

CUSTOMER RELEASE NOTES

RoamAbout® Wireless Switch 8x00 Release **Firmware Version 4.1.11.0** **Updated: June 19, 2006**

INTRODUCTION:

The RBT-8x00 family of wireless switches include the following: 1) the RBT-8100, which has the ability to control up to 24 access points; 2) the RBT-8200, which has the ability to control 24/48/72 access points; and 3) the RBT-8400, which has the ability to control 40/80/120 access points. The RoamAbout Switch Manager can manage all of these devices.

The 4.1.11.0 Firmware release addresses various customer escalations and internal fixes (please see the *Firmware Changes and Enhancements* section below).

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

NOTE: If you are using a 4.0 firmware image/software, Enterasys recommends that you upgrade the RoamAbout Switch Manager (RASM) to firmware version 4.1.9.0 BEFORE upgrading your RBT-8x00 wireless switches to firmware version 4.1.11.0.

NOTE: If you are upgrading a pre-existing AP4102 or AP4102-EU model Access Point from 4.1.4 or earlier, please read the instructions listed in the *Firmware Changes and Enhancements* section on page 4 of the RoamAbout Switch Manager (RASM) 4.1.9 Release Notes.

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Release	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

HARDWARE COMPATIBILITY:

Switches RBT-8100, RBT-8200, and RBT-8400, Thin Access Points RBT-1002, RBT-1002-EU, and Thin-mode Access Points RBT-4102, RBT-4102-EU, RBT-1602, and RBT3K-AG.

CUSTOMER RELEASE NOTES

NETWORK MANAGEMENT SOFTWARE SUPPORT:

NMS Platform	Version No.	Module No.
RoamAbout Switch Manager 50 Access Point User License	4.1.9.0	RBT-NMS-50
RoamAbout Switch Manager 200 Access Point User License	4.1.9.0	RBT-NMS-200
RoamAbout Switch Manager unlimited User License	4.1.9.0	RBT-NMS-UNL
RoamAbout RF Planning Tool	4.1.9.0	RBT-RFPLAN

RBT-8400 Platform	Version No.	Module No.
RBT-8400 40 Additional Access Point Upgrade License	4.1.11.0	RBT-8400-40
RBT-8400 80 Additional Access Point Upgrade License	4.1.11.0	RBT-8400-80
RBT-8200 Platform	Version No.	Module No.
RBT-8200 24 Additional Access Point Upgrade License	4.1.11.0	RBT-8200-24

SUPPORTED FUNCTIONALITY:

Refer to the RoamAbout Switch Manager (RASM) Software 4.1.9.0 release notes for detailed features.

INSTALLATION AND CONFIGURATION NOTES:

In general, the RoamAbout Wireless Switch RBT-8x00 has been, or is being, shipped to you with a previous firmware version. Please refer to the appropriate *RBT-8x00 Quick Start* or the *RBT-8x00 Installation Guide* for hardware installation information. Please refer to the next section, [Upgrading the RBT-8xxx Switches](#), for upgrading information and procedures.

UPGRADING THE RBT-8X00 SWITCHES FROM PREVIOUS 4.0.X VERSIONS:

To upgrade an RBT-8100 switch, the switch must be running RAS (RoamAbout Switch) version 4.0.4.0 or later. To upgrade an RBT-8400, the switch must be running RAS version 4.0.16.0 or later.

Note: The following upgrade procedures refer to all RBT-8x00 switches.

Preparing the RBT Switch for the Upgrade

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 might not be converted correctly.

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

```
RBT-8100# save config [filename]
```

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

```
RBT-8100# backup system [tftp://ip-addr/]filename [all | critical]
```

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

```
RBT-8100# 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*, chapter 20.

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/download.cgi?lib=csiws> 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-8100# reset system [force]
```

After resetting the RAS, the switch boots using the new RAS image. The switch also sends the DAP (Distributed Access Point) version of the new boot image to the DAPs and restarts the DAPs. After a DAP restarts, it checks the version of the new DAP boot image to make sure the boot image is newer than the boot image currently installed on the DAP. If the boot image is newer, the DAP completes installation of its new boot image by copying the boot image into the DAP’s flash memory, which takes about 30 seconds, then restarts again. The upgrade of the DAP is complete after the second restart.

Upgrade Scenario:

To upgrade an RBT-8x00 switch from one RAS Version to another, type commands such as the following.

