

CUSTOMER RELEASE NOTES

**Enterasys RoamAbout® Wireless Switch 8xx0 Release
Firmware Version 7.0.12.2
November 2009**

INTRODUCTION:

The RBT-8xx0 family of wireless switches includes the following devices:

- RBT-8100/RBT-8110 - Can control up to 24 access points
- RBT-8200/RBT-8210 - Can control 24/48/72 access points
- RBT-8400 - Can control 40/80/120 access points
- RBT-8500 - Can control 32/64/96/128 access points

The RoamAbout Switch Manager (RASM) can manage all of these devices.

The 7.0.12.2 Firmware release addresses firmware modifications and customer escalations (refer to the [Firmware and Enhancements](#) section).

Enterasys recommends that you thoroughly review this document prior to installing or upgrading this product.

NOTE: The following table provides the access points and features supported by the Wireless Switch 8xx0 Firmware Version 7.0.12.2

Access Point	Supported in 7.0.12.2	Hitless Failover	Direct Path Forwarding	Wireless Mesh Support
RBT3K-AG	Yes	No	No	No
RBT-1002	Yes	No	No	No
RBT-1002-EU	Yes	No	No	No
RBT-1602	Yes	Yes	No	No
RBT-4102	Yes	No	No	No
RBT-4102-EU	Yes	No	No	No
RBT-4102-BG	Yes	No	No	No
TRPZ-MP-372-CN	Yes	Yes	No	No
TRPZ-MP-372-IL	Yes	Yes	No	No
TRPZ-MP-422	Yes	Yes	Yes	Yes
TRPZ-MP-432	Yes	Yes	Yes	Yes (802.11a/b/g only)
TRPZ-MP-620	Yes	Yes	Yes	Yes

NOTE: Enabling Direct Path Forwarding (also known as local switching) for a given AP affects the number of ACEs that can be applied within a single ACL policy to a user connecting to that AP. When local switching is enabled on an AP in version 6.0.5.1 or greater of RAS firmware, up to 25 ACEs in an ACL policy can be applied to a user of that AP. Please refer to the [Firmware Changes and Enhancements](#) section for more information.

CUSTOMER RELEASE NOTES

NOTE: To avoid conflicts with internal RAS VLAN numbering schemes, it is strongly advised to use VLAN IDs less than 3520 on RBT-8xxx systems that are upgrading from MSS version 6.0 to 7.0. Failure to do so will result in a loss of configuration data.

NOTE: RoamAbout Wireless Switch Firmware version 5.0.9.2 and greater supports the RBT-8210, the small form factor switch that replaces the larger RBT-8200. The RBT-8210 uses the RBT-8200 firmware and commands. The RBT-8210 prompt displays as RBT-8200.

NOTE: If you are using a 4.x firmware image/software, Enterasys recommends that you upgrade the RoamAbout Switch Manager (RASM) to firmware version 5.0.12.2 BEFORE upgrading your RBT-8xx0 wireless switches to firmware version 5.0.12.2. Please refer to the [Upgrading the RBT8xxx switches](#) section of this release note for more information.

NOTE: If you are upgrading a pre-existing RBT-4102 or RBT-4102-EU model Access Point from 4.1.4 or earlier, please read the instructions listed in the *Firmware Release 4.1.5.0* section of the *Firmware Changes and Enhancements* section of the RoamAbout Switch Manager (RASM) 6.2.2.4 Release Notes.

NOTE: RoamAbout Wireless Switch Firmware version 6.0.4.2 and greater replaces the term 'DAP' with 'AP'.

NOTE: Beginning with the calendar year 2007, please be aware that the United States Daylight saving time period begins on the second Sunday in March, and ends on the first Sunday in November. Refer to the "Changing Timezone Properties" section in the "Configuring RoamAbout Switch System and Administrative Parameters" chapter of the *RoamAbout Switch Manager Interface Reference* document for detailed setup instructions.

CUSTOMER RELEASE NOTES

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Release	7.0.12.2	Customer Maintenance	November 2009
Previous Release	7.0.9.8	Customer Maintenance	May 2009
Previous Release	7.0.7.3	Customer Maintenance	January 2009
Previous Release	7.0.5.6	Customer Maintenance	October 2008
Previous Release	7.0.4.3	Customer Maintenance	August, 2008
Previous Release	7.0.3.7	Customer Maintenance	June, 2008
Previous Release	6.0.7.2	Customer Maintenance	April, 2008
Previous Release	6.0.6.1	Customer Maintenance	March, 2008
Previous Release	6.0.5.1	Customer, added RBT-8500 support	December 2007
Previous Release	6.0.4.4	Customer	October 2007
Previous Release	6.0.4.2	Customer, added TRPZ-MP-620 support	September 2007
Previous Release	5.0.12.2	Customer, added TRPZ-MP-422 support. Includes DFS2 Support for North American Models: RBT-1002 Rev 6A (AP ID: AP1002C), RBT-4102 Rev 6A (AP ID: AP4102C), RBT-1602 Rev 6A (AP ID: AP1602C)	June 2007
Previous Release	5.0.11.4	Customer	April 2007
Previous Release	5.0.10.3	Customer – Patch	March 2007
Previous Release	5.0.9.3	Customer	February 2007
Previous Release	5.0.9.2	Customer, added RBT-8210 support	January 2007
Previous Release	5.0.6.1	Customer, added TRPZ-MXR-2 support	December 2006
Previous Release	4.2.5.1	Customer, added RBT-8110 and TRPZ-MP-620 support	October 2006
Previous Version	4.1.11.0	Customer	June 2006
Previous Version	4.1.5.0	Customer	April 2006
Previous Version	4.1.4.0	Customer, added RBT-8200 support	February 2006
Previous Version	4.0.21.0	Customer	January 2006
Previous Version	4.0.20.0	Customer	December 2005
Previous Version	4.0.18.0	Customer	November 2005
Previous Version	4.0.16.0	Customer, added RBT-8400 support	September 2005
Previous Version	4.0.7.0	Customer	August 2005
Previous Version	4.0.4.0	Customer, added RBT-8100 support	July 2005

NOTE: For firmware release 5.0.12.2, please read the [TechTip](#) on page 22 for the channel availability information.

HARDWARE COMPATIBILITY:

Switches:

- RBT-8100, RBT-8110, RBT-8200, RBT-8210, RBT-8400, RBT-8500, and TRPZ-MXR-2.

