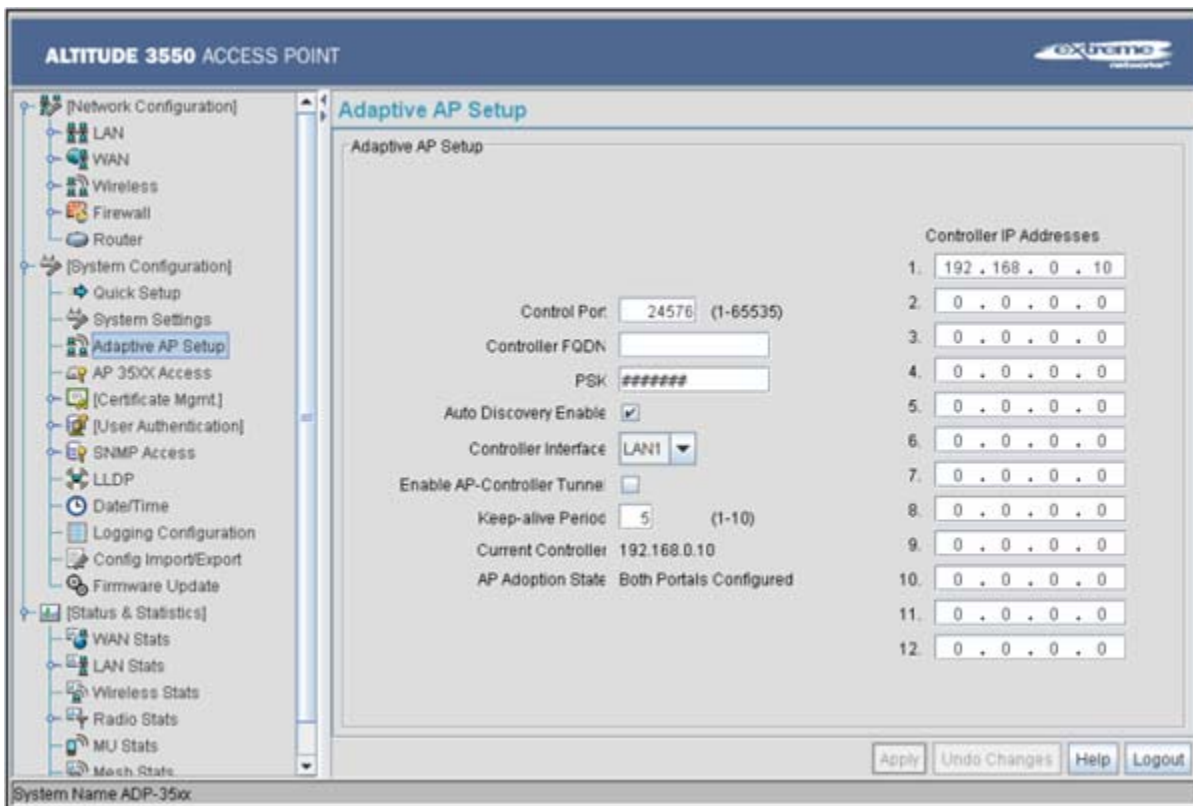
Tunnel to Controller  : disable
AC keepalive           : 5
Load Balancing         : enable

