

CUSTOMER RELEASE NOTES

RoamAbout® Switch Manager – Patch Release Version 5.0.9.2 March 2, 2007

INTRODUCTION:

The RoamAbout Switch Manager (RASM) software tools (RBT-NMS-50, RBT-NMS-200, RBT-NMS-UNL, and RBT-RFPLAN) are used to plan, configure, deploy, and monitor the RBT-8100, RBT-8110, RBT-8200, RBT-8210, and RBT-8400 RoamAbout switches, the TRPZ-MXR-2 wireless switch, the thin RBT3K-AG (AP-3000), RBT-1002, RBT-1002-EU, RBT-1602, and the thick/thin RBT-4102 and the RBT-4102-EU Access Points, the previously released MX-20 and MX-400 wireless switches, the outdoor MP-620 AP, and the MP-372 AP.

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

NOTICE: A Patch Release contains a small set of specific feature corrections which has not been subjected to the same standard of regression testing that a Generally Available Release would include. A Patch Release has been tested only to confirm that the specific feature set is functioning as expected. Unless otherwise stated in the Release Notes, a Patch Release has the same restrictions and limitations as the code upon which it was based. Please read *all* of the Release Notes pertaining to the Generally Available release prior to installation of any Patch in your production network. Please report any undocumented issues you find using the normal technical support procedures found in your product documentation.

NOTE: The 5.0.9.2 RoamAbout Switch Manager code fully supports the 5.0.10.3 RoamAbout Wireless Switch Firmware.

NOTE: If you are upgrading a pre-existing AP4102 or AP4102-EU model Access Point from 4.1.4.0 or earlier, please read the instructions listed in the [Firmware Changes and Enhancements on page 8](#).

NOTE: For the calendar year 2007, please be aware that the United States Daylight savings time period begins March 11, 2007, and ends November 4, 2007. Please 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.

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	5.0.9.2	Customer Patch	March 2007
Previous Version	5.0.8.1	Customer	January 2007
Previous Version	5.0.6.1	Customer	December 2006
Previous Version	4.2.5.1	Customer	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	February 2006
Previous Version	4.0.18.0	Customer	November 2005
Previous Version	4.0.16.0	Customer	September 2005

CUSTOMER RELEASE NOTES

Status	Version No.	Type	Release Date
Patch Release	4.0.7.0	Customer	August 2005
Initial Release Version	4.0.4.0	Customer	July 2005

HARDWARE COMPATIBILITY:

Switches:

- RBT-8100, RBT-8110, RBT-8200, RBT-8210, RBT-8400, TRPZ-MXR-2, MX-400, and MX-20.

Thin Access Points:

- RBT-1002, RBT-1002-EU, RBT-1602, the outdoor TRPZ-MP-620 Access Point, thin-RBT-4102, thin-RBT3K-AG, MP-372

Standalone Access Points:

- RBT-4102, RBT-4102-EU, and RBT3K-AG.

BOOTPROM COMPATIBILITY:

N/A

SYSTEM REQUIREMENTS:

Supported Platforms:

- Microsoft Windows Server 2003, Microsoft Windows XP with Service Pack 1 or higher, or Microsoft Windows 2000 with Service Pack 4
- SUSE Linux 9.1 and Red Hat WS 3

Hardware requirements to run the RASM client on Windows and Linux systems:

	Minimum	Recommended
Processor	Intel Pentium 4 2 GHz or equivalent	Intel Pentium 4 3 GHz or equivalent
RAM	512 MB	1 GB
Hard drive space available	100 MB	200 MB
Monitor resolution	1024x768 pixels, 24-bit color	1600x1200 pixels, 32-bit color
CD-ROM drive	CD-ROM or equivalent	CD-ROM

Hardware requirements to run RASM services on Windows and Linux systems:

	Minimum	Recommended
Processor	Intel Pentium 4 2.4 GHz or equivalent	Intel Pentium 4 3.6 GHz or equivalent
RAM	1 GB	2 GB
Hard drive space available	1 GB	2 GB
Monitor resolution	1024x768 pixels, 24-bit color	1600x1200 pixels, 32-bit color
CD-ROM drive	CD-ROM or equivalent	CD-ROM

SUPPORTED FUNCTIONALITY:**RASM Features for 5.0.9.2:**

RoamAbout Switch Manager 5.0 supports configuration and management of the following RBT switch enhancements:

- New WebView interface – Referred to as WebView 2, WebView now provides more configuration and management features, including numerous configuration wizards and a monitor dashboard.