Access Points:

- See the [Supported Access Point Table on page 1](#) for detailed information for version 7.0.12.2

CUSTOMER RELEASE NOTES

NETWORK MANAGEMENT SOFTWARE SUPPORT:

NMS Platform	Version No.	Module No.
RoamAbout Switch Manager 50 Access Point User License	7.0.11.2	RBT-NMS-50
RoamAbout Switch Manager 200 Access Point User License	7.0.11.2	RBT-NMS-200
RoamAbout Switch Manager unlimited User License	7.0.11.2	RBT-NMS-UNL
RoamAbout RF Planning Tool	7.0.11.2	RBT-RFPLAN
SmartPass Guest Access	7.0.11.2	TRPZ-SP TRPZ-SP-ENT

RBT-8400 Platform	Version No.	Module No.
RBT-8400 40 Additional Access Point Upgrade License	7.0.11.2	RBT-8400-40
RBT-8400 80 Additional Access Point Upgrade License	7.0.11.2	RBT-8400-80

RBT-82x0 Platform	Version No.	Module No.
RBT-82x0 24 Additional Access Point Upgrade License	7.0.11.2	RBT-8200-24
RBT-82x0 48 Additional Access Point Upgrade License	7.0.11.2	RBT-8200-48

RBT-8500 Platform	Version No.	Module No.
RBT-8500 32 Additional Access Point Upgrade License	7.0.11.2	RBT-8500-32

CUSTOMER RELEASE NOTES

SUPPORTED FUNCTIONALITY:

Please refer to the following documents available at <http://secure.enterasys.com/support/manuals> for more details on new 7.0 enhancements and overall functionality:

RoamAbout Switch Manager 7.0 Configuration Guide	RoamAbout Mobility System Software 7.0 Command Reference Guide
RoamAbout Switch Manager 7.0 Management Guide	RoamAbout Mobility System Software 7.0 Feature Guide
RoamAbout Switch Manager 7.0 Feature Guide	RoamAbout Mobility System Software 7.0 Configuration Guide
RoamAbout Switch Manager 7.0 Planning Guide	RoamAbout Mobility System Software 7.0 Quick Start Guide
RoamAbout Switch Manager 7.0 Quick Start Guide	

New Product Features in Release 7.0

Enterasys Virtual Controller Cluster	TRPZ-MP-432 to support 802.11n
Layer 2 ACL Enhancements	Snoop Filter Enhancements
Bandwidth Management by User and SSID	Dynamic RADIUS Extensions
MAC User Range Authentication	MAC Authentication Request Format
Additional User AAA Attributes for User Name and Simultaneous Logins	Group-based Authentication and Authorization
Location Policy Enhancements	RADIUS Ping
RF Enhancements	Mesh Enhancements

NOTES:

- Local switching is only available in RAS firmware version 6.0 and higher.
- Restricting Layer 2 forwarding for a VLAN is not supported if the VLAN is configured for local switching.
- The DHCP restrict feature is not supported for locally switched clients.
- Web Portal is not supported for locally switched clients.
- IGMP snooping is not supported with local switching.
- Locally Switched AP's can support a total of 25 ACL rules, including both inbound and outbound ACLs.
- For Wireless bridging, here are some best practice guidelines:
 - When connecting a Mesh Portal to the network, use only ethernet port 1 on the AP.
 - Because all AP CPU cycles are devoted to bridging, make other arrangements for service coverage in the bridge area as the endpoints cannot provide other wireless services.
 - A single radio must be devoted to maintaining the bridge.

CUSTOMER RELEASE NOTES

Existing Product Features	
RF Load Balancing	Mesh Services
Local Switching – also known as Direct Path Forwarding	Wireless Bridging
Enforceable Beacon Data Rate Control	Logout for Web Authentication
RAS Seed Redundancy	Password Management
WebView 2 – updated Web interface	RBT-RBT security (also called RAS-RAS security)
AirDefense software support on APs	AeroScout RFID tag support
Persistent VLAN assignment for roaming clients	Simplified Web-Portal and last-resort configuration
RF Auto-Tuning enhancements	Unscheduled Automatic Powersave Delivery (U-APSD) support
Local software images on AP's	DHCP server enhancements
RADIUS accounting enhancements	Support for special characters in SNMP community names
Increased life span of new self-signed certificates	Web Interface to RASM services
Web-Start Client	Static IP configuration for Aps
Sygate On-Demand Agent (SODA)	Broadcast settings per Wireless profile
Configurable data rate settings for clients	Session Based Call Admission Control
Static Class of Service	User Session Timers per SSID
Network Planning and Site Survey	Management services
SSID (Wireless Service)	Radio and Service profiling
Load Sharing	802.1Q VLANs
Spanning Tree – PVST	AAA/802.1X
ACLs	IP services
RF detection	Rogue detection
Countermeasures	Client and AP monitoring
Site policies	Reporting
Image repository and deployment	Auto-AP configuration
L2 traffic restriction	Default AAA attributes for each SSID
On-demand countermeasures	Network Domains
Configurable timeout for the RoamAbout Switch CLI sessions	Configurable CoS to QoS mappings

INSTALLATION AND CONFIGURATION NOTES:

In general, the RoamAbout Wireless Switch RBT-8xx0 has been, or is being, shipped to you with a previous firmware version. Please refer to the appropriate *RBT-8xx0 Quick Start* or the *RBT-8xx0 Installation Guide* for hardware installation information. Please refer to the next section, [Upgrading the RBT-8xx0 Switches](#), for upgrading information and procedures.

UPGRADING THE RBT-8XX0 SWITCHES FROM PREVIOUS 4.0.X VERSIONS:

Minimum RAS Requirements for Upgrade

Product	Minimum RAS version required	Recommended Upgrade Path
RBT-8100	4.0.4.0	6.0.7.2 → 7.0.7.x
RBT-8200	4.1.4.0	6.0.7.2 → 7.0.7.x
RBT-8110, RBT-8210	4.2.5.1	6.0.7.2 → 7.0.7.x
RBT-8400	4.0.16.0	6.0.7.2 → 7.0.7.x
RBT-8500	6.0.5.1	6.0.7.2 → 7.0.7.x

Note: You must upgrade to RAS Version 5.0 or later before upgrading to RAS Version 7.0.

Preparing the RAS for the Upgrade

Note: The following upgrade procedures refer to all RBT-8xx0 switches.

Caution!

Save the configuration, and then create a backup of your RAS files before you upgrade the switch. Enterasys Networks recommends that you make a backup of the switch, before you install the upgrade. If an error occurs during the upgrade, you can restore your switch to its previous state. If you later decide to downgrade the switch, commands with newer syntax in future RAS versions may not be converted correctly.

1. Use the following command to save the configuration. Unsaved changes will be lost during the upgrade procedure:

```
RBT-8xx0# save config [filename]
```

2. The following command should be used to back up the switch's files:

```
RBT-8xx0# backup system [tftp://ip-addr/]filename [all | critical]
```

3. To restore a switch that has been backed up, use the following command:

```
RBT-8xx0# restore system [tftp://ip-addr/]filename [all | critical] [force]
```

The "Upgrade Scenario" listed below shows an example use of the backup command. For more information about these commands, see the "Backing Up and Restoring the System" section in the "Managing System Files" chapter of the *RoamAbout Mobility System Software Configuration Guide*.