Current Controller     : 10.255.108.37
AP Adoption State      : AAP adopted, Both Portals Configured(adoption
successful)

```

Using Access Point Web GUI if Available.

- 1 Select *System Configuration -> Adaptive AP Setup* from the Access Point's menu tree.



- 2 Select the *Auto Discovery Enable* checkbox.

Enabling auto discovery will allow the AAP to be detected by a controller once its connectivity medium has been configured (by completing steps 3-6).



NOTE

Auto discovery must be enabled for a controller to detect an AP.

- 3 Enter up to 12 *Controller IP Addresses* constituting the target controllers available for AAP connection. The AAP will begin establishing a connection with the first addresses in the list. If unsuccessful, the AP will continue down the list (in order) until a connection is established.
- 4 If a numerical IP address is unknown, but you know a controller's *fully qualified domain name* (FQDN), enter the name as the *Controller FQDN* value.
- 5 Select the *Enable AP-Controller Tunnel* option to allow AAP configuration data to reach a controller using a secure VPN tunnel.
- 6 If using IPsec as the tunnel resource, enter the IPsec *Passkey* to ensure IPsec connectivity.
- 7 Click *Apply* to save the changes to the AAP setup.



NOTE

The manual AAP adoption described above can also be conducted using the Access Point's CLI interface using the *admin(system.aapsetup)>* command.

Adopting an Adaptive AP Using a Configuration File

To adopt an AAP using a configuration file:

- 1 Refer to "*Adopting an Adaptive AP Manually*" on page 606 and define the AAP controller connection parameters.
- 2 Export the AAP's configuration to a secure location.

Either import the configuration manually to other APs or the same AP later (if you elect to default its configuration). Use DHCP option 186 and 187 to force a download of the configuration file during startup (when it receives a DHCP offer).



NOTE

When an Adaptive AP is adopted over an IP Sec Tunnel you cannot export the configuration file to a system on the other side of the IP Sec Tunnel. You may still export the configuration file to a system local to the AAP.

Adopting an Adaptive AP Using DHCP Options

An AAP can be adopted to a wireless controller by providing the following options in the DHCP Offer:

Table 7: Adoption Options

Option	Data Type	Value
189	String	<Controller IP Address or Range of IP addresses separated by [, ; <space>]>
190	String	<Fully qualified Domain Name for the Wireless Controller>
191	String	<Hashed IPsec Passkey - configure on 1 AP and export to get hashed key>
192	String	<Value of "1" denotes enabling auto discovery for controllers with Non-IPsec mode and "2" with IPsec mode>



NOTE

Options 189 and 192 are mandatory to trigger adoption using DHCP options. Unlike an AP4600 Series Access Port, option 189 alone won't work. These options can be embedded in Vendor Specific Option 43 and sent in the DHCP Offer.

Controller Configuration

An Extreme Networks wireless LAN controller requires an explicit adaptive configuration to adopt an Access Point (if IPSec is not being used for adoption). The same licenses currently used for an AP4600 Series Access Port adoption can be used for an AAP.

Disable the controller's *Adopt unconfigured radios automatically* option and manually add AAPs requiring adoption, or leave as default. In default mode, any AAP adoption request is honored until the current controller license limit is reached.

To disable automatic adoption on the controller:

- 1 Select *Network > Access Point Radios* from the controller main menu tree.
- 2 Select the *Configuration* tab (should be displayed by default) and click the *Global Settings* button.

Network > Access Point Radios > Global

Global

Controller Adoption Preference ID (1 - 65535)

Adopt unconfigured radios automatically

Voice Call Admission Control

Primary WIPS Server Address

Secondary WIPS Server Address

Status:

- 3 Ensure the *Adopt unconfigured radios automatically* option is NOT selected.
- 4 When disabled, there is no automatic adoption of non-configured radios on the network. Additionally, default radio settings will NOT be applied to Access Ports/Points when automatically adopted.



NOTE

For IPsec deployments, refer to [“Sample Controller Configuration File for IPsec and Independent WLAN”](#) on page 612 and take note of the CLI commands in red and associated comments in green.

Any WLAN configured on the controller becomes an extended WLAN by default for an AAP.

- 5 Select *Network > Wireless LANs* from the controller main menu tree.
- 6 Select the target WLAN you would like to use for AAP support from those displayed and click the *Edit* button.
- 7 Select the *Independent Mode (AAP Only)* checkbox.

Selecting the checkbox designates the WLAN as independent and prevents traffic from being forwarded to the controller. Independent WLANs behave like WLANs as used on a standalone Access Point. Leave this option unselected (as is by default) to keep this WLAN an extended WLAN (a typical centralized WLAN created on the controller).

Network > Wireless LANs > Edit WLAN2

Edit

Configuration

ESSID: Description:

Deny Static MU Enable URL Logging Independent Mode(AAP Only) Client Bridge Backhaul

Enter a list (e.g: 1,3,7) or range (e.g: 3-7) of indices.
VLAN ID:
 Dynamic Assignment

802.11w-PMF:
SA Query Max Timeout: (100 - 6000 msec)
SA Query Retry Timeout: (10 - 1500 msec)

Authentication

802.1X EAP
 Kerberos
 Hotspot
 MAC Authentication
 No Authentication

Encryption

WEP 64
 WEP 128
 KeyGuard
 WPA/WPA2-TKIP
 WPA2-CCMP

Advanced

Accounting Mode:
 Answer Broadcast ESS
 Use Voice Prioritization

MU to MU Traffic:
MU Idle Time: seconds
Access Category:



NOTE

Additionally, a WLAN can be defined as independent using the "*wlan <index> independent*" command from the config-wireless context.



NOTE

For AAP to work properly with Summit WM3000 Series Controllers you need to have independent and extended WLANs mapped to a different VLAN than the ge port.

Once an AAP is adopted by the controller, it displays within the controller *Access Point Radios* screen (under the Network parent menu item) as an AP3510, AP3550 or AP4700 Series within the *AP Type* column.

SUMMIT® WM3600 CONTROLLER

Network > Access Point Radios

Configuration | Statistics | WLAN Assignment | WMM | Bandwidth | Group | VCAC Statistics | Mesh Statistics | Smart RF | Voice Statistics

Unconfigured radios are automatically adopted, use "Global Settings" to change this option.

Show Filtering Options <<< Page 1 of 1 Go >>>

Index	Description	AP Type	Type	Adopted	Parent AP MAC Address	MAC Address	State	VLAN
1	RADIO1	AP3510	802.11a	✓	00-04-96-43-50-70	00-04-96-43-50-C0	Normal	None
2	RADIO2	AP3510	802.11bg	✓	00-04-96-43-50-70	00-04-96-43-50-D0	Normal	None

Filtering is disabled Page 1 of 1 loaded.

Properties

Desired Channel	--	Desired Power (dBm)	--	Placement	--	Secondary Channel	--
AP Manufacturer	Extreme Networks	BSSIDs	--	AP IP Address	--		
Actual Channel	--	Actual Power	--	Last Adopted	--	Voice Calls	--

Save Logout Refresh Edit Delete Add Tools > AP Mesh Global Settings Help

Adaptive AP Deployment Considerations

Before deploying your controller/AAP configuration, refer to the following usage caveats to optimize its effectiveness:

- Extended WLANs are mapped to the AP's LAN2 interface and all independent WLANs are mapped to the AP's LAN1 Interface.
- If deploying multiple independent WLANs mapped to different VLANs, ensure the AP's LAN1 interface is connected to a trunk port on the Layer 2/Layer 3 controller and appropriate management and native VLANs are configured.
- The WLAN used for mesh backhaul must always be an independent WLAN.
- The controller configures an AAP. If manually changing wireless settings on the AP, they are not updated on the controller. It's a one way configuration, from the controller to the AP.
- An AAP always requires a router between the AP and the controller.
- An AAP can be used behind a NAT.
- An AAP uses UDP port 24576 for control frames and UDP port 24577 for data frames.
- Multiple VLANs per WLAN, Layer 3 mobility, NAC, and self healing are some of the important wireless features not supported in an AAP supported deployment.

Sample Controller Configuration File for IPSec and Independent WLAN

The following constitutes a sample controller configuration file supporting an AAP IPSec with Independent WLAN configuration. Please note new AAP specific CLI commands in **red** and relevant comments in **blue**.

The sample output is as follows:

```
!  
! configuration of WM3600  
!  
version 1.0  
!  
!  
aaa authentication login default none  
service prompt crash-info  
!  
hostname WM3600-1  
!  
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d  
username admin privilege superuser  
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f  
!  
!  
To configure the ACL to be used in the CRYPTO MAP  
!  
ip access-list extended AAP-ACL permit ip host 10.10.10.250 any rule-precedence 20  
!  
spanning-tree mst cisco-interoperability enable  
spanning-tree mst config  
name My Name  
!
```

```

wlan 5 client-bridge-backhaul enable
wlan 6 enable
wlan 6 ssid test-mesh
wlan 6 vlan 250
radio add 1 00-15-70-00-79-30 11bg aap35xx
radio 1 bss 1 3
radio 1 bss 2 4
radio 1 bss 3 2
radio 1 channel-power indoor 11 8
radio 1 rss enable
radio add 2 00-15-70-00-79-30 11a aap35xx
radio 2 bss 1 5
radio 2 bss 2 1
radio 2 bss 3 2
radio 2 channel-power indoor 48 8
radio 2 rss enable
radio 2 base-bridge max-clients 12
radio 2 base-bridge enable
radio add 3 00-15-70-00-79-12 11bg aap35xx
radio 3 bss 1 3
radio 3 bss 2 4
radio 3 bss 3 2
radio 3 channel-power indoor 6 8
radio 3 rss enable
radio add 4 00-15-70-00-79-12 11a aap35xx
radio 4 bss 1 5
radio 4 bss 2 6
radio 4 channel-power indoor 48 4
radio 4 rss enable
radio 4 client-bridge bridge-select-mode auto
radio 4 client-bridge ssid Mesh
radio 4 client-bridge mesh-timeout 0
radio 4 client-bridge enable
radio default-11a rss enable
radio default-11bg rss enable
radio default-11b rss enable
no ap-ip default-ap controller-ip
!
radius-server local
!
To create an IPSEC Transform Set
!
crypto ipsec transform-set AAP-TFSET esp-aes-256 esp-sha-hmac mode tunnel
!
To create a Crypto Map, add a remote peer, set the mode, add a ACL rule to match and
transform and set to the Crypto Map
!
crypto map AAP-CRYPTOMAP 10 ipsec-isakmp
set peer 255.255.255.255
match address AAP-ACL
set transform-set AAP-TFSET
!
interface gel
controllerport mode trunk
controllerport trunk native vlan 1
controllerport trunk allowed vlan none

```

