EDGEWATER
wireless

EAP303X-O User Manual

001-00016-A02

Table of Contents

1 Quick Start

1. Mount EAP3030/EAP3031 on wall mount or pole-mount location (See EAP3030/EAP3031 Outdoor Installation Guide for more detail).
2. Attach Tx and Rx antennas to N-connector on top and bottom side of unit respectively
3. Insert PoE (Power over Ethernet) enabled 10/100 Ethernet cable into RJ45 jack (Ethernet Port 0) on lower end of the EAP3030/EAP3031 (see Figure 1)
4. Allow unit 30 seconds for software boot-up.
5. Log into unit.

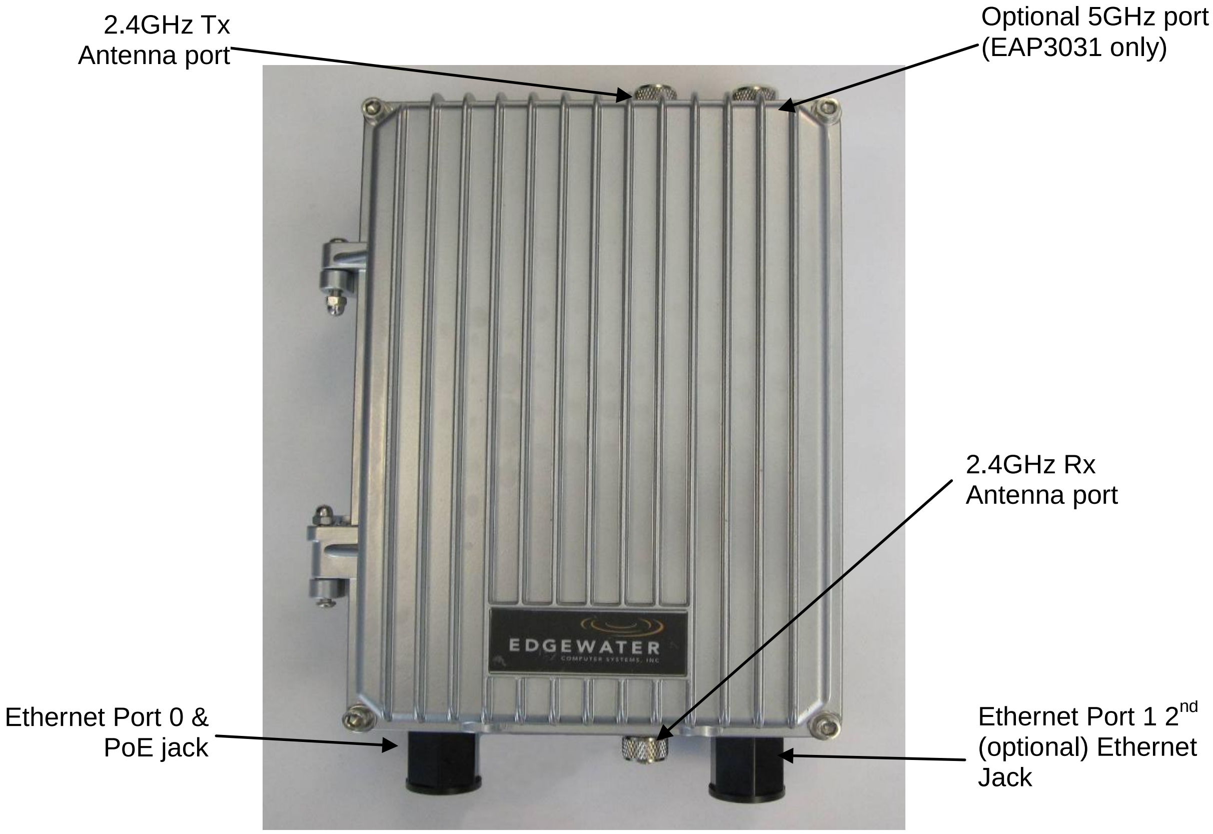


Figure 1 - Power and Ethernet Rear-panel Connections

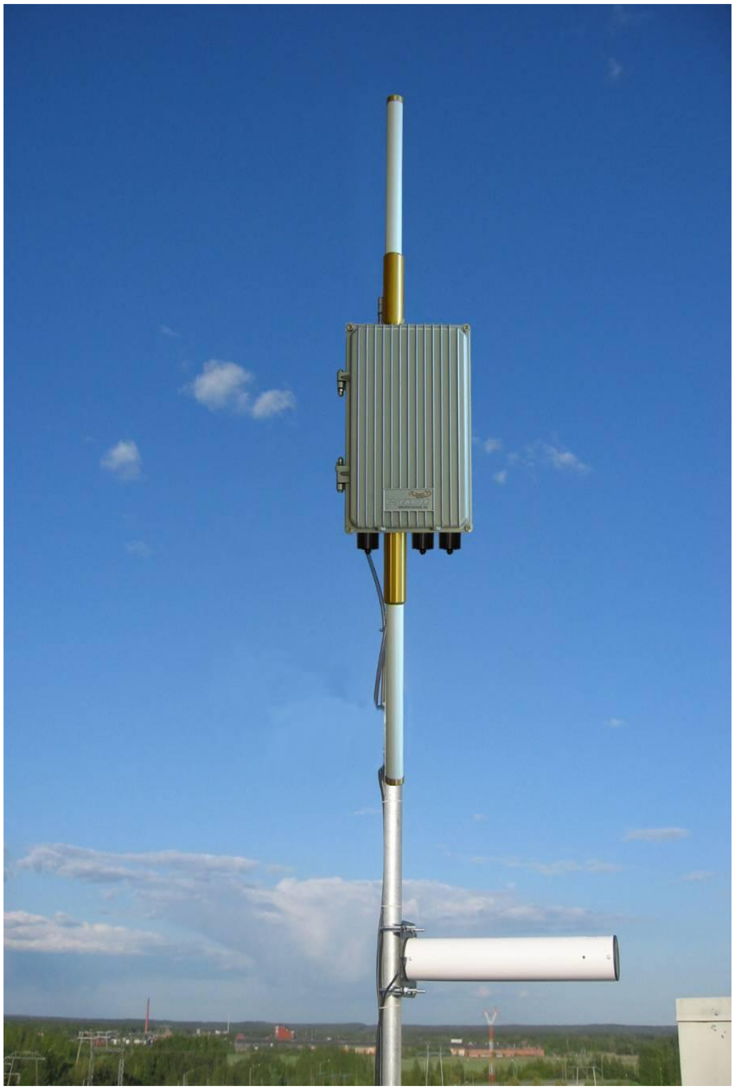
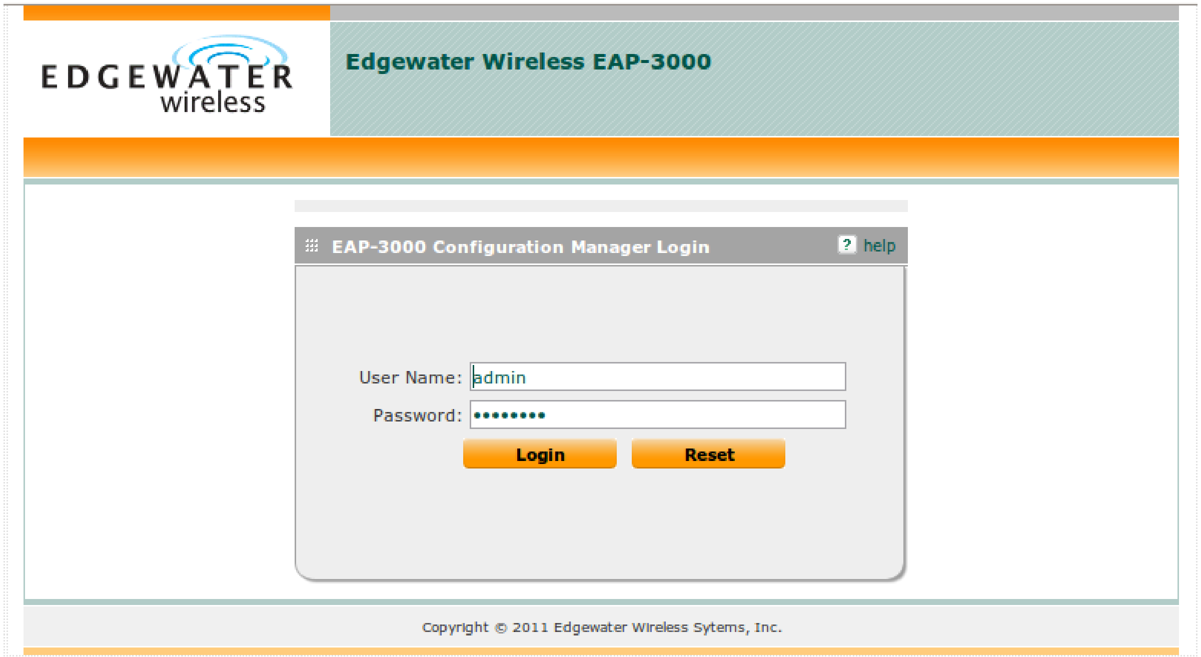


Figure 2 – Possible Omni Directional Antenna Configuration for Pole Mount

2 Login



Edgewater Wireless EAP-3000

EAP-3000 Configuration Manager Login

User Name: admin

Password: ••••••••

Copyright © 2011 Edgewater Wireless Sytems, Inc.

Welcome to the Edgewater EAP3000

The login page authenticates users and ensures that only authorized users can view or modify this device’s settings.

Login user name and password

The device accepts two types of logins, one with administrative privileges and one with guest privileges. With administrative privileges, you can view and also modify the configuration of the Access Point. Logging in with guest privileges will only allow you to view the existing configuration, but not to change it.

Enter the user name and password in the indicated areas to login to the Access Point to view or edit its configuration. The default user names and passwords are as follows:

User Name: admin

Password: password

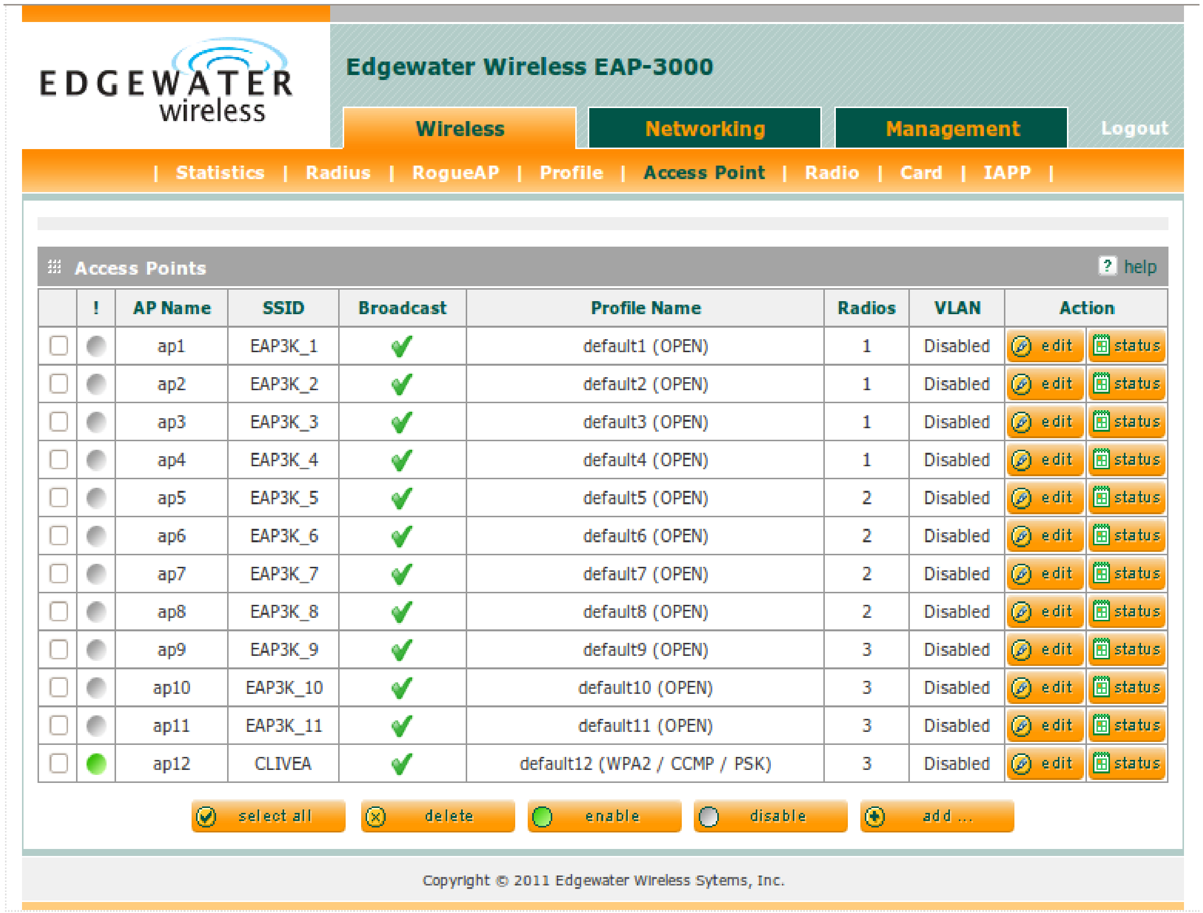
User Name: guest

Password: password

Session Timeout

Once logged in, the Access Point will maintain a session for the login. If there is no activity for a specified period, the session will expire and you will be asked to login again. The default idle session time is five minutes, but can be changed by logging in and updating the timeout value in the Management -> Users page.

3 Wireless



EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Access Points
? help

	!	AP Name	SSID	Broadcast	Profile Name	Radios	VLAN	Action	
□	○	ap1	EAP3K_1	✓	default1 (OPEN)	1	Disabled	edit	status
□	○	ap2	EAP3K_2	✓	default2 (OPEN)	1	Disabled	edit	status
□	○	ap3	EAP3K_3	✓	default3 (OPEN)	1	Disabled	edit	status
□	○	ap4	EAP3K_4	✓	default4 (OPEN)	1	Disabled	edit	status
□	○	ap5	EAP3K_5	✓	default5 (OPEN)	2	Disabled	edit	status
□	○	ap6	EAP3K_6	✓	default6 (OPEN)	2	Disabled	edit	status
□	○	ap7	EAP3K_7	✓	default7 (OPEN)	2	Disabled	edit	status
□	○	ap8	EAP3K_8	✓	default8 (OPEN)	2	Disabled	edit	status
□	○	ap9	EAP3K_9	✓	default9 (OPEN)	3	Disabled	edit	status
□	○	ap10	EAP3K_10	✓	default10 (OPEN)	3	Disabled	edit	status
□	○	ap11	EAP3K_11	✓	default11 (OPEN)	3	Disabled	edit	status
□	●	ap12	CLIVEA	✓	default12 (WPA2 / CCMP / PSK)	3	Disabled	edit	status

3.1 Wireless -> Access Point

The Access Point table displays the list of configured Virtual Access Points (VAPs) for this device. From this summary list, status and parameters of each VAP are available for display or configuration.

! (Status): A Virtual Access Point (VAP) can be disabled if not in use and enabled as needed. The VAP is disabled if the status light is Grey and it is enabled if the status light is green. Disabling a VAP does not delete it's configuration, but prevents association with the VAP. Enabling the VAP creates a wireless network where computers and other devices can join and communicate with the devices connected to the VAP or the devices on the local area network (LAN).

AP Name: This is the Virtual Access Point (VAP) identifier which uniquely identifies this VAP in the list of configured VAPs.

SSID: The name or Service Set Identifier (SSID) is the name of the wireless network serviced by this VAP; it is configured on the Profile page and later associated with the VAP by selecting it from the profile drop down box. Note that a given wireless profile can be common to multiple VAPs, therefore the SSID is not unique to any particular VAP. In order for computers or devices to communicate via this wireless network serviced by this VAP, all devices must select the same SSID from the list of wireless networks in the area.

Broadcast: The icon here indicates whether the SSID is broadcast or not in the beacon frames transmitted by the VAP. If the SSID is not broadcast then wireless devices will not be able to see the network name (SSID). The green tick mark indicates that the VAP's SSID is broadcast to the public; the red 'cancel' icon indicates that the SSID is not broadcast and a device would have to specify the SSID exactly to connect to this VAP.

Profile: This field has a brief description of the security, encryption and authentication combination assigned to the VAP. A Profile is not necessarily unique to a VAP; rather this grouping of wireless settings can be used on more than one VAP at the same time.

Radio: The physical radio(s) on which this VAP is running on.

VLAN: The VAP can be part of a logical network defined by the VLAN ID; this allows devices connected to the VLAN through this VAP to exchange data with one another as in a LAN.