Note: If you have made configuration changes but have not saved the changes, use the **save config** command to save the changes, before you back up the switch.

If the RAS is running an earlier version of firmware, use the **copy tftp** command to copy files from the switch onto a TFTP server.

Upgrading an Individual Switch Using the CLI:

1. Save the configuration, using the **save configuration** command.
2. Back up the switch, using the **backup system** command.

3. Copy the new system image onto a TFTP server.

For example, login to <http://www.enterasys.com/download/> using a web browser on your TFTP server and download the image onto the server.

4. Copy the new system image file from the TFTP server into a boot partition in the switch's nonvolatile storage. You can copy the image file only into the boot partition that was not used for the most recent restart. For example, if the currently running image was booted from partition 0, you can copy the new image only into partition 1.
5. Set the boot partition to the one with the upgrade image for the next restart.
 - a. To verify that the new image file is installed, type `show boot`.
6. Reboot the software.

- a. To restart a RAS and reboot the software, type the following command:

```
RBT-8xx0# reset system [force]
```

After resetting the RAS, the switch boots using the new image. The RAS also sends the AP version of the new boot image to the configured APs and restarts the APs. After an AP restarts, it checks the version of the new AP boot image to make sure the boot image is newer than the boot image currently installed on the AP. If the boot image is newer, the AP completes installation of its new boot image by copying the boot image into the AP's flash memory, which takes about 30 seconds, then restarts again. The upgrade of the AP is complete after the second restart.

Upgrade Scenario:

To upgrade an RBT-8xx0 switch from one RAS version to another, type commands such as the following.

Note: This upgrade scenario uses the firmware image file 6.0.7.2 to show the download features. Please follow these procedures for any of the 4.0.x, 4.1.x, 4.2.x, and 5.0.x firmware images.

Note: This example copies the image file into boot partition 1. On your switch, copy the image file into the boot partition not used for the last restart. For example, if the switch booted from boot partition 1, copy the new image into boot partition 0. To see boot partition information, type the `show boot` command.

```
RBT-8200# save config success: configuration saved.  
RBT-8200# backup system tftp://[ip-addr]/sysa_bak success: sent 28263 bytes in 0.324 seconds [ 87231  
bytes/sec]  
RBT-8200# copy tftp://[ip-addr]/R2060701.REL boot1:R2060701.REL success: received 11257345 bytes  
in 16.230 seconds [693613 bytes/sec]  
RBT-8200# set boot partition boot1 success: Boot partition set to boot1.
```

```
RBT-8200# show boot  
Configured boot version:      6.0.7.2.0  
Configured boot image:       boot1: R2060701.rel  
Configured boot configuration: file:configuration  
Backup boot configuration:    file:backup  
Booted version:              6.0.6.1.0  
Booted image:                boot0:R2060601.REL  
Booted configuration:        file:configuration  
Product model:               RBT-8200
```

Upgrading an Individual Switch Using the RoamAbout Switch Manager (RASM)

Please refer to the chapter “Managing with RoamAbout Switch Manager”, section “Distributing System Images” in the *RoamAbout Switch Manager Management Guide* when upgrading the RBT-8xx0 switch to the released version.

SYSTEM PARAMETER SUPPORT:

RoamAbout System Parameters:

Parameter:	Supported Value:
RASs in a single Network Domain	500
RASs in a single Mobility Domain	32
Roaming VLANs per RAS	300 Does not include local statically configured VLANs
VLANs per Mobility Domain	400 This number consists of 300 roaming VLANs plus 100 local statically configured VLANs
APs per RAS	RBT-81x0: 120 configured, 24 active RBT-82x0: 360 configured, 72 active RBT-8400: 480 configured, 120 active RBT-8500: 512 configured, 128 active
SSIDs per radio	8
Minimum link speed within a Mobility Domain	128 Kbps

Network Parameters:

Parameter:	Supported Value:
Forwarding database entries	RBT-81x0: 8192 RBT-82x0: 8192 RBT-8400: 16383 RBT-8500: 8192
Statically configured VLANs	128
Virtual ports (sum of all statically configured VLAN physical port memberships)	256
Spanning trees (STP/PVST+ instances)	64
ACLs and Location Policies	ACEs per switch RBT-81x0: 700 RBT-82x0: 700 RBT-8400: 2308 RBT-8500: 2308 ACEs per ACL: RBT-81x0: 25 RBT-82x0: 25 RBT-8400: 267 RBT-8500: 267 Locations Policies per switch: All models: 1 The Location Policy can have up to 150 rules. ACL rules (ACEs) with Local Switching (Direct Path Forwarding) enabled: 25
IGMP Streams	500 Note: Replications of a stream on multiple VLANs count as separate streams on each VLAN.

Management Parameters:

Parameter:	Supported Value:
Maximum instances of the RoamAbout Software Management system simultaneously managing a network	3
Telnet management sessions	RBT-81x0: 8 RBT-82x0: 8 RBT-8400: 8 RBT-8500: 8 Note: The maximum combined number of management sessions for Telnet and SSH together is 8 for the RBT-8400, RBT-81x0, and the RBT-82x0.
SSHv2 management sessions	RBT-81x0: 8 RBT-82x0: 8 RBT-8400: 8 RBT-8500: 8
Telnet client sessions (client for remote login)	RBT-81x0: 8 RBT-82x0: 8 RBT-8400: 8 RBT-8500: 8
NTP servers	3
SNMP trap receivers	8
Syslog servers	4
RADIUS servers	100 configured on the switch 10 in a server group 4 server group in a AAA rule

Client and Session Parameters:

Parameter:	Supported Value:
Authenticated and associated clients per radio	100 Clients who are authenticated but not yet associated are included in the total
Active clients per radio	50 Total number of active clients simultaneously sending or receiving data
Active AAA sessions (clients trying to establish active connections) per RAS switch	RBT-81x0: 600 RBT-82x0: 1800 RBT-8400: 2500 RBT-8500: 3200
AAA users configured in local user database	RBT-81x0: 999 RBT-82x0: 999 RBT-8400: 999 RBT-8500: 999

CUSTOMER RELEASE NOTES

FIRMWARE CHANGES AND ENHANCEMENTS:

Firmware Release 7.0.12.2:
Resolved an issue where LED behavior on the RBT-1602 became erratic and did not accurately reflect the AP status.
Resolved an issue where, in certain conditions, the MP-432 did not transmit traffic on the network.
Resolved an issue where incorrect information sent from the AP was causing false positive radar detection in the DFS3 algorithm.
Resolved an issue where the keep-alive process for cluster configuration was not executed quickly enough to synchronize configurations between switches.
Resolved an issue where using the spanning tree functionality with third party APs caused connectivity problems on the network.
Resolved an issue where, if VRRP was configured, the packets impacted the MX-2800 which caused problems on the network.
Resolved an issue where the time on the trace log entries slowly drifted until it was different from the timestamp on the switch.
Resolved an issue where the username was not interpreted correctly from the RADIUS packet when used for authentication.
Resolved an issue where, when too many packets were queued on the switch, the switch became unresponsive on the network.
Resolved an issue where clients were unable to connect to the network when the switch did not process a DNS request.
Resolved an issue where the data length received by the AP was too long and the AP discarded it as invalid.
Resolved an issue where continuous requests from Web portal clients caused the switch to become unresponsive.
Resolved an issue where the maximum number of Web portal transactions could not be processed on the switch.
Resolved an issue where DFS3 channels were not enabled for EU regulatory domains on the MP-422B and MP-620B.
Resolved an issue where certain APs did not receive association responses on the network.
Resolved an issue where attempting to authenticate using HTTPD before the switch had initialized or while the configuration updated caused the switch to cease responding on the network.
Resolved an issue where incorrect sensor errors were displayed on the switch.
Resolved an issue where an SNMP query incorrectly caused the switch to cease responding on the network.
Resolved an issue where the secondary seed in a cluster configuration did not process auto-dap requests.
Resolved an issue where inconsistent packet length usage and check caused the switch to become unresponsive on the network.
Resolved an issue where multiple mesh hops were not supported in bridging mode.
Resolved an issue where using Webview to create custom webportal pages caused the switch to become unresponsive.
Resolved an issue where under some circumstances, the switch did not properly process packets from dormant tunnels.
Resolved an issue where Web authentication was not working correctly on the switch.
Resolved an issue where invalid EAPOL packets did not generate error messages on the switch.
Resolved an issue where switches with different versions of MSS and configured in a Mobility Domain may not interpret messages from different versions correctly.
Resolved an issue where APs became unresponsive on the network.
Resolved an issue where ELF messages were displayed when the switch miscalculated the available memory while rebooting on the network.
Resolved an issue where the switch became unresponsive when it did not receive a "sanity" message.
Resolved an issue where a software event on the switch caused it to cease responding on the network.
Resolved an issue where an AP became unresponsive after receiving bad packets from an switch.

CUSTOMER RELEASE NOTES

Firmware Release 7.0.12.2:

- Resolved an issue where large configurations (>1MB) were not compatible with RBT-8500 and RBT-8400 due to file size limitations.
- Resolved an issue where incorrect XML transactions occurred on the switch and it became unresponsive on the network.
- Resolved an issue where an XML transaction on the switch did not contain all of the required information resulting in a core crash of the system.
- Resolved an issue where changing an auto AP configuration after it booted on the network caused errors on the AP.
- Resolved an issue where using the clear tunnel command when no tunnels were configured on the switch did not generate an error message.
- Resolved an issue where the custom Web Portal feature was calling an incorrect file name.
- Resolved an issue where short packet error messages were generated on the switch.
- Resolved an issue where counter errors caused problems on the switch by exceeding the queue depth limit.
- Resolved an issue where all switch platforms other than the RBT-8500 and RBT-8400 now support automatic grouping of users with the same ACL. The ACL is mapped to the group instead of the user which greatly improves scaling and performance.
- Resolved an issue where some APs were generating beacon loss events on the network.
- Resolved an issue where, when the number of sessions on the switch reached the maximum limit, the switch generated socket errors.

Firmware Release 7.0.9.8:

- Resolved an issue where 802.11b protection mode was not correctly initialized on some AP platforms.
- Resolved an issue where Mesh services and bridging temporarily experienced service interruptions.
- Resolved a timing issue on the AP transmit buffer to better support 802.11n client chip sets.
- Resolved an issue where some load-balancing packets caused the RBT to cease responding on the network.
- Resolved an issue where incorrect radios were displayed when Tunisia was selected as the country code.
- Resolved an issue where certain channels for DFS2 were not enabled.
- Resolved an issue where certificates were not displayed after the related command was issued.
- Resolved an issue where an older AP did not boot correctly in a cluster configuration.
- Resolved an issue where bad packets on the network caused the RBT to cease responding on the network.
- Resolved an issue where BPDU packets were returned on the same port that the packets were sent out.
- Resolved an issue where Mesh AP packets were not duplicated on the network and prevented the Mesh feature from performing as expected.
- Resolved an issue where notifications were sent about the power change on an AP even if auto-tuned was not configured.
- Resolved an issue where configuration changes were not processed correctly when sent from the cluster seed.
- Resolved an issue where the transmit underrun message had the incorrect severity level.
- Resolved an issue with VLANs not rekeying that occurred when unicast and multicast ciphers were different.
- Resolved an issue where using the command "show sessions network ap <apnum>" displayed incorrect output.
- Resolved an issue where an AP configured with a static IP address would not boot up on the network.
- Resolved an issue where out of date information caused certain country codes to be unsupported.
- Resolved an issue where corrupted or unrecognized frames were incorrectly interpreted by the AP.
- Resolved an issue where special characters in URLs were incorrectly interpreted by the controller.
- Resolved an issue where log messages displayed timestamps that were inconsistent with the RBT system clock.
- Resolved an issue where Mesh APs did not function as expected due to rate adaptation errors.
- Resolved an issue where spanning tree state or port group membership was read and stored incorrectly.
- Resolved an issue where the transmitted BSSID in the multicast packet did not match the BSSIDs on the AP.
- Resolved an issue where the 802.11n adapter was incompatible with Spectralink Voice Protocol (SVP) enabled service profiles.

CUSTOMER RELEASE NOTES

Firmware Release 7.0.7.3:

Resolved an issue where static WEP keys did not work for some service profiles.
Resolved an SNMP error that caused an AP to become unresponsive.
Resolved an issue where the RBT-8500 became unresponsive on the network.
Resolved an issue where a large number of user sessions caused the Web portal login page to become inaccessible.
Resolved an issue where merging configurations between the primary and secondary seed caused the RASs to become unresponsive.
Resolved an issue where using a question mark symbol in a Web AAA page URL caused the page to not display properly.
Resolved an issue where the TCP connection to the RAS did not close immediately after sending a 403 error in response to a request from a Skype client.
Resolved an issue where a corrupted cluster configuration update caused the RAS to become unresponsive.
Resolved an issue where configuring multiple user groups and using local authentication for web logins caused the RAS to become unresponsive.
Resolved an issue where MSS did not report the maximum transmit power on any particular channel as a proxy for the maximum power allowed by the regulatory domain.
Resolved an issue where a large number of location policies caused the cluster configuration to be unresponsive.
Resolved an issue where the show network verbose command displayed the incorrect output in the CLI.
Resolved an issue where upgrading to a later version of MSS caused the RAS to become unresponsive.
Resolved an issue where a corrupted control packet caused the AP to become unresponsive.
Resolved an issue where an invalid IGMP message caused the RAS to become unresponsive.
Resolved a problem where some 802.11n wireless adapters experienced packet loss on wireless services with the SVP enabled. Existed only on the MP-432.
Resolved a TCP buffer issue that caused a RAS within a Mobility Domain to crash.
Resolved a corrupt control packet issue causing APs to become unresponsive and reset.
Resolved an issue that, when using MacOS, an unsupported protocol option would cause SSH admin connections to fail.
Resolved an issue where Auto-tune's lower boundary was not implemented for AP power tuning.
Resolved an issue where an invalid AP configuration caused the RAS to become unresponsive.
Resolved an issue where a large number of EAP offload sessions caused the RAS to crash.
Resolved an issue where, in certain configurations, the RAS incorrectly reports channel configuration.