```

controllerport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
controllerport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge2
controllerport access vlan 1
!
interface ge3
controllerport mode trunk
controllerport trunk native vlan 1
controllerport trunk allowed vlan none
controllerport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
controllerport trunk allowed vlan add 180,190,200,210,220,230,240,250,
static-channel-group 1
!
interface ge4
controllerport access vlan 1
!
interface me1
ip address dhcp
!
interface sa1
controllerport mode trunk
controllerport trunk native vlan 1
controllerport trunk allowed vlan none
controllerport trunk allowed vlan add 1-9,100,110,120,130,140,150,160,170,
controllerport trunk allowed vlan add 180,190,200,210,220,230,240,250,
!
!
!
!
interface vlan1
ip address dhcp
!
To attach a Crypto Map to a VLAN Interface
!
crypto map AAP-CRYPTOMAP
!
sole
!
ip route 157.235.0.0/16 157.235.92.2
ip route 172.0.0.0/8 157.235.92.2
!
ntp server 10.10.10.100 prefer version 3
line con 0
line vty 0 24
!
end

```





Troubleshooting Information

This appendix provides basic troubleshooting information and workarounds to known conditions the user may encounter. Wherever possible, it includes possible suggestions or solutions to resolve the issues. It is divided into the following section:

- [General Troubleshooting on page 617](#)
- [Troubleshooting SNMP Issues on page 623](#)
- [Security Issues on page 624](#)

General Troubleshooting

This section describes common system issues and what to look for while diagnosing the cause of a problem.

The following information is included:

- [Wireless Controller Issues](#)
- [Access Port/Point Issues](#)
- [Mobile Unit Issues](#)
- [Miscellaneous Issues](#)
- [System Logging Mechanism](#)

Wireless Controller Issues

This section describes various issues that may occur when working with an Extreme Networks wireless LAN controller. Possible issues include:

- [Controller Does Not Boot Up](#)
- [Controller Does Not Obtain an IP Address through DHCP](#)
- [Unable to Connect to the Controller using Telnet or SSH](#)
- [Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond](#)
- [Console Port is Not Responding](#)

Controller Does Not Boot Up

The Extreme Networks wireless LAN controller does not boot up to a username prompt via CLI console or Telnet.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Controller has no power	<ul style="list-style-type: none">• Verify power cables, fuses, UPS power. The front panel LEDs lights up when power is applied to the controller.• Have a qualified electrician check the power source to which the controller is connected.
All else...	Contact Extreme Networks Support.

Controller Does Not Obtain an IP Address through DHCP

An Extreme Networks wireless LAN controller requires a routable IP address for the administrator to manage it via Telnet, SSH or a Web browser.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
DHCP is not configured, or not available on same network as the Extreme Networks wireless LAN controller	<ul style="list-style-type: none">• Verify the configuration for the controller has DHCP enabled. By default, the ports have DHCP enabled. Otherwise, refer to the <i>Summit WM3000 Series Controller CLI Reference Guide, Software Version 4.3</i> or the <i>Summit WM3000 Series Controller System Reference Guide, Software Version 4.3</i> for instructions on enabling the controller interfaces.• Connect another host configured for DHCP and verify it is getting a DHCP address
DHCP is not enabled on a Gigabit Ethernet interface	<ul style="list-style-type: none">• Enable DHCP for the port by using the CLI command or the Web UI to enable DHCP on the port connected to your external network.• Verify that DHCP packets are being sent to the port using a sniffer tool• If DHCP packets are seen, check to ensure that the controller is not configured for a static IP on the port.
All else...	Contact Extreme Networks Support.

Unable to Connect to the Controller using Telnet or SSH

The Extreme Networks wireless LAN controller is physically connected to the network, but connecting to the controller using SSH or Telnet does not work.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Telnet is not enabled and/or SSH is disabled	Verify Telnet or SSH are enabled by using the CLI or Web UI (By default, telnet is disabled.)
Max sessions have been reached	Maximum allowed sessions is 8 concurrent users connected to a controller. Verify the threshold has not been reached.
Primary LAN is not receiving Telnet or SSH traffic	Verify Telnet and SSH traffic is allowed on the primary VLAN.

Possible Problem	Suggestions to Correct
All else...	Contact Extreme Networks Support.

Web UI is Sluggish, Does Not Refresh Properly, or Does Not Respond

When configuring the controller, it is easy to overlook the fact that the host computer is running the browser while the Extreme Networks wireless LAN controller is providing the data to the browser. Occasionally, while using the Web UI the controller does not respond or appears to be running very slow; this could be a symptom of the host computer or the network, and not the controller itself. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Bad connection between controller and console system	Verify the line between the controller and the host computer is functioning normally.
Slow transmission of data packets	Verify the data packets are being sent to and from the controller using a sniffer tool.
Access Ports/Points may try to adopt while country code is not set	Set the country name for the controller, which is set to “none” by default.
Packet storm	Check Syslog for any type of a packet storm.
Overburdened with a large number of Access Ports/Points	With large numbers of Access Ports/Points, changing the configuration quickly may cause the controller to not refresh properly, at least immediately following configuration.
Java JRE is out of date	Be sure you are using Sun Java JRE 1.5 or later. To download the appropriate for your system go to: http://www.sun.com/java/
Cannot access Web UI through a Firewall	To successfully access the controller Web UI through a firewall, UDP port 161 must be open in order for the controller’s SNMP backend to function.
All else...	Contact Extreme Networks Support.

Console Port is Not Responding

The Extreme Networks wireless LAN controller console port is connected to the host computer’s serial port, but pressing the [Enter] key gets no response from the controller.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Cabling issue	Ensure a console cable is connected from the console port to the host computer’s serial port.
Not using a terminal emulation program	Verify a serial terminal emulation program, such as HyperTerminal, is in use on the host computer.

Possible Problem	Suggestions to Correct														
Settings in terminal emulation program are incorrectly set	<p>Check the serial port settings in the serial terminal emulation program being used. The correct settings are:</p> <table> <tr> <td>Terminal Type</td> <td>VT-100</td> </tr> <tr> <td>Port</td> <td>Any COM port</td> </tr> <tr> <td>Terminal Settings</td> <td>19200 bps transfer rate</td> </tr> <tr> <td></td> <td>8 data bits</td> </tr> <tr> <td></td> <td>no parity</td> </tr> <tr> <td></td> <td>1 stop bit</td> </tr> <tr> <td></td> <td>no flow control</td> </tr> </table>	Terminal Type	VT-100	Port	Any COM port	Terminal Settings	19200 bps transfer rate		8 data bits		no parity		1 stop bit		no flow control
Terminal Type	VT-100														
Port	Any COM port														
Terminal Settings	19200 bps transfer rate														
	8 data bits														
	no parity														
	1 stop bit														
	no flow control														
All else...	Contact Extreme Networks Support.														

Access Port/Point Issues

This section describes various issues related to Access Ports within the Extreme Networks wireless LAN controller network. Possible issues include:

- [Access Ports/Points are Not Adopted](#)
- [Access Ports/Points are Not Responding](#)

Access Ports/Points are Not Adopted

Access Ports are not being adopted. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Access Port/Point is not configured	Verify the license key that is set in the controller.
Country code for controller is not set	Verify the country code is entered into the controller prior to adopting any Access Ports/Points. The controller is not fully functional until a country code is set.
Access Ports/Points are off-network	Verify the Access Ports/Points are connected to the network and powered on.
Access Ports/Points are restricted in configuration	<p>Verify the controller is not configured with an access control list that does not allow Access Port/Point adoption; verify that Access Port/Point adoption is not set to "deny".</p> <p>Ensure that the Access Port/Point adoption policy is added with a WLAN.</p>
Access Port/Point is on Exclude List	Verify the Extreme Networks wireless LAN controller ACL adoption list does not include the Access Ports/Points that are not being adopted.
Miscellaneous other issues	<p>With a packet sniffer, look for 8375 (broadcast) packets.</p> <p>Reset the Extreme Networks wireless LAN controller. If the controller is hung, it may begin to adopt Access Ports/Points properly once it has been reset.</p>
All else...	Contact Extreme Networks Support.

Access Ports/Points are Not Responding

Access Ports/Points are not responding. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Access Port/Point not responding after converting to a Detector AP	When converting an AP4600 Series Access Port to an Intrusion Detection Sensor, the conversion requires approximately 60 seconds.
All else...	Contact Extreme Networks Support.

Sensor Port frequently goes up and down

Possible Problem	Suggestions to Correct
Sensor Port flapping (going up and down)	This may be caused by the sensor being unable to find its server. Ensure that the detection configuration is correct and that all cables are secure.
All else...	Contact Extreme Networks Support.

Mobile Unit Issues

This section describes various issues that may occur when working with the mobile units associated with the wireless controller or associated Access Ports. Possible issues include:

- [Access Port/Point Adopted, but MU is Not Being Associated](#)
- [MUs Cannot Associate and/or Authenticate with Access Ports/Points](#)
- [Poor Voice Quality Issues](#)

Access Port/Point Adopted, but MU is Not Being Associated

Access Port/Point associated with an MU is not yet being adopted. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Unadopted Access Port/Point	Verify that the controller has adopted the Access Port/Point with which the MU is trying to associate.
Incorrect ESSID applied to the MU	Verify on the MU the correct ESSID has been applied to the MU.
Ethernet port configuration issues	<ul style="list-style-type: none">• Verify that the Ethernet port connected to the network and has a valid configuration.• If DHCP is used, verify that the Ethernet cable is connected to the same NIC upon which DHCP services are enabled.
Incorrect security settings	Verify the correct security settings are applied to a WLAN in which the MU is trying to associate.
All else...	Contact Extreme Networks Support.

MUs Cannot Associate and/or Authenticate with Access Ports/Points

MUs cannot associate and/or authenticate with Access Ports/Points. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Preamble differences	Verify the preamble type matches between controller and MUs. Try a different setting.
Device key issues	Verify in Syslog there is not a high rate of decryption error messages. This could indicate a device key is incorrect.
MU is not in Adopt List	Verify the device is not in the “do not adopt ACL”.
Keyguard not set on client	Verify Keyguard is set on the client if the Security/WLAN Policy calls for Keyguard.
Encryption Problems	If Encryption is being used, verify the encryption settings on the MU and the controller match. If WEP encryption is used on the WLAN, ensure proper encryption key in either HEX format or Passphrase is used on the MU.
Authentication Problems	If the controller is configured to use RADIUS authentication, check the RADIUS log file for any failure information.
Encryption or Authentication Problems	If you are using Authentication and/or Encryption on the controller, and the previous troubleshooting steps have not fixed the problem, try temporarily disabling Authentication and Encryption to see if that fixes the problem.

Poor Voice Quality Issues

VOIP MUs, BroadCast MultiCast and SpectraLink phones have poor voice quality issues. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Traffic congestion with data traffic	<ul style="list-style-type: none">• Maintain voice and data traffic on separate WLANs.• Use a QoS Classifier to provide dedicated bandwidth if data and voice traffic are running on the same WLAN.
Long preamble not used on Spectralink phones	Verify a long preamble is used with Spectralink phones.

Miscellaneous Issues

This section describes various miscellaneous issues related to the Extreme Networks wireless LAN controller which don't fall into any of the previous categories. Possible issues include:

- [Excessive Fragmented Data or Excessive Broadcast](#)
- [Excessive Memory Leak](#)

Excessive Fragmented Data or Excessive Broadcast

Excessive fragmented data or excessive broadcast.

The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Fragmentation	<ul style="list-style-type: none">Do not allow VoIP traffic when operating on a flat network (no routers or smart controllers).Move to a trunked Ethernet port.Move to a different configuration.
All else...	Contact Extreme Networks Support.

Excessive Memory Leak

Excessive memory leak. The table below provides suggestions to troubleshoot this issue.

Possible Problem	Suggestions to Correct
Memory leak	Using the CLI or Web UI's Diagnostics section to check the available virtual memory. If any one process displays an excessive amount of memory usage, that process could be one of the possible causes of the problem.
Too many concurrent Telnet or SSH sessions	Keep the maximum number of Telnet or SSH sessions low (6 or less), even though up to 8 sessions are allowed.
All else...	Contact Extreme Networks Support.

System Logging Mechanism

The Extreme Networks wireless LAN controller provides subsystem logging to a Syslog server. There are two Syslog systems, local and remote. Local Syslog records system information locally, on the controller. The remote Syslog sends messages to a remote host. All Syslog messages conform to the RFC 3164 message format.

Troubleshooting SNMP Issues

The following SNMP-related issues could require troubleshooting as SNMP issues are experienced with the Extreme Networks wireless LAN controller.

- [MIB Browser not able to contact the agent](#)
- [Not able to SNMP WALK for a GET](#)
- [MIB not visible in the MIB browser](#)
- [SNMP SETs not working](#)
- [Not receiving SNMP traps](#)
- [Additional Configuration](#)

MIB Browser not able to contact the agent

General error messages on the MIB Browser: Timeout, No Response.

The client IP where the MIB browser is present should be made known to the agent. Adding SNMP clients through CLI or Web UI can do this.

Not able to SNMP WALK for a GET

- Check whether the MIB browser has IP connectivity to the SNMP agent on the controller. Use IP Ping from the client system which has the MIB Browser.
- Check if the community string is the same at the agent side and the manager (MIB Browser) side. The community name is case sensitive.

MIB not visible in the MIB browser

The filename.mib file should be first compiled using a MIB compiler, which creates a smidb file. This file must be loaded in the MIB browser.

SNMP SETs not working

Check to see if environment variables are set. The following are the environment variables to be set.