Action/Edit: The edit button links to the AP Configuration page, allowing you to change the Role, Profile, Radio, Mode, etc. that is used by this VAP.

Action/Status: The status button links to a statistics page for this VAP, displaying traffic statistics for the VAP and the list of the connected clients.

The actions that can be taken on VAPs are:

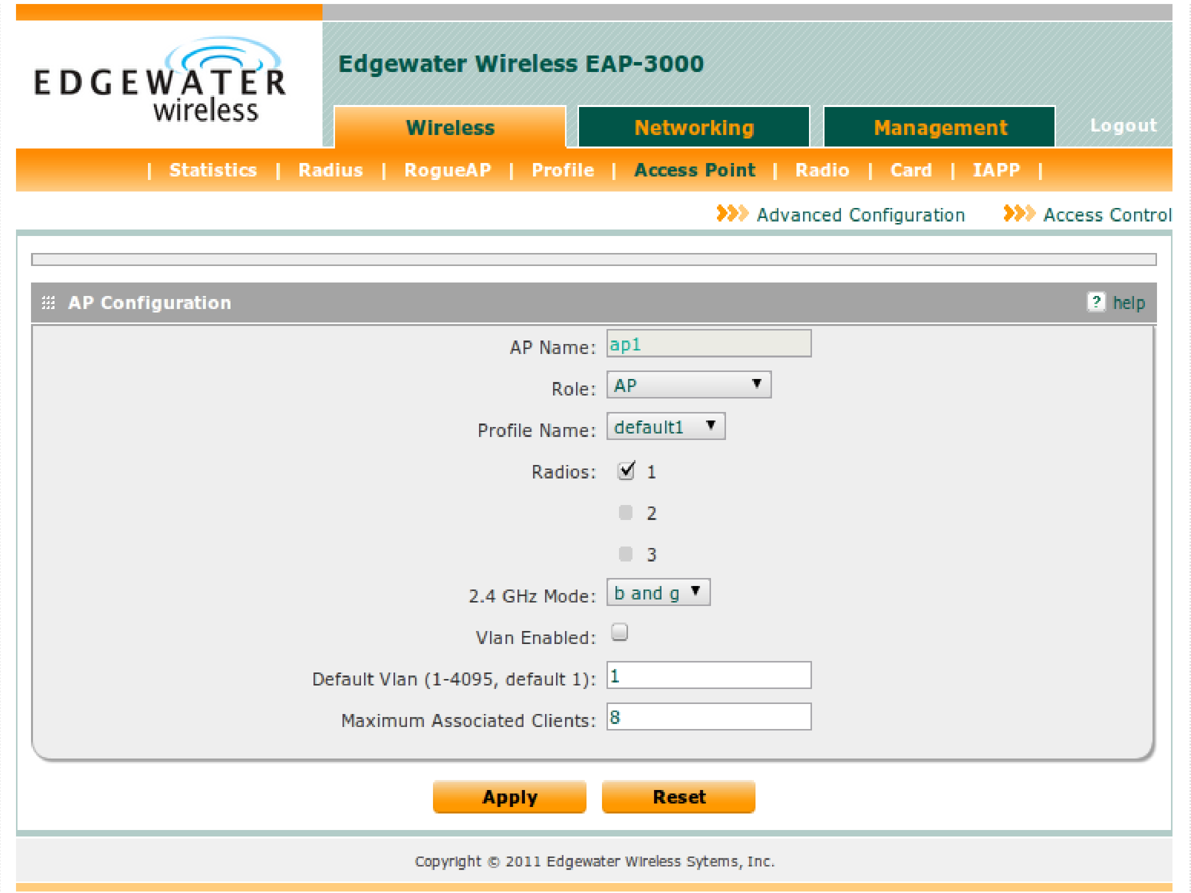
Select All: Select all the VAPs in the table

Enable: Enable the selected VAPs

Disable: Prevents wireless association with the selected VAPs

Delete: Deletes the selected VAP or VAPs

Add: Add a new VAP



AP Name:	ap1
Role:	AP ▼
Profile Name:	default1 ▼
Radios:	☑ 1
	□ 2
	□ 3
2.4 GHz Mode:	b and g ▼
Vlan Enabled:	□
Default Vlan (1-4095, default 1):	1
Maximum Associated Clients:	8

3.2 Wireless -> Access Point -> edit

Clicking “Edit” under the Action column for a particular VAP on the Access Points page will take you to the AP Configuration Page. This page allows you to add a new VAP or edit the configuration of the selected VAP. The details will then be displayed in the AP table on the main Access Points page under the Wireless menu.

AP Name: This is the unique name of the VAP selected to be configured.

Role: The VAP can act as a traditional Access Point device, WDS repeater, or WDS Root. When the VAP is configured as a WDS repeater, it acts like a wireless client and can connect to a VAP configured in WDS Root mode on another EAP3000 device. A successful connection to WDS Root VAP creates a WDS link and the traffic from the clients connected to other VAPs on this EAP3000 device is forwarded over the WDS link (only the broadcast traffic and the traffic destined to other devices which is not connected to VAPs on this EAP3000 device is forwarded). Note that when a VAP is configured in WDS repeater mode or WDS Root mode, clients will not be able to connect to the VAP.

Profile Name: Choose the encryption and authentication methods to be used by clients connecting to this AP from the drop down list of profiles. This list is populated by adding profiles in the Profile menu.

Radio: Select the physical radio on which this VAP will run.