RBT Switch Requirements

1. The RBT switch's HTTPS server must be enabled. (This option is enabled by default.) If HTTPS is disabled you can enable it using the following command:

```
set ip https server enable
```
2. The switch must have an IP interface that can be reached by the PC where the browser is installed.

Logging Into WebView

1. Type `https://ip-addr` in the Web browser's Address or Location field and press Enter. For ip-addr, type an IP address you configured on the switch.
2. If your browser displays a certificate warning, select the option to accept the certificate.

The certificate is presented to your browser by the RBT switch to authenticate the switch's identity. You can select to accept the certificate for the current web management session, or for all web management sessions.

After you accept the certificate, the browser might display another dialog asking whether you want to view the certificate. You can view the certificate, or continue without viewing it.

3. In the User Name field, type admin.
 4. In the Password field, type the enable password configured on the switch.
 5. Click OK.
- RBT-RBT security (also called RAS-RAS security) – RBT-RBT security encrypts management traffic exchanged by RBT switches in a Mobility Domain. When RBT-RBT security is enabled, management traffic among RBT switches in the Mobility Domain is encrypted using AES. The keying material is dynamically generated for each session and passed among switches using public keys that you configure.
 - AirDefense software support on MPs – RBT switch Version 5.0 enables you to convert DAPs into AirDefense sensors. The AirDefense system is an enterprise-class security solution that allows you to protect against threats and intrusions into your wireless network. The AirDefense solution can be integrated with the Enterasys Software Switch System, complementing Enterasys network security features by providing a centralized server dedicated to security analysis and record keeping.
 - AeroScout RFID tag support – RBT switch Version 5.0 enables DAPs to detect AeroScout RFID tags, and respond to commands from an AeroScout Engine. AeroScout RFID tags are wireless transmitters that you can place on assets such as office equipment to track the equipment's location. Each tag regularly transmits its unique ID. AeroScout listeners detect the transmissions from the RFID tags and relay this information to an AeroScout Engine or RBT switch. You can use an AeroScout Engine or RoamAbout Switch Manager to locate the asset. DAPs can be configured as AeroScout listeners. A DAP configured to be an AeroScout listener detects RFID tag IDs and sends the tag information to the RBT switch managing the DAP. If an AeroScout Engine is configured to request the information from the DAP, the DAP also sends the information to the AeroScout Engine.
 - Persistent VLAN assignment for roaming clients – RBT switch Version 5.0 provides a new service profile option, keep-initial-vlan, which allows you to keep users who roam on the same VLAN after roaming, even after they roam to another MX switch.

NOTE: The keep-initial-vlan option does not apply to Web-Portal clients. Instead, VLAN assignment for roaming Web-Portal clients automatically works the same way as when keep-initial-vlan is enabled. The VLAN initially assigned to a Web-Portal user is not changed except by a location policy, AAA, or SSID default setting on the roamed-to switch.

- Simplified Web-Portal and last-resort configuration – In previous RBT switch Versions, each of these authentication types required configuration of special users in the local database for wireless access: web-portal-ssid for Web Portal and last-resort-ssid. In RBT switch Version 5.0, these special users are not supported. In fact, they cannot even be configured in the local database. However, special users web-portal-wired and last-resort-wired are still required for Web-Portal or last-resort access on a wired authentication port.

The default authorization attributes set on the SSID are applied to last-resort users and also to Web-Portal users while they are being authenticated (that is, while they are in the portal). For example, if the vlan-name attribute on the service profile is set to guest-vlan, users are placed in guest-vlan.

The Web-Portal ACL (portalacl by default), which used to be associated with the web-portal-ssid or last-resort-ssid user, is now associated with the SSID's service profile instead. The ACL is still automatically generated by RBT switch the first time you set the fallthru authentication type on any service profile or wired authentication port to web-portal. If you use a different ACL, you can change the ACL name used by the service profile, with the set service-profile name web-portal-acl aclname command.