```
SNMPCONFPATH=/butterfly/snmp
MIBDIRS=/butterfly/snmp/mibs
MIBS=ALL
```

Restart the SNMP agent (the snmpd daemon).

Not receiving SNMP traps

Check whether SNMP traps are enabled through CLI or Applet. Configure the MIB browser to display notifications or traps. (This would generally be a check box in the MIB browser preferences).

Additional Configuration

Double check Managers' IP Address, community string, port number, read/write permissions, and snmp version. Remember community string is CASE SENSITIVE.

Security Issues

This chapter describes the known troubleshooting techniques for the following data protection activities:

- [Controller Password Recovery](#)
- [RADIUS Troubleshooting](#)
- [Troubleshooting RADIUS Accounting Issues](#)
- [Rogue AP Detection Troubleshooting](#)
- [Troubleshooting Firewall Configuration Issues](#)

Controller Password Recovery

If the controller Web UI password is lost, you cannot get past the Web UI login screen for any viable controller configuration activity. Consequently, a password recovery login must be used that will default your controller back to its factory default configuration.

To access the Extreme Networks wireless LAN controller using password recovery:



CAUTION

Using this recovery procedure erases the controller's current configuration and data files from the controller /flash dir. Only the controller's license keys are retained. You should be able to log in using the default username and password (admin/admin123) and restore the controller's previous configuration (only if it has been exported to a secure location before the password recovery procedure was invoked).

Connect a terminal (or PC running terminal emulation software) to the serial port on the front of the controller.

The controller login screen displays. Use the following CLI command for normal login process:

```
WLANController login: cli
```

- 1 Enter a password recovery username of *restore* and password recovery password of *restoreDefaultPassword*.