Mode: This selects the 802.11 modulation technique. This device supports 802.11a, 802.11b and and 802.11g modes. Select g only if all devices in the wireless network can support 802.11g. Select b only mode if other devices and computers in the network can only support 802.11b. Select g and b if there will be some devices in this wireless network that will use 802.11g and some that will use 802.11b. If the device is an EAP3031 then 802.11a mode may be selected.

VLAN Enabled: Select this check box to tag the traffic received from connected clients with this VAP with a VLAN ID.

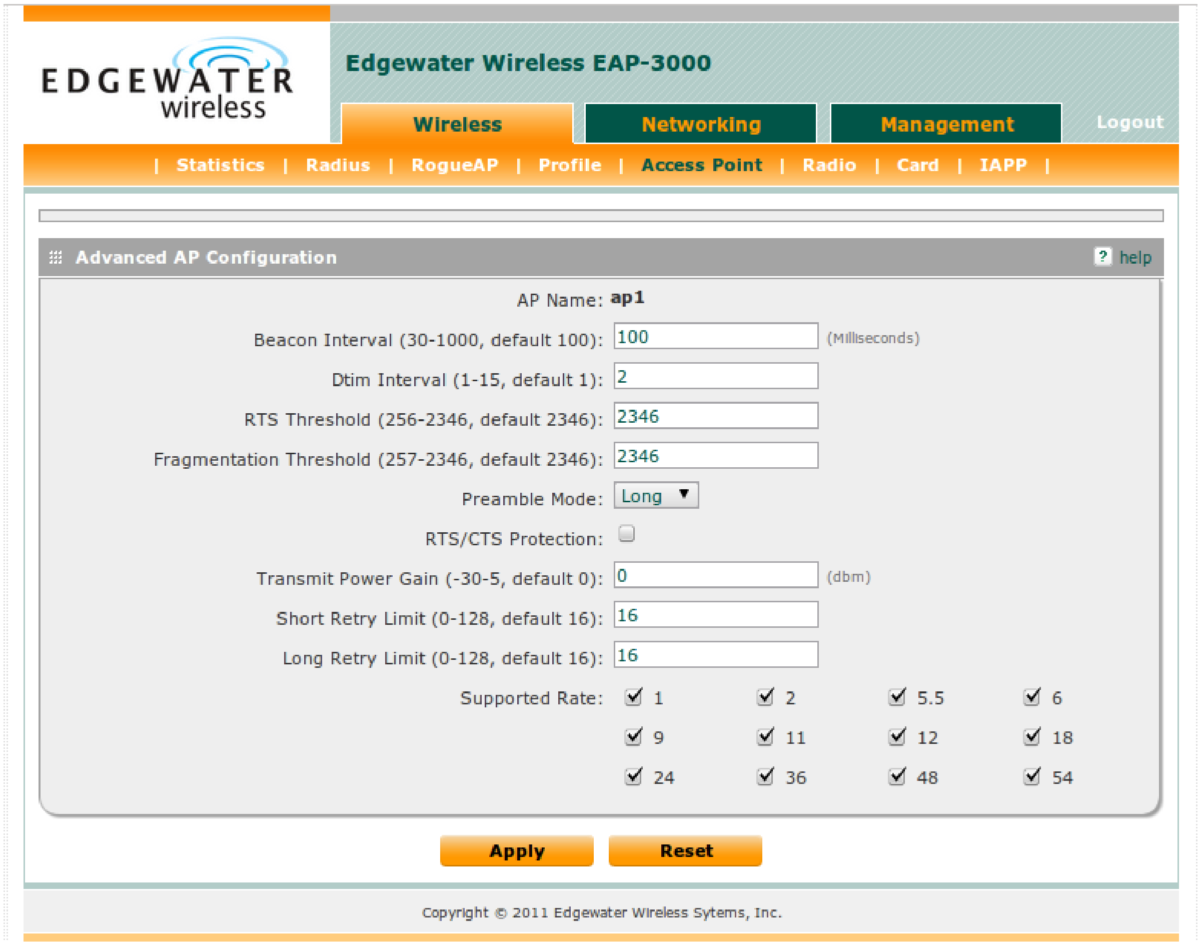
Default VLAN: VLAN ID which will be used to tag the traffic from connected clients.

Maximum Associated Clients: The maximum number of clients that can connect to this VAP.

The EAP3000 currently supports 8 clients per VAP for a total of 96 clients simultaneously.

Click Apply to save your changes.

Click Reset to revert to the previous settings.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
? help
Apply
Reset

Advanced AP Configuration

AP Name: **ap1**

Beacon Interval (30-1000, default 100): 100 (Milliseconds)

Dtim Interval (1-15, default 1): 2

RTS Threshold (256-2346, default 2346): 2346

Fragmentation Threshold (257-2346, default 2346): 2346

Preamble Mode: Long ▼

RTS/CTS Protection: □

Transmit Power Gain (-30-5, default 0): 0 (dbm)

Short Retry Limit (0-128, default 16): 16

Long Retry Limit (0-128, default 16): 16

Supported Rate:	☑ 1	☑ 2	☑ 5.5	☑ 6
	☑ 9	☑ 11	☑ 12	☑ 18
	☑ 24	☑ 36	☑ 48	☑ 54

3.3 Wireless -> Access Point -> edit -> Advanced Configuration

This page is used to specify advanced Access Point configuration details.

AP Name: This is the name of the VAP that was selected to be configured.

Beacon Interval: Enter the amount of time in milliseconds between beacon transmissions.

Dtim Interval: This interval sets when the delivery traffic indication message is sent; related to beacon interval.

RTS Threshold: The Request to Send (RTS) threshold is the value hat the VAP checks against its transmitting frames to determine if the RTS/CTS handshake is required with the receiving client. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of the network packet. The default is 2346, which effectively disables RTS.