Firmware Release 7.0.5.6:

Resolved an error message: "network: radio_decode_data: read A-MSDU subframe snap header failed" occurred on the network.
Resolved an issue that caused MIC errors on the network when configuring WPA TKIP.
Resolved an RBT-8500 memory corruption at cfg_memory.c error message that caused network problems.
Resolved an issue where the RBT-8xxx sent too many access requests to the RADIUS server after configuring RADIUS to authenticate users with EAP-TLS, or EAP-PEAP.
Resolved an issue where SSIDs using "#" as part of the name were not accepted in the configuration.
Resolved an issue with Internet Explorer and WebView where the date format was displayed incorrectly.
Resolved an issue reloading a configuration with cluster mode enabled prevented RASM from determining the active seed.
Resolved an issue with clients that could not re-associate without first authenticating on the network.
CAPWAP data plane UDP port changed from 5001 to 5247.
Resolved an issue when using telnet over a WAN link adversely affected the telnet session.
Resolved an issue when using the active-scan feature triggered packet loss on legacy AP's/ RASs with older Intel wireless adaptors.

You should check our web site on a regular basis for updates at <http://www.enterasys.com/products/wireless/>.

KNOWN RESTRICTIONS AND LIMITATIONS:

Firmware Release 7.0.12.2:

If an AP has vlan-tagging enabled, it will not boot in bridging mode.

Description – The static vlan tag is not supported in mesh/bridging. It is not a valid configuration to enable both at the same time.

Workaround — No workaround available at this time.

Auto-Tune power failures on Enterasys Access Points

Description—The RBT-1002, RBT-4102, and RBT3K-AG units when using Auto-Tune for power, will gradually tune down to a value of 1db.

Workaround— Manually set the output power to a static value. A fix will be added in the next release to resolve this issue.

Using the global load-balancing command does not load-balance traffic on AP's across the network appropriately.

Description—Load balancing on every AP should be enabled or disabled (implicit value or set by user). This value has a higher priority than the global setting so the global setting is always ignored.

Workaround—To configure global load-balancing, use the following two commands:

set ap 1-9999 radio 1 load-balancing [enable | disable]

set ap 1-9999 radio 2 load-balancing [enable | disable]

Mesh services does not allow multiple encryptions in a mesh configuration.

Description— If you have previously enabled TKIP, WEP40, or WEP104, mesh services do not work properly and do not associate on the network.

Workaround— Before you upgrade to MSS 7.0.12.2, disable these encryption methods on the mesh profile.

The aggregate throughput exceeds the bandwidth limit of the SSID.

Description — Per SSID max-bw is only enforced within the scope of one radio. Therefore, if you configure multiple SSIDs per radio and configure bandwidth management on the SSIDs, you can exceed the bandwidth for each SSID.

Workaround—Configure bandwidth management on a per radio basis. The limits for service-profile max-bw and service-profile cac-session are enforced independently on each radio.

Upgrading from MSS 6.0 to MSS 7.0 changes the antenna location from Indoor to Outdoor on the AP.

Description—If an AP is configured with the antenna location as Indoor and you upgrade a MSS version from anything prior to MSS 6.0.10.2 to 7.0, the antenna location changes to Outdoor.

Workaround — Reconfigure the antenna with the proper location after upgrading the MSS version.

Changes to the DTD cause incompatibility with cluster configuration.

Description— MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members.

Workaround—All switches in a cluster configuration should have the same version of MSS.

Using the quickstart command on the MX-2800 incorrectly sets VLAN tag ID.

Description — When configuring the MX-2800 using the quickstart command, it is possible to configure an invalid VLAN tag value for the default management VLAN.

Workaround — After completing the quickstart configuration, create a new VLAN with the correct VLAN tag.

Using the auto-ap feature does not allow load balancing on individual radios.

Description — When using the auto-ap feature, it is not possible to set all of the AP attributes. Per-AP load-balancing control is not supported on auto-ap. The system global settings for load balancing apply to all auto-aps.

Workaround — If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.

Auto-aps do not behave correctly on cluster seed when the maximum number of APs is configured.

Description — When a cluster seed switch boots an auto-ap, it checks the seed configuration on the switch to determine if the cluster can support any additional AP's. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly.

Workaround — Reduce the number of configured APs in the cluster configuration.

Firmware Release 7.0.12.2:

Voice handsets can be sensitive to changes on an in-service SSID.

Description — Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.

Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.

The time and date do not synchronize with an NTP server, if the NTP client on the switch is enabled before the NTP service is started on the server.

Firmware Release 7.0.9.8:

Using Webview to create custom webportal pages can cause the RBT switch to become unresponsive.

Description — In certain circumstances, when using the Webview interface to create a custom webportal login page, the Webview interface becomes unresponsive.

Workaround — Create custom webportal pages with an external tool and upload them to the RBT switch using the CLI.

The aggregate throughput exceeds the bandwidth limit of the SSID.

Description — Per SSID max-bw is only enforced within the scope of one radio. Therefore, if you configure multiple SSIDs per radio and configure bandwidth management on the SSIDs, you can exceed the bandwidth for each SSID.

Workaround — Configure bandwidth management on a per radio basis. The limits for service-profile max-bw and service-profile cac-session are enforced independently on each radio.

Upgrading from MSS 6.0 to MSS 7.0 changes the antenna location from Indoor to Outdoor on the AP.

Description — If an AP is configured with the antenna location as Indoor and you upgrade the MSS version from 6.0 to 7.0, the antenna location changes to Outdoor.

Workaround — Reconfigure the antenna with the proper location after upgrading the MSS version.

Changes to the DTD cause incompatibility with cluster configuration.

Description — MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members.

Workaround — All RASs in a cluster configuration should have the same version of MSS.

Using the quickstart command on the MX-2800 incorrectly sets VLAN tag ID.

Description — When configuring the MX-2800 using the quickstart command, it is possible to configure an invalid VLAN tag value for the default management VLAN.

Workaround — After completing the quickstart configuration, create a new VLAN with the correct VLAN tag.

Using the auto-ap feature does not allow load balancing on individual radios.