To further simplify last-resort configuration, last-resort AAA rules (configured by set authentication last-resort commands) are no longer required or supported. Instead, if the fallthru authentication type for an SSID or wired authentication port is set to last-resort, and no 802.1X or MAC access rules are configured for a service profile's SSID, users are automatically granted access.

- RF Auto-Tuning enhancements – RBT switch Version 5.0 contains new commands that provide the following RF Auto-Tuning options:
 1. Lockdown options for dynamically assigned channels and power levels. You can convert dynamically assigned channel or power settings into statically configured settings. Previous RBT switch versions allowed this capability only through RoamAbout Switch Manager.
 2. Configurable time interval for ramped power changes. When RF Auto-Tuning determines that power should be increased or decreased, the RBT switch gradually ramps the power up or down, in 1 dBm increments. By default, power is ramped up or down by 1 dBm every 60 seconds until the power setting is reached.
- Unscheduled Automatic Powersave Delivery (U-APSD) support – RBT Version 5.0 enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from DAP radios by using U-APSD.

When U-APSD support is enabled on the RBT switch, a client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority. U-APSD can be enabled for individual traffic priorities, for individual clients, based on the client's request. A client enables U-APSD for a traffic priority by indicating this preference when (re)associating with the DAP radio.

A client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority.

A client can but is not required to request U-APSD for all four traffic priorities. The DAP radio still buffers packets for all traffic priorities even if the client does not request U-APSD for them. However, to retrieve buffered packets for priorities that are not using U-APSD, a client must send a separate PSpoll for each buffered packet.

U-APSD is supported only for QoS mode WMM.

- Local software images on DAPs – RBT Version 5.0 supports local storage of DAP software images on the DAPs themselves. When a DAP boots, it can load its local image and does not need to download its image from an RBT switch unless the image on the RBT switch is newer.

- DHCP server enhancements – RBT Version 5.0 allows configuration of the following new options on the RBT switch DHCP server:
 - DNS domain name
 - Primary and secondary DNS servers
 - Default router (gateway)

In previous RBT Versions, the RBT switch DHCP server obtained values for these options from other parts of the switch's configuration. (This is still the default, if the options are not set on the server.)

- RADIUS accounting enhancements – RBT Version 5.0 includes support for the acct-interim-interval user attribute. You can use this attribute to configure the RBT switch to send accounting update records at periodic intervals. RBT Version 5.0 also supports system accounting. When system accounting is enabled, the RBT switch generates an Accounting-On message when the RBT switch starts and an Accounting-Off message when the RBT switch is administratively shut down. This new accounting functionality can be used in conjunction with billing systems that require periodic accounting messages.
- Support for special characters in SNMP community names – RBT Version 5.0 allows any printable ASCII characters except white space to be used in SNMP community names. Previous RBT versions allowed letters and numbers only.

NOTE: SNMP community names cannot begin with numerals.

- Increased life span of new self-signed certificates – Self-signed certificates created using RBT switch Version 5.0 have a longer life span than self-signed certificates generated using previous RBT versions. Self-signed certificates generated in RBT Version 5.0 are valid for three years. Self-signed certificates generated in previous RBT versions are valid for one year.
- Web Interface to RASM services – In previous version of the RASM application, dialog windows were used to make service changes.
- Web-Start Client – RoamAbout Switch Manager Version 5.0 provides a Java-based version of the RoamAbout Switch Manager client, the Web-Start client. The Web-Start client simplifies installation and upgrade of the client. Because the client and server versions must match, an upgrade to RoamAbout Switch Manager Services requires an upgrade of the client on each machine to the same version. The versions of the client and server also must match when the client is Java-based. However, you can easily install the Web-Start client simply by browsing to the server and clicking an option. You do not need to install from the product CD or an installation executable stored on a file server. The appearance and options in the Java version of the client are identical to those in the standard version.

System Requirements:

- 1 A Java plugin is required. You cannot launch the Web-Start client using a Java enabled web browser.
- 2 One of the following browsers:
 - Internet Explorer 5.5 or higher
 - Mozilla Firefox 1.5 or higher

Installing the Web-Start Client:

- 1 Use a browser to establish a secure (HTTPS) connection to the host running RASM Services.
- 2 Select the Home option.
- 3 Click Launch Client.