Fragmentation Threshold: This is the maximum length of the frame beyond which a packet must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because sending them occupies the channel for a longer time.   The default is 2346, which effectively disables Fragmentation.

Preamble mode: 802.11b requires that a preamble be pre-pended to every frame before it is transmitted to the air. That preamble may be either the traditional "long" preamble, which requires 192 µs for transmission, or it may be an optional "short" preamble that requires only 96 µs.   The long preamble is needed for compatibility with legacy 802.11 systems operating at 1 and 2 Mbps. The default is "long".

RTS/CTS protection: Select to always do RTS/CTS handshake before transmitting a packet; it is generally used to minimize collisions among hidden stations

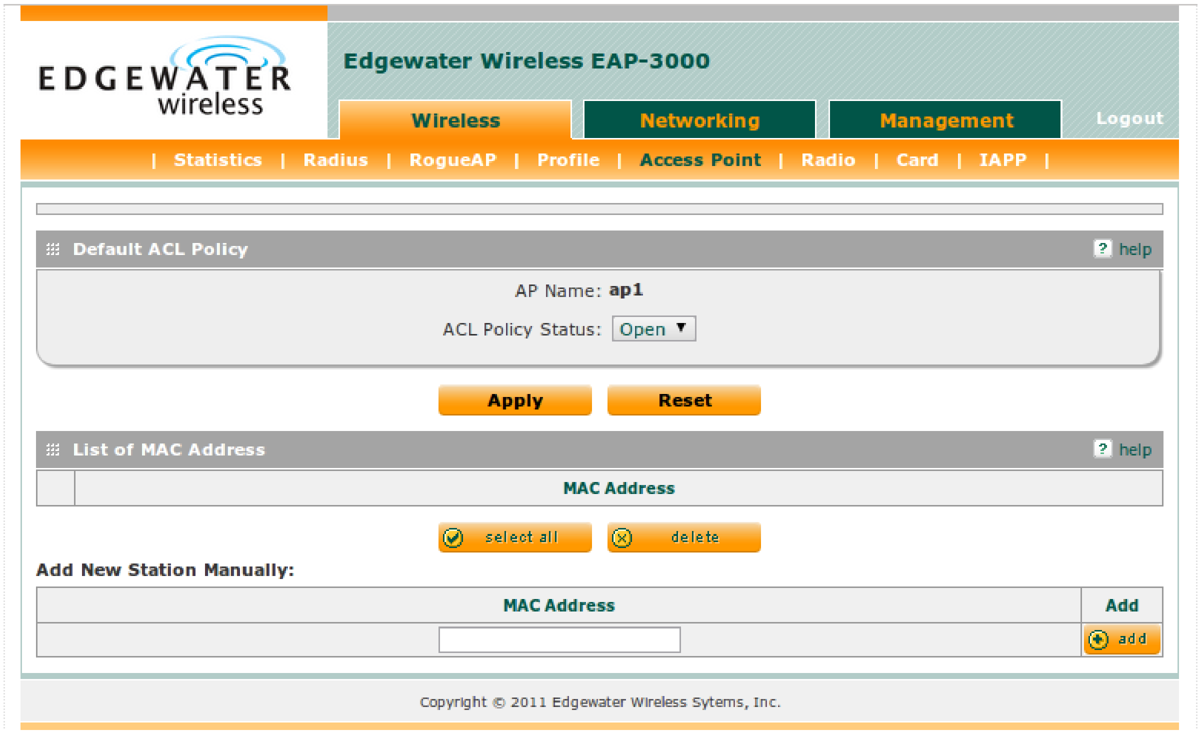
Transmit Power Gain: Define the relative amplification (gain) in dBm for transmitted packets which is added to the TX power configured on the physical radio.

Retry Limit: This limits the number of retries the VAP will use when a frame transmission fails. It is used for both long and short frames, of size less than or equal to the RTS threshold.

Supported Rate: Select the rate or rates (in Mbps) which the VAP will advertise in the beacon frames; at least 1 check box must be selected.

Click Apply to save your changes.

Click Reset to revert to the previous settings.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
help
Apply
Reset
help
select all
delete
add
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Default ACL Policy

AP Name: ap1

ACL Policy Status: Open

List of MAC Address

	MAC Address

Add New Station Manually:

MAC Address	Add
	add

3.4 Wireless -> Access Point -> edit -> Access Control

This page allows you to define specific MAC addresses to permit or deny connections to the selected VAP. The default is “open” access, which does no filtering on specific MAC addresses.

Default ACL Policy

AP Name: This is the name of the AP that is being configured.

ACL Policy Status: Select between Allow, Deny, or Open. An ACL Policy Status of “Allow” will permit only clients with MAC addresses in the List of MAC Address to connect to the VAP. An ACL Policy Status of “Deny” will prevent clients with a MAC address in the List of MAC Address to connect to the VAP. An ACL Policy Status of “Open” allows all clients to connect to the VAP.

Click Apply to save your changes.

Click Reset to revert to the previous settings.