```
User Access Verification
```

```
Username: restore
```

```
Password: restoreDefaultPassword
```

```
WARNING: This will wipe out the configuration (except license key) and user data under "flash:/" and reboot the device
```

```
Do you want to continue? (y/n):
```

- 2 Press *Y* to delete the current configuration and reset factory defaults.

The controller will login into the Web UI with its reverted default configuration. If you had exported the controller's previous configuration to an external location, it now can be imported back to the controller.

RADIUS Troubleshooting

This section covers troubleshooting and workarounds for common RADIUS problems. It includes the following issues:

- [RADIUS Server does not start upon enable](#)
- [RADIUS Server does not reply to my requests](#)
- [RADIUS Server is rejecting the user](#)
- [Time of Restriction configured does not work](#)
- [Authentication fails at exchange of certificates](#)
- [When using another Summit WM3700 \(controller 2\) as RADIUS server, access is rejected](#)
- [Authentication using LDAP fails](#)
- [VPN Authentication using onboard RADIUS server fails](#)
- [Accounting does not work with external RADIUS Accounting server](#)

RADIUS Server does not start upon enable

Ensure the following have been attempted:

- Import valid server and CA certificates

-
- Add a RADIUS client in AAA context.
 - Ensure that key password in AAA/EAP context is set to the key used to generate imported certificates.
 - DO NOT forget to SAVE!

RADIUS Server does not reply to my requests

Ensure the following have been attempted:

- Add a RADIUS client in RADIUS server configuration with the Controller's VLAN interface, IP address and subnet, which have been marked as management.
- Save the current configuration.
- Ensure that the WLAN settings have been set to use the on-board/local RADIUS server by entering the local IP address or the controller management VLAN IP address.

RADIUS Server is rejecting the user

Ensure the following have been attempted:

- Verify a SAVE was done after adding this user.
- Is the user present in a group?
 - If yes, check if the WLAN being accessed is allowed on the group.
 - Check if time of access restrictions permit the user.

Time of Restriction configured does not work

Ensure that date on the system matches your time.

Authentication fails at exchange of certificates

Ensure the following have been attempted:

- Verify that valid certificates were imported.
- If the Supplicant has "Validate Server Certificate" option set, then make sure that the right certificates are installed on the MU.

When using another Summit WM3700 (controller 2) as RADIUS server, access is rejected

Ensure the following have been attempted:

- Make sure that the user, group and access policies are properly defined on controller 2.
- Add a AAA client on controller 2 with a VLAN interface IP address which can communicate with controller 1.
- Save the current configuration.

Authentication using LDAP fails

Ensure the following have been attempted:

- Is LDAP server reachable?
- Have all LDAP attributes been configured properly?
- Dbtype must be set to LDAP in AAA configuration.
- Save the current configuration.

VPN Authentication using onboard RADIUS server fails

Ensure the following have been attempted:

- Ensure that the VPN user is present in AAA users.
- This VPN user MUST NOT added to any group.
- Save the current configuration.

Accounting does not work with external RADIUS Accounting server

Ensure that accounting is enabled.

- Ensure that the RADIUS Accounting server reachable.
- Verify that the port number being configured on accounting configuration matches that of external RADIUS Accounting Server.
- Verify that the shared secret being configured on accounting configuration matches that of external RADIUS Accounting Server.

Troubleshooting RADIUS Accounting Issues

Use the following guidelines when configuring RADIUS Accounting:

- The RADIUS Accounting records are supported for clients performing 802.1X EAP based authentication or using the Hotspot functionality.
- The user name present in the accounting records, could be that of the name in the outer tunnel in authentication methods like: TTLS, PEAP.
- If the controller crashes for whatever reason, and there were active EAP clients, then there would be no corresponding STOP accounting record.
- If using the on-board RADIUS Accounting server, one can delete the accounting files, using the del command in the enable context.
- If using the on-board RADIUS Accounting server, the files would be logged under the path:
/flash/log/radius/radacct/

Rogue AP Detection Troubleshooting

Extreme Networks recommends adhering to the following guidelines when configuring Rogue AP detection:

- Basic configuration required for running Rogue AP detection:
 - Enable any one of the detection mechanisms.
 - Enable rogueap detection global flag.
- After enabling rogueap and any one of the detection mechanisms, look in the roguelist context for detected APs. If no entries are found, do the following:
 - Check the global rogueap flag by doing a show in rogueap context. It should display Rogue AP status as “enable” and should also the status of the configured detection scheme.
 - Check for the “Extreme Networks AP” flag in rulelist context. If it is set to “enable”, then all the detected APs will be added in approved list context.
 - Check for Rulelist entries in the rulelist context. Verify it does not have an entry with MAC as “FF:FF:FF:FF:FF:FF” and ESSID as “*”.
- If you have enabled AP Scan, ensure that at least a single radio is active. AP scan does not send a scan request to an inactive or unavailable radio.
- Just enabling detectorscan will not send any detectorscan request to any adopted AP. User should also configure at least a single radio as a detectorAP. This can be done using the set detectorap command in rogueap context.

Troubleshooting Firewall Configuration Issues

Extreme Networks recommends adhering to the following guidelines when dealing with problems related to Firewall configurations:

- [Configuration Issue 1 on page 628](#)
- [Configuration Issue 2 on page 629](#)
- [Configuration Issue 3 on page 629](#)
- [Configuration Issue 4 on page 629](#)

Configuration Issue 1

A Wired Host (Host-1) or Wireless Host (Host-2) on the untrusted side is not able to connect to the Wired Host (Host-3) on the trusted side.

- 1 Check that IP Ping from Host-1/Host-2 to the Interface on the Trusted Side of the Extreme Networks wireless LAN controller works.

CLI (from any context) - ping <host/ip_address>

- 2 If it works then there is no problem in connectivity.

- 3 Check whether Host-1/Host-2 and Host-3 are on the same IP subnet.

If not, add proper NAT entries for configured LANs under FireWall context.

- 4 After last step, check again, that IP Ping from Host1 to the Interface on the Trusted Side of the Extreme Networks wireless LAN controller works.

If it works then problem is solved.

Configuration Issue 2

A wired Host (Host-1) on the trusted side is not able to connect to a Wireless Host (Host-2) or Wired Host (Host-3) on the untrusted side.

- 1 Check that IP Ping from Host-1 to the Interface on the Untrusted Side of the controller works.
- 2 If it works then there is no problem in connectivity.
- 3 Now check whether Host-1 and Host-2/Host-3 are on the same IP subnet.
If not, add proper NAT entries for configured LANs under FireWall context.
- 4 Once step 3 is completed, check again, that IP Ping from Host1 to the Interface on the Untrusted Side of the controller works.
If it works then problem is solved.

Configuration Issue 3

Disabling of telnet, ftp and web traffic from hosts on the untrusted side does not work.

- 1 Check the configuration for the desired LAN under FW context (which is under configure context).
CLI - configure fw <LAN_Name>
- 2 Check whether ftp, telnet and web are in the denied list. In this case, web is https traffic and not http.
- 3 Ensure that “network policy” and “Ethernet port” set to the LAN is correct.

Configuration Issue 4

How to block the request from host on untrusted to host on trusted side based on packet classification.

- 1 Add a new Classification Element with required Matching Criteria.
- 2 Add a new Classification Group and assigned the newly created Classification Element. Set the action required.
- 3 Add a new Policy Object. This should match the direction of the packet flow i.e. Inbound or Outbound.
- 4 Add the newly created PO to the active Network Policy.
- 5 Associate WLAN and Network Policy to the active Access Port/Point Policy.
Any request matching the configured criteria should take the action configured in the Classification Element.



D

APPENDIX

Open Source Software Information

For instructions on obtaining a copy of any source code being made publicly available by Extreme Networks related to software used in this Extreme Networks product, you may send a request in writing to Extreme Networks.

This document contains information regarding licenses, acknowledgments and required copyright notices for open source packages used in this Extreme Networks product.

Open Source Software Used

Table 8: Open Source Software Used

Name	Version	URL	License
autoconf	2.62	http://www.gnu.org/software/autoconf/	GNU General Public License 2.0
automake	1.96	http://www.gnu.org/software/automake/	GNU General Public License 2.0
binutils	2.19.1	http://www.gnu.org/software/binutils/	GNU General Public License 2.0
bison	2.3	http://www.gnu.org/software/bison/	GNU General Public License 2.0
busybox	1.11.3	http://www.busybox.net/	GNU General Public License 2.0
dnsmasq	2.47	http://www.thekelleys.org.uk/dnsmasq/doc.html	GNU General Public License 2.0
dropbear	0.51	http://matt.ucc.asn.au/dropbear/dropbear.html	Drop Bear License
e2fsprogs	1.40.11	http://e2fsprogs.sourceforge.net/	GNU General Public License 2.0
gcc	4.1.2	http://gcc.gnu.org/	GNU General Public License 2.0
gdb	6.8	http://www.gnu.org/software/gdb/	GNU General Public License 2.0
genext2fs	1.4.1	http://genext2fs.sourceforge.net/	GNU General Public License 2.0
glibc	2.7	http://www.gnu.org/software/libc/	GNU General Public License 2.0
hostapd	0.6.9	http://hostap.epitest.fi/hostapd/	GNU General Public License 2.0
hotplug2	0.9	http://isteve.bofh.cz/~isteve/hotplug2/	GNU General Public License 2.0
ipkg-utils	1.7	http://www.handhelds.org/sources.html	GNU General Public License 2.0
iproute2	2.6.25	http://www.linuxfoundation.org/collaborate/	workgroups/networking/iproute2 GNU General Public License 2.0
iptables	1.4.1.1	http://www.netfilter.org/	GNU General Public License 2.0
libpcap	0.9.8	http://www.tcpdump.org/	BSD Style Licenses
libtool	1.5.24	http://www.gnu.org/software/libtool/	GNU General Public License 2.0

Table 8: Open Source Software Used (Continued)

Name	Version	URL	License
linux	2.6.28.9	http://www.kernel.org/	GNU General Public License 2.0
lzma	4.32	http://www.7-zip.org/sdk.html	GNU Lesser General Public License 2.1
lzo	2.03	http://www.oberhumer.com/opensource/lzo/	GNU General Public License 2.0
m4	1.4.5	http://www.gnu.org/software/m4/	GNU General Public License 2.0
madwifi	truck-r3314	http://madwifi-project.org/	BSD Style Licenses
mtd	2009-05-05	http://www.linux-mtd.infradead.org/	GNU General Public License 2.0
mtd-utils	2009-02-27	http://www.linux-mtd.infradead.org/	GNU General Public License 2.0
openssl	0.9.8j	http://www.openssl.org/	Open SSL License
openwrt	truck-r15025	http://www.openwrt.org/	GNU General Public License 2.0
opkg	truck-r4564	http://code.google.com/p/opkg/	GNU General Public License 2.0
pkg-config	0.22	http://pkg-config.freedesktop.org/wiki/	GNU General Public License 2.0
ppp	2.4.3	http://ppp.samba.org/ppp/	BSD Style Licenses
quilt	0.47	http://savannah.nongnu.org/projects/quilt/	GNU General Public License 2.0
sed	4.1.2	http://www.gnu.org/software/sed/	GNU General Public License 2.0
squashfs	3.0	http://squashfs.sourceforge.net/	GNU General Public License 2.0
u-boot	trunk-2010-03-30	http://www.denx.de/wiki/U-Boot/	GNU General Public License 2.0
uci	0.7.5	http://www.openwrt.org/	GNU General Public License 2.0
uClibc	0.9.29	http://www.uclibc.org/	GNU General Public License 2.0
udev	r106	http://www.kernel.org/pub/linux/utils/kernel/	hotplug/ GNU General Public License 2.0
wireless_tools	r29	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html	GNU General Public License 2.0
zlib	1.2.3	http://www.zlib.net/	ZLIB License

OSS Licenses

A list of open source licenses for Extreme Networks software is available on the Extreme Networks website at: <http://www.extremenetworks.com/go/SoftwareLicensing>.

E

APPENDIX

Best Practices

This document lists a set of best practices that can improve the performance of your network and the devices that constitute it.

ACL configuration to reduce the amount of broadcast or multicast traffic in the network

Use these commands to create an extended MAC access list with the name IPV6-BLOCK. From the (config) mode execute the following commands.