Note: This upgrade scenario uses the firmware image file 4.1.11.0 to show the download features. Please follow these procedures for any of the 4.0.x and 4.1.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-8100# save config success: configuration saved.
RBT-8100# backup system tftp://[ip-addr]/sysa_bak success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
RBT-8100# copy tftp://[ip-addr]/RB104111.REL boot1:RB104111.REL success: received 9629696 bytes in 14.343 seconds [ 671386 bytes/sec]
RBT-8100# set boot partition boot1 success: Boot partition set to boot1.
```

```
RBT-8100# show boot
Configured boot version:      4.1.11.0
Configured boot image:       boot1:RB104111.REL
Configured boot configuration: file:configuration
Booted version:              4.1.5.0
Booted image:                boot0:RB104105.REL
Booted configuration:        file:configuration
Product model:               RBT-8100
```

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

To upgrade the RBT-8x00 switch to the released version, please refer to the “Managing and Monitoring Your Network” chapter, section “Distributing Image and Configuration Files” in the *RoamAbout Switch Manager User’s Guide*.

FIRMWARE CHANGES AND ENHANCEMENTS:

Firmware Release 4.1.11.0:

- Added support for the following countries in the RBT-4102-EU and RBT-1002-EU AP models:

AU	AUSTRALIA	VN	VIETNAM
CN	CHINA	EG	EGYPT
IN	INDIA	KW	KUWAIT
JP	JAPAN (W52/W53)	IL	ISRAEL
KR	KOREA, REPUBLIC OF	SA	SAUDI ARABIA
MY	MALAYSIA	AE	UNITED ARAB EMIRATES
NZ	NEW ZEALAND	AR	ARGENTINA
PH	PHILIPPINES	BR	BRAZIL
SG	SINGAPORE	VE	VENEZUELA
TW	TAIWAN	ZA	SOUTH AFRICA
TH	THAILAND		

- Added support for the RBT-4102 North American Access Point.
- Resolved an issue where RBT-1602s would reset every 18 hours and report a fingerprint mismatch error.
- Resolved an issue where the RBT-1602 would report a power level outside its regulatory limits, causing a configuration mismatch.
- Resolved an issue where the RBT-1002 DAPs would not boot up due to a switch and homologation configuration download timing issue (switch DAP configuration would get pushed down before the homologation information had finished processing).

- Resolved an issue where WPA2 clients roaming through the mobility domain would resend their RADIUS authentication information, forcing a re-association.
- Resolved an issue where the RBT-8100 would core dump after processing a serial debug command.
- Resolved an issue where the RBT-8400 eeprom (nvram) settings were corrupted after code upgrade.

Note: Refer to the [Tech Tip](#) on page 7 for important information about configuring antenna types for an RBT-1602 Access Point.

Firmware Release 4.1.5.0:

- The AP1102 and AP1102-EU names have been changed to AP4102 and AP4102-EU. If you are installing this code onto pre-existing AP4102-EU models (with 4.1.4.0 firmware), then please refer to the RoamAbout Switch Manager (RASM) 4.1.5 Release Notes for complete instructions to upgrade your AP correctly.
- Resolved an issue where the DAPs were not responding to the bias settings correctly for AP redundancy.

Firmware Release 4.1.4.0:

- Added support for the RBT-8200 RAS, and the RBT-1002-EU and RBT-4102-EU Access Points.
- Resolved an issue where the RBT-8100 would crash after a dot1x authentication using MSCHAPv2.
- Resolved an open issue dealing with the configuration and operation of Third-Party APs.
- Resolved an issue where the Called-Station-ID RADIUS attribute was not returning from the RoamAbout Switches.
- Resolved an issue where the RBT-8100 Ethernet ports could be enabled for PoE (ETS only supports Distributed Access Points, and while the directly connected access point configuration will work, it is not a supported configuration).
- Resolved a netsys:core dump issue which occurred after issuing a reset DAP command.
- Resolved a DNS memory issue when the DNS functionality was disabled and the RBT-8100 auto-configuration was enabled.

Firmware Release 4.0.21.0:

- Resolved an issue where ACLs were not properly assigned to users due to the incorrect parsing of the Enterasys filter ID string (Enterasys:version=1:policy=<policy name>) returned from a RADIUS server.
- The default MAC authentication RADIUS password has been changed from 'nopassword' to 'NOPASSWORD'.

Firmware Release 4.0.20.0:

- Added support for the RBT-1602 Access Point.
- Increased the limit of local mac authenticated users from 75 to 2400 (this fix was originally listed in the 4.0.18.0 Firmware Release section, but the implementation did not occur until this 4.0.20.0 release).
- Resolved the issue where a WebAAA user would not be redirected to a web page if the proxy setting was enabled.

Firmware Release 4.0.18.0:

- MTU for tunnelled traffic was too long — Previous versions of MSS required an IP Path MTU (PMTU) of 1484 bytes for tunneled traffic, and used a non-standard implementation of IP Fragmentation to transport IP datagrams larger than that PMTU. Because of the non-standard fragmentation, tunnel IP datagrams could be dropped by devices attempting to validate packets for proper formatting. The current MSS version fixes this issue. IP Fragmentation is supported in accordance with RFC 2003. This change allows third-party devices in the communication path to properly validate fragmented tunnel IP datagrams. In addition, the maximum packet size is smaller. In the current MSS version, the PMTU requirement has been reduced to 1384 bytes, to allow devices along the communication path to further encapsulate the tunnel packets without introducing additional fragmentation.