List of MAC Addresses

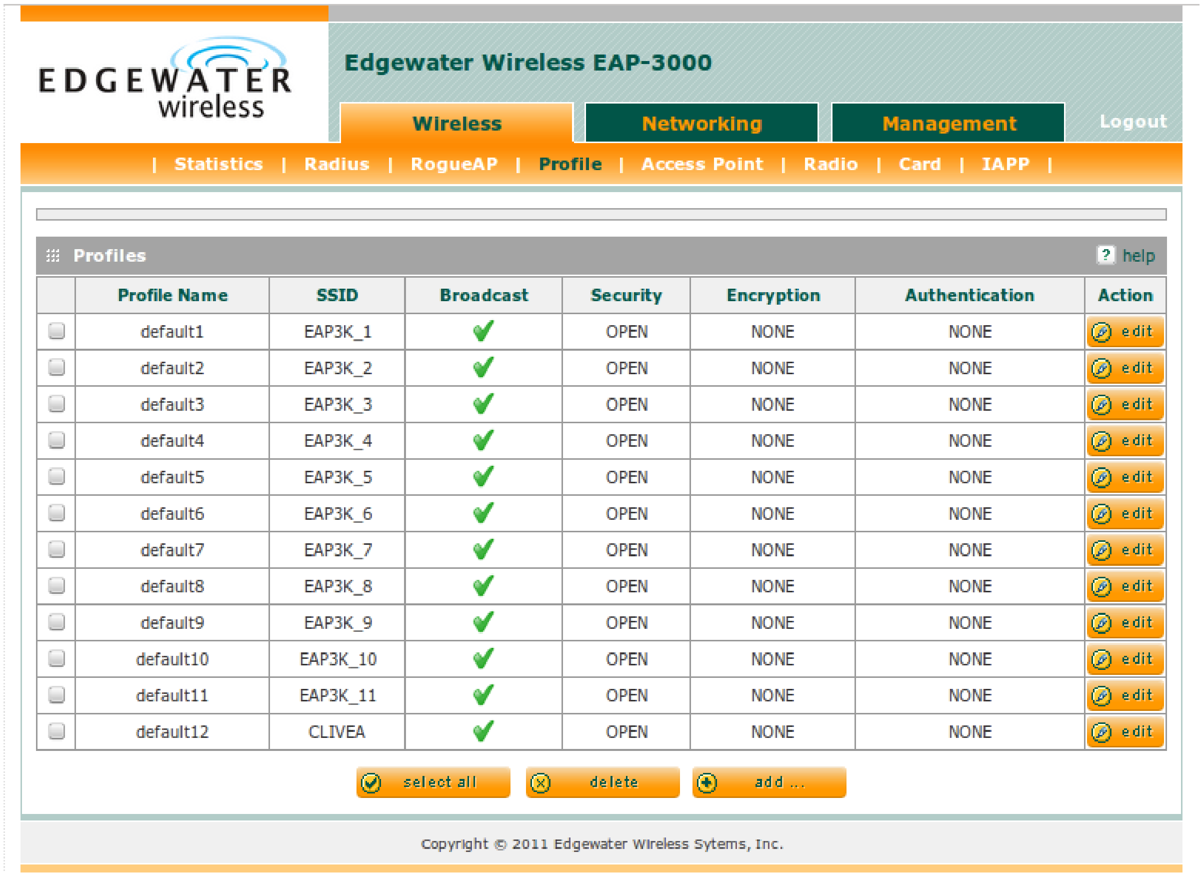
This list shows all the MAC addresses of computers and devices which are authorized/unauthorized (based on the default ACL Policy) to connect to this VAP.

Select All: Select all the MAC addresses in the list

Delete: Delete the selected MAC address or addresses from the list

Add New Station Manually: Enter the MAC address of the client that you would like to add to the list of MAC addresses above.

3.5 Wireless -> Profile


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Profiles
? help
select all
delete
add ...
Copyright © 2011 Edgewater Wireless Sytems, Inc.

	Profile Name	SSID	Broadcast	Security	Encryption	Authentication	Action
□	default1	EAP3K_1	✓	OPEN	NONE	NONE	edit
□	default2	EAP3K_2	✓	OPEN	NONE	NONE	edit
□	default3	EAP3K_3	✓	OPEN	NONE	NONE	edit
□	default4	EAP3K_4	✓	OPEN	NONE	NONE	edit
□	default5	EAP3K_5	✓	OPEN	NONE	NONE	edit
□	default6	EAP3K_6	✓	OPEN	NONE	NONE	edit
□	default7	EAP3K_7	✓	OPEN	NONE	NONE	edit
□	default8	EAP3K_8	✓	OPEN	NONE	NONE	edit
□	default9	EAP3K_9	✓	OPEN	NONE	NONE	edit
□	default10	EAP3K_10	✓	OPEN	NONE	NONE	edit
□	default11	EAP3K_11	✓	OPEN	NONE	NONE	edit
□	default12	CLIVEA	✓	OPEN	NONE	NONE	edit

A Profile is a definition of generic wireless settings which can be shared across multiple VAPs. VAP-specific settings are configured from the Access Point page. The profile allows for easy duplication of SSIDs, security settings, encryption methods, client authentication, etc. across VAPs.

Profile Name: This is the unique (alphanumeric) identifier of this wireless profile.

SSID: This is the Service Set Identifier that clients use to connect to the VAP that has this profile; it is referenced in the AP tables and statistics.

Broadcast: The icon here indicates whether this Profile will configure the assigned VAP to broadcast its SSID or not. The green tick mark indicates that the SSID will be broad-casted; the red ‘cancel’ icon indicates the SSID will not be broad-casted and a device would have to specify the SSID exactly to connect to the VAP.

Security: This field displays the type of wireless security (if any) assigned to this Profile: The security types are: None, WEP, WPA, WPA2, WPA+WPA2

Encryption: This field displays the encryption type that is assigned to this Profile: The encryption types are: WEP, TKIP, CCMP, TKIP + CCMP.

Authentication: This field displays the client authentication that is assigned to this Profile. The authentication types are: None, PSK, RADIUS, PSK + RADIUS.

Action/Edit: The edit button links to the Profile Configuration page, allowing you to change the properties shown in the table for this Profile.