Overall Functionality:

- Static DAP IP addresses – Please refer to the *RoamAbout Switch RBT-8xx0_v50103* Release Notes for further explanation.

- Sygate On-Demand Agent (SODA) – The RBT switches now work with a Sygate server to download an agent profile to the user to check for all network required specifications before allowing the user to gain access to the network.
- Broadcast settings per Wireless profile – This feature allow users to set broadcast settings for Proxy ARPs, restricted DHCP access, and no broadcast packets. The RBT switch responds to ARPs on behalf of the client, denies all client traffic until the client has a DHCP address, and send unicast messages for client ARP and DHCP multicast messages.
- Configurable data rate settings for clients – This feature is also in the Wireless Profile, and allows the network administrator to tailor the data traffic to the services required for each channel. This also helps to fine tune the network performance for VoIP traffic.
- Session Based Call Admission Control – The network administrator can set the number of calls allowed per SSID.
- Static Class of Service – Statically assigns a CoS value to the SSID to help ensure Voice quality.
- User Session Timers per SSID – Allows network administrators to set a session time-out for inactive users.
- Network Planning and Site Survey – This tool allows the user to upload a CAD, Visio, jpeg, or bitmap drawing into the RoamAbout Switch Manager Site area and create a three-dimensional layout for AP placement. This tool will automatically calculate the distances and placement of each AP based upon the floor plan's RF factors.
- Management services – Including SNMP communities, trap servers, USM users, trace log settings, and time zone configuration.
- SSID – The RoamAbout Switch Manager will allow 8 SSIDs to be deployed to the wireless fabric per radio.
- Radio and Service profiling – User-configurable settings to control the AP radio activity and the SSID encryption settings.
- Load Sharing – Gives the user the option to spread the traffic patterns between the two RBT-8x00 ports.
- VLANs – this is where the interfaces will be created, as well as options for 802.1Q port tagging and port VLAN assignments.
- Spanning Tree – The RBT-8x00 supports 802.1D Spanning Tree and Per VLAN Spanning Tree (PVST) protocols.
- AAA/802.1X – This includes the RADIUS servers, the local authentication database, Administrator and Network access rules, and third party AP creation. The user can add and modify users and groups to match any RADIUS server in the fabric.
- ACLs – Various Access Control List modifications can be created and modified to allow or deny users, IP subnets, or VLANs to the fabric.
- IP services – User-configurable area for IP routes and gateways, DNS servers, Network Time Protocol services, and ARP cache entries.
- RF detection – The area to modify Ignored Users, permitted OUI users (for Rogue detection usage), permitted or denied SSIDs, the client black list (for known malicious users), and the attack list (the known rogues in the fabric).
- Rogue detection – Each AP has the ability to monitor its neighbors and report to the RoamAbout Switch Manager. If a detected neighbor is not in the configured AP list, it will be classified as a rogue until the network administrator accepts or denies the rogue label.
- Countermeasures – Each AP can use countermeasures against known rogue devices, or unknown APs and users to stop clients from infecting the network.

- Client and AP monitoring – The RoamAbout Switch Manager can keep track of each AP and any clients associated to that AP, and track the network usage for historical and countermeasure usage.
- Site policies – Based upon area in the floor plan and network layout, certain configurable policies can be enforced to ensure the APs within each area have a similar configuration.
- Reporting – All client activity, user watch lists, RF summaries, network usage and rogue details can be extracted and sent to a report for investigative and historical tracking.
- Image repository and deployment – Each RoamAbout Wireless Switch's firmware image can be loaded into the image repository for future distribution.
- Auto-DAP configuration – Now the user can pre-configure the settings for newly discovered access points that are not configured in the network. This functionality has been in the MSS system for the previous releases, but now the user can utilize RASM to control, accept, or delete new access points to the system.
- L2 traffic restriction – The MSS can now restrict traffic between users within the same VLAN.
- Default AAA attributes for each SSID – These are the set of attributes, including VLAN information, that will be applied to the SSID when the normal AAA or policy rules do not apply.
- On-demand countermeasures – Pre-configured countermeasures to specifically target those devices already configured on the system's black list, not other devices that have been classified as rogue by hitting a policy violation.
- Network Domains – Groups of geographically dispersed Mobility Domains that share information over a WAN link. This shared information allows a user configured in one Mobility Domain to establish connectivity on a RoamAbout switch in a remote Mobility Domain. The RoamAbout switch forwards the user traffic by creating a VLAN tunnel to a RoamAbout switch in the remote Mobility Domain.
- Configurable timeout for the RoamAbout Switch CLI sessions.
- Configurable CoS to QoS mappings – This helps to keep the overall network traffic consistency.