```
mac access-list extended IPV6-BLOCK
  permit any any type ip rule-precedence 10
  permit any any type arp rule-precedence 60
```

Use these commands to create an extended IP access list with the name BCMC-CTRL-VOICE. From the (config) mode, execute the following commands.

```
ip access-list extended BCMC-CTRL-VOICE
  permit ip any host 224.0.0.1 rule-precedence 20
  permit tcp any any rule-precedence 30
  permit udp any eq 67 any eq bootpc rule-precedence 40
  deny ip any 224.0.0.0/4 rule-precedence 50
  deny udp any range 137 138 any range 137 138 rule-precedence 60
  deny ip any host 255.255.255.255 rule-precedence 80
  permit ip any any rule-precedence 100
```

These rules must be applied in the OUT direction. For example:

```
wlan-acl <idx> BCMC-CTRL-VOICE out
wlan-acl <idx> IPV6-Block out
```

where <IDX> is the index of the WLAN on which the ACL must be applied.

Settings to reduce DHCP and ARP traffic on air

Use these commands to reduce on air DHCP and ARP traffic.

This command enables the sniffing DHCP packets to update the the MU table and keeping it current. From the (config-wireless) context, issue this command.

```
dhcp-sniff-state enable
```

This command sends DHCP packets only to the AP on which the MU that requested DHCP is located. DHCP packets are not sent to the other APs.

```
dhcp-one-portal-forward enable
```

This command prevents sending broadcast/multicast packets to APs that do not have any MUs.

```
no service wireless idle-radio-send-multicast enable
```

This commands prevents sending ARP packets for unknown device over air.

```
proxy-arp enable strict
```

Settings to set the rate at which multicast and broadcast packets are sent

By default, multicast and broadcast packets are sent at the highest basic rate. Though this increases the transmission rate, the range is restricted. To increase the range, use the range parameter.

To configure to send these packets at a lower rate issue this command:

```
broadcast-tx-speed [range|throughput]
  range use lowest basic rate. Provides maximum range
  throughput use highest basic rate. Provides maximum throughput (default)
```

Depending on your requirement, select the appropriate action to increase your performance.

Remove DFS channels from ACS

Removing the Dynamic Frequency Selection (DFS) channels from your Automatic Channel Selection (ACS) list increases performance. This selects channels from a list of available channels for a particular frequency band. The following example is specific to US. Issue this command from the (config-wireless) context.

```
auto-select-channels 11a 36,38,40,42,44,46,48,149,153,157,161,165
```

Operate a 11bgn radio in the 20MHz band

Operate a 11bgn radio in the 20MHz band. Extreme Networks recommends a 802.11bgn radio be operated in 20 MHz band for optimal performance. An 802.11an radio can operate optimally in 20 MHz as well as 40 MHz bands.

While configuring channel power settings for indoor APs, do not configure the upper channel band. From the (config-wireless) context, issue this command:

```
radio <RADIO-INDEX> channel-power indoor <CHANNEL-NUMBER> <CHANNEL-POWER>
```

For example,

```
WM3600(config-wireless)#radio 1 channel-power indoor 1 20
```

Enable Dynamic Chain Selection

Enable Dynamic Chain Selection. 11n AP uses MIMO which uses multiple antennas to coherently resolve more information than when using a single antenna.

Some older devices have trouble hearing and accepting MIMO transmitted packets at legacy rates. When dynamic chain selection is enabled, the AP transmits legacy rates on one antenna. This feature does not affect 802.11n devices but makes co-existence with older devices easier.

To enable Dynamic Chain Selection, from the (config-wireless) context, issue the following command.

```
radio <index> dynamic-chain-sel enable
```

Disable Stateful Firewall Inspection Engine

Disable the stateful firewall inspection engine. This increases the performance while there is a compromise on the level of security in the network. To disable stateful packet inspection, from the (config) context, issue this command.

```
no firewall stateful-packet-inspection 12
```

Disable Cluster Master Support

Disable cluster master support to stop synchronization of radio configuration among cluster members. This reduces the amount of network traffic.

```
no cluster-master-support enable
```

Disable MSTP if not used in the network

If Multiple Spanning Tree Protocol (MSTP) is enabled in your network and if it is not used, then disable it. This increases the total throughput of the network as devices need not keep themselves updated with the current state of the network.

```
no bridge multiple-spanning-tree enable bridge-forward.
```