Description — When using the auto-ap feature, it is not possible to set all of the AP attributes. Per-AP load balancing control is not supported on auto-ap. The system global settings for load balancing apply to all auto-aps.

Workaround — If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.

Auto-aps do not behave correctly on cluster seed when the maximum number of APs are configured.

Description — When a cluster seed RBT-8xxx boots an auto-ap, it checks the seed configuration on the RBT-8xxx to determine if the cluster can support any additional AP's. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly.

Workaround — Reduce the number of configured APs in the cluster configuration.

Voice handsets can be sensitive to changes on an in-service SSID.

Description — Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.

Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.

Firmware Release 7.0.7.3:
<p>802.11n adapter incompatibility with Spectralink Voice Protocol (SVP) enabled service profiles.</p> <p>Description — Some 802.11n wireless adapters may experience packet loss on wireless services with the Spectralink Voice Protocol enabled. This problem only exists when using the MP-432 with frame aggregation enabled.</p> <p>Workaround — When using SVP on the MP-432 disable frame aggregation.</p>
<p>The aggregate throughput exceeds the bandwidth limit of the SSID.</p> <p>Description — Per SSID max-bw is only enforced within the scope of one radio. Therefore, if you configure multiple SSIDs per radio and configure bandwidth management on the SSIDs, you can exceed the bandwidth for each SSID.</p> <p>Workaround — Configure bandwidth management on a per radio basis. The limits for service-profile max-bw and service-profile cac-session are enforced independently on each radio.</p>
<p>Upgrading from MSS 6.0 to MSS 7.0 changes the antenna location from Indoor to Outdoor on the AP.</p> <p>Description — If an AP is configured with the antenna location as Indoor and you upgrade the MSS version from 6.0 to 7.0, the antenna location changes to Outdoor.</p> <p>Workaround — Reconfigure the antenna with the proper location after upgrading the MSS version.</p>
<p>Changes to the DTD cause incompatibility with cluster configuration.</p> <p>Description — MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members.</p> <p>Workaround — All RASs in a cluster configuration should have the same version of MSS.</p>
<p>Using the quickstart command on the MX-2800 incorrectly sets VLAN tag ID.</p> <p>Description — When configuring the MX-2800 using the quickstart command, it is possible to configure an invalid VLAN tag value for the default management VLAN.</p> <p>Workaround — After completing the quickstart configuration, create a new VLAN with the correct VLAN tag.</p>
<p>Using the auto-ap feature does not allow load balancing on individual radios.</p> <p>Description — When using the auto-ap feature, it is not possible to set all of the AP attributes. Per-AP load balancing control is not supported on auto-ap. The system global settings for load balancing apply to all auto-aps.</p> <p>Workaround — If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.</p>
<p>Auto-aps do not behave correctly on cluster seed when the maximum number of APs are configured.</p> <p>Description — When a cluster seed RBT-8xxx boots an auto-ap, it checks the seed configuration on the RBT-8xxx to determine if the cluster can support any additional AP's. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly.</p> <p>Workaround — Reduce the number of configured APs in the cluster configuration.</p>
<p>Voice handsets can be sensitive to changes on an in-service SSID.</p> <p>Description — Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.</p> <p>Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.</p>
<p>Some RAS controllers show an incorrect CPU load.</p> <p>Description — RAS controllers show an erroneous CPU load of 100% in the command line interface. This will be fixed in the next version of MSS.</p> <p>Workaround — None.</p>

Firmware Release 7.0.5.6:

802.11n adapter incompatibility with Spectralink Voice Protocol (SVP) enabled service profiles.

Description — Some 802.11n wireless adapters may experience packet loss on wireless services with the Spectralink Voice Protocol enabled. This problem only exists when using the MP-432 with frame aggregation enabled.

Workaround — When using SVP on the MP-432 disable frame aggregation.

The aggregate throughput exceeds the bandwidth limit of the SSID.

Description — Per SSID max-bw is only enforced within the scope of one radio. Therefore, if you configure multiple SSIDs per radio and configure bandwidth management on the SSIDs, you can exceed the bandwidth for each SSID.

Workaround — Configure bandwidth management on a per radio basis. The limits for service-profile max-bw and service-profile cac-session are enforced independently on each radio.

Upgrading from MSS 6.0 to MSS 7.0 changes the antenna location from Indoor to Outdoor on the AP.

Description — If an AP is configured with the antenna location as Indoor and you upgrade the MSS version from 6.0 to 7.0, the antenna location changes to Outdoor.

Workaround — Reconfigure the antenna with the proper location after upgrading the MSS version.

Changes to the DTD cause incompatibility with cluster configuration.

Description — MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members.

Workaround — All RASs in a cluster configuration should have the same version of MSS.

Using the quickstart command on the MX-2800 incorrectly sets VLAN tag ID.

Description — When configuring the MX-2800 using the quickstart command, it is possible to configure an invalid VLAN tag value for the default management VLAN.

Workaround — After completing the quickstart configuration, create a new VLAN with the correct VLAN tag.

Using the auto-ap feature does not allow load balancing on individual radios.

Description — When using the auto-ap feature, it is not possible to set all of the AP attributes. Per-AP load-balancing control is not supported on auto-ap. The system global settings for load balancing apply to all auto-aps.

Workaround — If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.

Auto-aps do not behave correctly on cluster seed when the maximum number of APs are configured.

Description — When a cluster seed RBT-8xxx boots an auto-ap, it checks the seed configuration on the RBT-8xxx to determine if the cluster can support any additional AP's. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly.

Workaround — Reduce the number of configured APs in the cluster configuration.

Voice handsets can be sensitive to changes on an in-service SSID.

Description — Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.

Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.

Firmware Release 7.0.4.3:

Changes to the DTD cause incompatibility with cluster configuration.

Description — RoamAbout MSS Cluster Configuration relies on configuration options being consistent between cluster members. Changes to configuration options introduced between releases can result in synchronization problems between cluster members.

Workaround — All RASs in a cluster configuration should have the same version of RoamAbout MSS.

Using the auto-ap feature does not allow load-balancing on individual radios.

Description — When using the auto-ap feature, it is not possible to set all of the AP attributes.

Per AP load-balancing control is not supported on auto-ap. The system global settings for load-balancing apply to all auto-aps.

Workaround — If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.

Using telnet over a WAN link may affect the telnet session.

Description — When using telnet to manage a RAS over a high-latency WAN link, it is possible for the telnet session to stop responding.

Workaround — Restart the telnet session.

Auto-aps do not behave correctly on cluster seed when the maximum number of APs is configured.

Description — When a cluster seed RAS boots an auto-ap, it checks the seed configuration on the RAS to determine if the cluster can support any additional APs. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly.

Workaround — Reduce the number of configured APs in the cluster configuration.

Voice handsets can be sensitive to changes on an in-service SSID.