INSTALLATION AND CONFIGURATION NOTES:

Please refer to the *RoamAbout Switch Manager User's Guide* for complete installation instructions, located on your CD, or on the Enterasys Web site <http://www.enterasys.com/products/wireless/>.

NOTE: RASM version 5.0.x can be installed directly over previous RASM 4.2.x and 5.0.x versions without uninstalling those versions first.

NOTE: The RASM 4.2.5.1 version can be installed directly over the previous 4.0 and 4.1 versions. However, due to the database structure changes made between 4.0 and 4.1, as well as all the new feature enhancements, it is recommended to do an uninstall of the 4.0 RASM version, and a new install of the 4.2 executable. The major points to focus on for this procedure are as follows:

1. Start the uninstall by going to the Control Panel, and selecting Adding/Removing programs. Choose RASM.
2. When uninstall starts, the RASM Uninstall Options window is displayed. Four choices are already checked. Uncheck the first and third choices, deleting the network plans, and deleting the license information. The other two choices can remain checked. Click Continue.
3. When the uninstall is complete, click Done.
4. From this point, the installation of 4.1 or 4.2 RASM can begin from either the files retrieved from the Enterasys Firmware Download page, or the CD received with your order.

If you have the RASM CD, you can install the product directly from the CD.

CUSTOMER RELEASE NOTES

If you do not have the RASM CD, download the firmware from the Enterasys Firmware Download page and install on your PC.

UPGRADING THE ROAMABOUT SWITCH MANAGER FROM PREVIOUS VERSIONS:

To upgrade the RoamAbout Switch Manager on your PC, please refer to the “Upgrading RASM” section in the “Installing RoamAbout Switch Manager” chapter of the *RoamAbout Switch Manager Interface Reference* document, which can be downloaded from the following site:

<http://www.enterasys.com/support/manuals/n-s.html#R>.

DOWNGRADING THE ROAMABOUT SWITCH MANAGER FROM THE 5.0 VERSION:

If you need to downgrade from a RoamAbout Switch Manager 5.0.x version to a previous 5.0.x version, use the following procedure:

1. Back up the network plans, by copying the config-db directory to a location that is not in the RASM installation path.
2. Uninstall the current RASM installation. Select to delete all but the license and the network plans.
3. Install the earlier RASM software version.
4. After installation, copy the folders in the backed up config-db directory to the one that is created by the installation in step 3.
5. After installation, copy the folders in the backed up services-db directory to the one that is created by the installation in step 3.

When you start the downgrade version of the RoamAbout Switch Manager, it opens the Default network plan.

If you need to downgrade the RBT switches managed by the RoamAbout Switch Manager, you can do so before or after the RASM downgrade.

NOTE: Enterasys Networks recommends that you do not downgrade to previous RoamAbout Switch Manager Versions. Database files saved in RoamAbout Switch Manager Version 5.0 cannot be used in earlier RoamAbout Switch Manager Versions. In addition, RBT switch features that are new in the RBT switch Version 5.0 are not supported in previous versions of the RoamAbout Switch Manager.

FIRMWARE CHANGES AND ENHANCEMENTS:

Firmware Release 5.0.9.2:

Resolved an issue where alarms were generated for DAPs in a down state when the DAPs were up and running. After a refresh and acknowledge of these alarms, they would reappear after 30-40 seconds.

Resolved an issue where the RASM application would crash after moving between the different alarm severity screens.

Resolved an issue where the RBT switch name was not showing up in the Client Sessions Monitor window.

Resolved an issue where the RASM application would crash with a “java.lang.StackOverflowError” after running a Rogue Summary Report.

Resolved an issue with the Rogue client report, where a manually entered rogue client MAC address returned no information and an incorrect date and time stamp.