- Resolved an issue where associated clients (to clear SSID) could access WebView and changing system configurations.

Firmware Release 4.0.16.0:

- Added support for the RBT-8400 RAS and the RBT-1002 Access Point.
- Resolved an issue where MAC addresses would be dropped from the Filter Database without the session timing out (fdb hashing error in the database).
- Resolved an issue where the RBT-8100 would have a core dump after trying to save a configuration file with a name longer than 16 characters.
- Resolved an issue where a user would not get a DHCP address using WebAAA and the internal DHCP server on the RBT-8100.
- Resolved the password recovery method, where the “Esc” prompt during the RBT-8100 boot-up cycle appeared too late in the boot-up cycle.
- Resolved an issue where the Service Profile would only allow a 16-character name.

Firmware Release 4.0.7.0:

- Fixed an issue where Distributed APs would reset across a routed network.
- Fixed an issue with RBT-8100 port auto-negotiation.
- Fixed an issue when an RBT-8100 would display the wrong prompt values after clearing the system configuration.

Firmware Release 4.0.4.0:

- Initial Release for the RBT-8100 RAS and the RBT3K-AG Access Point in thin mode.

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 4.1.11.0:

Due to the AP name change from AP1102-EU to AP4102-EU in both the RBT-8x00 firmware and RASM management application, these devices will need to be re-associated to a coverage area in the RF Planning Tool.
An Auto-DAP issue on the RBT-8200 only seen in the lab, where the RBT-8200 will accept an Auto-DAP after the DAP has been converted to a configured DAP. The Auto-DAP mode is disabled. The workaround at this time is to reset the Auto-DAP ID, or reset the RBT-8200, after verifying that the Auto-DAP feature is disabled.
Clients using the RBTBG/RBTBJ wireless client card with the RBTBX-PC wireless PCI NIC adapter have experienced extended periods of traffic loss (up to 33% ping loss over a ten-minute time span).
There is an open issue when using RASM to modify the RBT configuration where certain Policy settings will not get applied to the RBT switch.
There is an open issue with unexplained decrypt errors from clients when using a static WEP authorization profile.
Upgrading the RBT switch from 4.0.21 to a 4.1.4 or greater firmware will fail if there is a banner MOTD with multiple returns in the configuration. The workaround is to boot your system back to the 4.0.21 code, remove the banner MOTD, then upgrade to 4.1 and reenter the banner MOTD message.
The external antenna names for the RBT-1602 AP have not been converted to the Enterasys specific naming convention. Note: Refer to the Tech Tip on page 7 for important information about configuring antenna types for an RBT-1602 Access Point.
If you use a location policy/ACL, you will overwrite the web-portal ACL and cause Web-portal to fail. This is not a supported configuration.
Disabling the dot1x authcontrol function may cause authentication issues. This is a global setting, reaching many portions of the authentication code. It should remain enabled at all times unless specifically directed to disable it. This does NOT turn on dot1x on any of the SSIDs.
ACL names can contain special characters (/,\,-,_), but they cannot contain spaces. ACL names must also begin with a letter and not a number.
Issue under investigation at time of release: Due to a hardware limitation for the RBT3K, the lowest achievable power setting is 10 dB (lowest setting).
The RBT-8400 supports 1, 2, 3 and 4 1Gb link connections only.
The unmanaged RBT3K (fat-AP) may encounter conversion upgrade issues to managed mode (thin-AP) across a routed network.
A single "*" used for User Glob does not work when using TLS.
WEP keys cannot be entered in ASCII format.
The RBT-1002 does not support the automatic generation of RSA values (fingerprints). The dynamic creation of the fingerprint occurs on Access Points that are 'fat-to-thin' conversion types.

Tech Tip for Choosing External Antenna Types for the RBT-1602

When you select an antenna type for the RBT-1602, the menu choices that are displayed are listed in the left-hand column in the table below. Use the antenna part numbers listed the 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

CUSTOMER RELEASE NOTES

Please report any problems other than those listed above to our Technical Support Staff.

IETF STANDARDS MIB 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 2869	RADIUS Extensions
	RFC 2986	PKCS #10: Certification Request Syntax Specification Version 1.7
	RFC 3580	IEEE 802.1X RADIUS Guidelines
	draft-ietf-tls-extensions	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)	

CUSTOMER RELEASE NOTES

Groups Supported	RFC No. / Title	Description
IP Multicast	RFC 1112 IGMPv1	
	RFC 2236 IGMPv2	
	draft-ietf-idmr-igmp-mrdisc-09.txt	
	draft-ietf-magma-snoop-05.txt	
Quality of Service	RFC 2472 DiffServ Precedence	
	RFC 2597 DiffServ Assured Forwarding	
	RFC 2598 DiffServ Expedited Forwarding	

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 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.

CUSTOMER RELEASE NOTES

SNMP Trap	Description
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 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 MP radio is nonoperational.
ApOperRadioStatusTraps	Generated when the status of an MP 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/services/support/contact/>

By Email: support@enterasys.com

By Web: <http://www.enterasys.com/services/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.