Description — Particular voice handsets are sensitive to changes made to an in-service SSID.

This can result in the handset operating with stale connection information.

Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.

The time and date do not synchronize with an NTP server, if the NTP client on the RAS is enabled before the NTP service is started on the server.

Firmware Release 7.0.3.7:

Description — If you reload a switch configuration with cluster mode turned on, RASM cannot determine which RoamAbout switch is the active seed in the cluster configuration. (53952)

Workaround — Disable cluster mode and then re-enable it. Normal operation resumes on the network.

Using the auto-ap feature does not allow load-balancing on individual radios. (53331)

Description — When using the auto-ap feature, it is not possible to set all of the AP attributes. Per AP load-balancing control is not supported on auto-ap. The system global settings for load-balancing applies to all auto-aps. (53331)

Workaround — If you must configure a load-balance group for a specific AP, configure the AP as a regular AP.

Using telnet over a WAN link may affect the telnet session. (52853)

Description — When using telnet to manage a RoamAbout switch over a high-latency WAN link, it is possible for the telnet session to stop responding. (52853)

Workaround — Restart the telnet session.

Auto-aps do not behave correctly on cluster seed when the maximum number of APs is configured. (52633)

Description — When a cluster seed RoamAbout switch boots an auto-ap, it checks the seed configuration on the RoamAbout switch to determine if the cluster can support any additional APs. If the system is already configured with the maximum number of APs allowed, new auto-aps do not operate correctly.

Workaround — Reduce the number of configured APs in the cluster configuration.

CAPWAP data plane UDP port changed from 5001 to 5247. (53029)

Description — The UDP port for CAPWAP data packets has changed from 5001 to 5247 to comply with the updated CAPWAP specification. You may experience problems with roaming VLANs between RoamAbout switches with MSS Version 7.0 and RoamAbout switches with earlier versions of MSS.

Workaround — If your network configuration requires tunneled VLANs, be sure that all RoamAbout switches on the network are configured with the same version of MSS.

Firmware Release 7.0.3.7:

Using the active-scan feature triggers packet loss on legacy APs with older Intel wireless adaptors. (50901)

Description — When using active-scan on legacy APs with the Intel 2915 wireless adaptor, a station may experience some level of packet loss. (50901)

Workaround — Disable active-scan on any legacy APs supporting older Intel clients.

Voice handsets can be sensitive to changes on an in-service SSID. (41603)

Description — Particular voice handsets are sensitive to changes made to an in-service SSID. This can result in the handset operating with stale connection information.

Workaround — When using affected handsets, disable the Service Profile prior to making any configuration changes.

The time and date do not synchronize with an NTP server, if the NTP client on the RoamAbout switch is enabled before the NTP service is started on the server. (20382)

For the most up-to-date information concerning known issues, go to the **Global Knowledgebase** section at <http://www.enterasys.com/support/>. To report an issue not listed in this document or in the **Global Knowledgebase**, contact our Technical Support Staff.

Tech Tip for Choosing External Antenna Types for the RBT-1602 (AP ID: AP1602 & AP1602C) and MP-422 (AP ID: MP422 & MP422A)

When you select an antenna type for the RBT-1602 and MP-422, the menu choices that are displayed are listed in the left-hand column in the table below. Use the antenna part numbers listed in the right-hand column to identify the correct menu choice.

RASM/RBT Antenna Choice:	Enterasys Antenna Part Number:
ANT1060	RBTES-BG-S1060
ANT1120	RBTES-BG-S07120
ANT1180	RBTES-BG-S06180
ANT5060	RBTES-AW-S1460
ANT5120	RBTES-AW-S12120
ANT5180	RBTES-AW-S10180

Tech Tip for the Channel availability for the new DFS2 model Access Points

DFS2 compliant Access Points support fewer channels than non-DFS2 compliant Access points.

Channel availability is based on the AP ID of the installed Access Point. An Access Point with the character of “A “ or “C” on AP ID label denotes a DFS2 compliant device. The country of operation and regulatory domain determine exactly what channels are available for use.

CUSTOMER RELEASE NOTES

IETF STANDARDS PROTOCOL SUPPORT:

Groups Supported	RFC No. / Title	Description
Security and AAA	RFC 2246	Transport Layer Security (TLS)
	RFC 2284	EAP
	RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
	RFC 2548	Microsoft RADIUS VSAs
	RFC 2716	PPP EAP-TLS Authentication Protocol
	RFC 2759	Microsoft PPP CHAP Extensions, Version 2
	RFC 2865	RADIUS Authentication
	RFC 2866	RADIUS Accounting
	RFC 2868	RADIUS Attributes for Tunnel Protocol Support
	RFC 2869	RADIUS Extensions
	RFC 2986	PKCS #10: Certification Request Syntax Specification Version 1.7
	RFC 3580	IEEE 802.1X RADIUS Guidelines
	RFC 3546	Transport Layer Security (TLS) Extensions
	draft-josefsson-pppext-eap-tls-eap	Protected EAP Protocol (PEAP)
	draft-kamath-pppext-peapv0-00.txt	Microsoft PEAP
	draft-kamath-pppext-eap-mschapv2	Microsoft EAP
CHAP extensions v2		
IEEE	IEEE Std 802.1X-2001	Port-Based Network Access Control
	IEEE Std 802.11i	Enhanced Security for 802.11 Wireless Networks Based on AES
	IEEE Std 802.11h	
	IEEE Std 802.11d	
Encryption	WEP and TKIP: RC4 40-bit and 104-bit	
	SSL and TLS: RC4 128-bit and RSA 1024-bit and 2048-bit	
	CCMP: AES 128-bit (FIPS-197)	
General	RFC 1122 Host Requirements	
	RFC 1393 Traceroute	
	RFC 1519 CIDR	
	RFC 1591 DNS (client)	
	RFC 1769 SNTP	
	RFC 768 UDP	
	RFC 783 TFTP	
	RFC 791 IP	
	RFC 792 ICMP	
	RFC 793 TCP	
	RFC 826 ARP	
	IEEE 802.1D Spanning Tree	
	IEEE 802.1Q VLAN Tagging	
IEEE 802.3ad (Static Config)		
IP Multicast	RFC 1112 IGMPv1	
	RFC 2236 IGMPv2	

CUSTOMER RELEASE NOTES

Groups Supported	RFC No. / Title	Description
Quality of Service	draft-ietf-idmr-igmp-mrdisc-09.txt	
	draft-ietf-magma-snoop-05.txt	
	RFC 2472 DiffServ Precedence	
	RFC 2597 DiffServ Assured Forwarding	
	RFC 2598 DiffServ Expedited Forwarding	

STANDARD MIB SUPPORT:

NOTE: MIB support for the RoamAbout System is for monitoring only.