CUSTOMER RELEASE NOTES

Firmware Release 5.0.8.1:

- Resolved an issue where the RASM application would stop with an Out of Memory error, forcing the user to reset the RASM server.
- Resolved an issue where the RASM monitoring page would show a new DAP's status as unknown.
- Resolved an issue where the RASM alarm page would stay in a waiting state when refreshed.
- Resolved an issue where the RBT-4102-EU and the RBT-1002-EU were not supported in the country code Hong Kong.
- Resolved an issue where the country code Puerto Rico could not be deployed to the RBT switches.
- Resolved an issue where the Configuration/System/Ports web page in RASM did not display any port information.
- Resolved an issue where RASM would generate an internal application error when moving between the Alarms page and the Monitoring page.
- Resolved an issue where active countermeasure activities were not displayed in the Alarm page.
- Resolved an issue where new, unconfigured DAPs in the network were not displayed in the Alarm page.

Firmware Release 5.0.6.1:

- Resolved an issue when the system is set to country code Thailand, the radio status in RASM showed an incorrect radio A status of 'up' (the 5.4 GHz – A band – is not supported in Thailand).
- Resolved an issue converting the AP RBT-1002-EU from an auto-DAP to a configured DAP in country code South Africa (error proclaimed that channel 44 was not supported, but it was listed in the homologation table as a fully-supported channel).
- Resolved an issue where the Network Changes in RASM are accepted, but the Accept option stays highlighted.
- Replaced the 0.0.0.0 default IP settings in the IP fields to a blank default setting.
- Resolved an issue where RASM did not regain the RBT switch connection after changing the RBT system IP address.
- Resolved an issue with high CPU utilization every five minutes when rogue detection and RF monitoring were enabled.

Firmware Release 4.2.5.1:

- Resolved an issue where the Image Install from RASM would fail due to a back-up file inconsistency between the RASM application and the RBT switch.
- Resolved an issue where the RASM Server CPU would spike to 95% every five minutes due to the simultaneous RF Monitoring and Rogue Detection polling times.
- Resolved an issue where the user could not deploy more than one DAP in a Location Policy configuration.
- Resolved an issue where RASM would not correctly report the client activity in the Monitor window.
- Resolved an issue where the RASM Services would crash after clicking on screens in the Monitoring tab.
- Resolved an issue where RASM reported the RBT-8200 filename as the RBT-8100 filename in the Image Repository, and this name was applied to the RBT-8200 upon image upgrade.
- Resolved an issue where an applied Policy does not associate the AAA network methods to the correct Wireless or Radio Services.
- Resolved an issue where the AP3000, AP1002, and AP4102-EU were not reporting RF Trends in the Monitor section.

Firmware Release 4.1.11.0:

- After installing the RASM application, it will ask the user to restart the PC to complete the installation.
- Resolved an issue where the RASM Application would crash if a Wireless Profile was configured with a static WEP key with alpha-numeric values.
- Resolved an issue where the "Local Changes" would remain at "Available" even though there are no local or network changes in the system.
- Resolved an issue where RASM would not allow the addition of a local last-resort user with spaces.

CUSTOMER RELEASE NOTES

Firmware Release 4.1.11.0:

Resolved an issue where the Enterasys DAPs were not visible in the RF Trends or RF Monitoring windows.

Resolved an RF Planning Tool issue where levels in a newly imported CAD drawing would be renamed to a new level's name if there were no previous RF obstacles defined.

Resolved a Policy issue where the network plan would be corrupted and lost after applying the Policy to the RASs.

Resolved an issue where converted Auto-DAP's radios would not be enabled even though the default Auto-DAP radio setting was enabled.

Note: Refer to [TechTip on page 12](#) for important information about configuring antenna types for the RBT-1602 Access Point.

Firmware Release 4.1.5.0:

IMPORTANT: 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 complete the following instructions to upgrade your AP successfully:

1. Convert the AP back to the "stand-alone" state by resetting the AP and holding the reset button down for 30 seconds.
2. Configure the AP so it can communicate with a TFTP server, and download the RBT-4102-thin-bin.img to the device. This firmware is provided on the [Enterasys Wireless Firmware Download](#) page.
3. After the "thin-image" has been downloaded to the AP, please reset the AP. You are now ready to use the AP-4102-EU as a "thin" client.
4. If the AP1102-EU was associated to an area in the RF Planning Tool, the AP4102-EU will need to be re-associated to the same area.