RFC No:	Title:
RFC 1213	RFC1213-MIB
RFC 2863	IF-MIB
RFC 1493	BRIDGE-MIB
RFC 2674	Q-BRIDGE-MIB
RFC 2620	RADIUS-ACC-CLIENT-MIB
RFC 2618	RADIUS-AUTH-CLIENT-MIB
RFC 3418	SNMPv2-MIB

ENTERASYS NETWORKS PRIVATE ENTERPRISE MIB SUPPORT:

Title:	Title:
rbtws-system-mib	rbtws-basic-mib
rbtws-trap-mib	rbtws-ap-tc
rbtws-root-mib	rbtws-ap-status
rbtws-port-mib	rbtws-registration-mib
rbtws-info-rf-detect-mib	rbtws-client-session-mib
rbtws-external-server-mib	rbtws-client-session-tc

RADIUS STANDARD AND EXTENDED ATTRIBUTES SUPPORT:

For more information on the supported RADIUS attributes, please refer to the appendix entitled "Supported RADIUS Attributes" in the *Mobility System Software Configuration Guide*.

For more information on assigning authorization attributes, please refer to the chapter entitled "Configuring AAA for Network Users" in the *Mobility System Software Configuration Guide*.

RADIUS Authentication and Authorization Attributes

Attribute:	RFC Source:
Called-Station-Id	RFC2865, RFC3580
Calling-Station-Id	RFC2865, RFC3580
CHAP-Password	RFC2865
Class	RFC2865
Event-Timestamp	RFC2869
Filter-Id	RFC2865, RFC3580
NAS-Identifier	RFC2865, RFC3580

CUSTOMER RELEASE NOTES

Attribute:	RFC Source:
NAS-IP-Address	RFC2865, RFC3580
NAS-Port-Id	RFC2865, RFC3580
Reply-Message	RFC2865
Service-Type	RFC2865, RFC3580
Session-Timeout	RFC2865, RFC3580
State	RFC2865
Tunnel-Private-Group-ID	RFC3580
User-Name	RFC2865, RFC3580
User-Password	RFC2865
Vendor-Specific	See table below

RADIUS Accounting Attributes

Attribute:	RFC Source:
Acct-Authentic	RFC2866
Acct-Delay-Time	RFC2866
Acct-Input-Gigawords	RFC2866
Acct-Input-Octets	RFC2866
Acct-Input-Packets	RFC2866
Acct-Multi-Session-Id	RFC2866
Acct-Output-Gigawords	RFC2866
Acct-Output-Octets	RFC2866
Acct-Output-Packets	RFC2866
Acct-Session-Id	RFC2866
Acct-Session-Time	RFC2866
Acct-Status-Type	RFC2866

Vendor Specific Attributes

Attribute:	Type, Vendor ID, Vendor Type:
VLAN-Name	26, 14525, 1
Mobility-Profile	26, 14525, 2
Encryption-Type	26, 14525, 3
Time-Of-Day	26, 14525, 4
SSID	26, 14525, 5
End-Date	26, 14525, 6
Start-Date	26, 14525, 7
URL	26, 14525, 8

SNMP TRAP SUPPORT:

SNMP Trap	Description
APBootTraps	Generated when an access point boots.
APTimeoutTraps	Generated when an access point fails to respond to the RoamAbout Switch.
AuthenTraps	Generated when the RoamAbout Switch's SNMP engine receives a bad community string.
AutoTuneRadioChannelChangeTraps	Generated when the RF Auto-Tuning feature changes the channel on a radio.
AutoTuneRadioPowerChangeTraps	Generated when the RF Auto-Tuning feature changes the power

CUSTOMER RELEASE NOTES

SNMP Trap	Description
	setting on a radio.
ClientAssociationFailureTraps	Generated when a client's attempt to associate with a radio fails.
ClientAuthorizationSuccessTraps	Generated when a client is successfully authorized.
ClientAuthenticationFailureTraps	Generated when authentication fails for a client.
ClientAuthorizationFailureTraps	Generated when authorization fails for a client.
ClientClearedTraps	Generated when a client's session is cleared.
ClientDeAssociationTraps	Generated when a client is dissociated from a radio.
ClientDot1xFailureTraps	Generated when a client experiences an 802.1X failure.
ClientRoamingTraps	Generated when a client roams.
CounterMeasureStartTraps	Generated when MSS begins countermeasures against a rogue access point.
CounterMeasureStopTraps	Generated when MSS stops countermeasures against a rogue access point.
DAPConnectWarningTraps	Generated when an AP whose fingerprint has not been configured in MSS establishes a management session with the switch.
DeviceFailTraps	Generated when an event with an Alert severity occurs.
DeviceOkayTraps	Generated when a device returns to its normal state.
LinkDownTraps	Generated when the link is lost on a port.
LinkUpTraps	Generated when the link is detected on a port.
MichaelMICFailureTraps	Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.
MobilityDomainJoinTraps	Generated when the RoamAbout Switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.
MobilityDomainTimeoutTraps	Generated when a timeout occurs after a RoamAbout Switch has unsuccessfully tried to communicate with a seed member.
PoEFailTraps	Generated when a serious PoE problem, such as a short circuit, occurs.
RFDetectAdhocUserTraps	Generated when MSS detects an ad-hoc user.
RFDetectRogueAPTraps	Generated when MSS detects a rogue access point.
RFDetectRogueDisappearTraps	Generated when a rogue access point is no longer being detected.
RFDetectClientViaRogueWiredAPTraps	Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
RFDetectDoSPortTraps	Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.
RFDetectDoSTraps	Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.
RFDetectInterferingRogueAPTraps	Generated when an interfering device is detected.
RFDetectInterferingRogueDisappearTraps	Generated when an interfering device is no longer detected.
RFDetectSpoofedMacAPTraps	Generated when MSS detects a wireless packet with the source

CUSTOMER RELEASE NOTES

SNMP Trap	Description
	MAC address of an Enterasys AP, but without the spoofed AP's signature (fingerprint).
RFDetectSpoofedSsidAPTraps	Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.
RFDetectUnauthorizedAPTraps	Generated when MSS detects the MAC address of an AP that is on the attack list.
RFDetectUnauthorizedOuiTraps	Generated when a wireless device that is not on the list of permitted vendors is detected.
RFDetectUnauthorizedSsidTraps	Generated when an SSID that is not on the permitted SSID list is detected.
ApNonOperStatusTraps	Generated to indicate an AP radio is nonoperational.
ApOperRadioStatusTraps	Generated when the status of an AP radio changes.

GLOBAL SUPPORT:

By Phone: 978-684-1000
1-800-872-8440 (toll-free in U.S. and Canada)

For the Enterasys Networks Support toll-free number in your country:

<http://www.enterasys.com/support/>

By Email: support@enterasys.com

By Web: <http://www.enterasys.com/support/>

By Fax: 978-684-1499

By Mail: Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810 (USA)

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Enterasys Networks Support web site.