The user will be asked to restart the computer system if the 4.1.5 firmware is installed over any 4.0 firmware, in order to fully reinitialize the Services.

Resolved an issue when a user creates and places an RF obstacle in the Planning Tool and the remaining unconfigured RF obstacles assume the newly created name.

Resolved an Internal Application error when a user would delete a mapped ACL.

Fixed the wording in two pop-up windows under the License Information window.

Resolved a license error with a new install.

Firmware Release 4.1.4.0:

Resolved various installation crashes between the 4.0 and 4.1 firmware track.

Resolved issues where configuration changes made to the RoamAbout Switches using the RASM software would cause the RASM software to crash.

Resolved a RoamAbout Switch and DAP monitoring problem after upgrading to 4.1.

Resolved an issue where the SSID name could not be changed without deleting and recreating the SSID. Now, in the Wireless Services area, the SSID name can be changed.

Resolved an issue where the Rogue detection would time out after a few minutes.

Resolved an issue when Auto-DAPs were accepted into the configuration, but were not included in the current configuration view.

Resolved an issue where the RASM software was reporting an incorrect value for the DAP MAC addresses.

Resolved many issues involving configuration changes made in RASM, but not being able to deploy due to the deploy option remaining grayed out. These include STP changes, Service Profile updates, authentication changes (Static WEP key), DAP fingerprint changes, and VLAN information.

Resolved an issue where the SNMP enable choice was not persistent between firmware upgrades.

Resolved an issue where the RBT-8400 port type was incorrectly displayed in the RASM port status window.

Resolved an issue where RASM would accept an incorrect fingerprint value.

CUSTOMER RELEASE NOTES

Firmware Release 4.1.4.0:

Resolved an Auto-DAP numbering issue.

Firmware Release 4.0.18.0 (The following issues were resolved with the MSS firmware):

MTU for tunneled 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 change system configurations.

Firmware Release 4.0.16.0:

Added support for the RBT-8400 Wireless Switch.

Added support for the RBT-1002 Distributed Access Point.

Fixed an issue where the DAP would not recover for greater than 5 minutes after changing the DAP number.

Resolved an issue that limited the Service Profile name to 16 characters.

Resolved an issue where newly uploaded switches would remain in an “unknown” state until the application was restarted.

Resolved an issue limiting the DAP numbering to 99.

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

KNOWN RESTRICTIONS AND LIMITATIONS:

Firmware Release 5.0.9.2:

When an RBT switch configured in a network plan, and associated to a Wiring Closet in the RF Planning tool, the only way to change the country code settings and push the configuration change to the RBT switches is to change the country code through the RF Planning Tool.

At the time of this release, there is an open issue where multiple clients changing RASM RF Plan at same time can cause an error.

There is an open issue where RASM will display a DAP with a MAC address of 00:00:00:00:00:00.

When running remote clients that access the server, all monitoring and configuration functions are possible from the client even if he doesn't have a license of any kind. Only the planning portion of RASM requires each remote client to have a license key. RASM employs a locking mechanism to prevent two remote clients from changing configuration in the same area of the plan.

The channel and power settings shown in the RF Planning Tool portion of RASM do not reflect the current DAP channels or power settings. To see the current DAP settings, please go to the Monitoring screen, Status Summary, and the Access Points tab.

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 an area coverage in the RF Planning Tool.

RASM application and other applications utilizing web services can run on the same PC/Server if the default port number (443) is changed in the RoamAbout Switch Manager.

RASM does not accept AutoCAD files larger than 1 MB.

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 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

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

IETF STANDARDS PROTOCOL SUPPORT:

Refer to the RoamAbout Wireless Switch (RBT-8xx0) software release notes for detailed features.

RADIUS STANDARD AND EXTENDED ATTRIBUTES SUPPORT:

Refer to the RoamAbout Wireless Switch (RBT-8xx0) software release notes for detailed features.

SNMP TRAP SUPPORT:

Refer to the RoamAbout Wireless Switch (RBT-8xx0) software release notes for detailed features.

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.