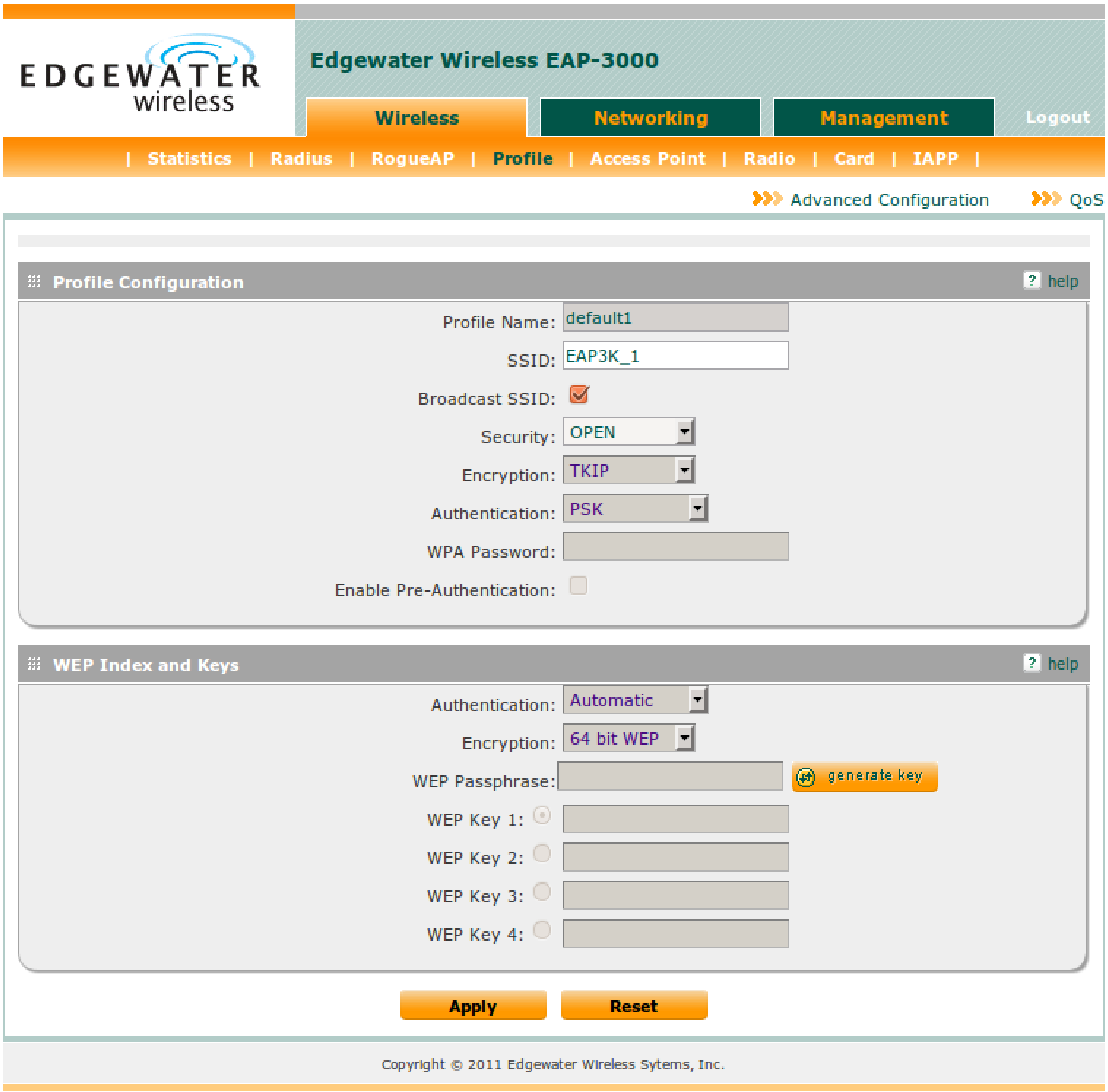
The actions that can be taken on Profiles are:

Select All: Select all the Profiles in the table

Delete: Delete the selected Profile or profiles

Add: create a new Profile and add it to the list

3.6 Wireless -> Profile -> edit


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Advanced Configuration
QoS
help
generate key
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Profile Configuration

Profile Name: default1

SSID: EAP3K_1

Broadcast SSID: ☑

Security: OPEN

Encryption: TKIP

Authentication: PSK

WPA Password:

Enable Pre-Authentication: □

WEP Index and Keys

Authentication: Automatic

Encryption: 64 bit WEP

WEP Passphrase:

WEP Key 1: ●

WEP Key 2: ○

WEP Key 3: ○

WEP Key 4: ○

The Profile Configuration page allows you to define the SSIDs and wireless settings of a particular Profile.

Profile Name: The selected Profile name is displayed here.

SSID: Define the Service Set Identifier (SSID) that clients use to connect to the VAP(s) that has this Profile; it is referenced in the AP tables and statistics.

Broadcast SSID: Enable this check box to broadcast the SSID. Disable this check box to prevent auto-detection of the SSID and force clients wishing to connect to this AP to specify the SSID without seeing it as a detected network.

Security: Select the type of security to be configured in this Profile from the drop down selector:

None: No security. Any wireless device can connect (subject to VAP ACL policy).

WEP (Wired Equivalent Privacy): Select this to use WEP encryption on the data packets. WEP is not considered to be secure and can be easily broken. Select this only if there are clients which can only support WEP security.

WPA (Wi-Fi Protected Access): WPA is part of the wireless security standard (802.11i) standardized by the Wi-Fi Alliance and was intended as an intermediate measure to take the place of WEP while 802.11i was being prepared. It supports Temporal Key Integrity Protocol (TKIP)/Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption (default is TKIP) and Pre-Shared Key (PSK)/Remote Authentication Dial In User Service (RADIUS) based authentication.

WPA2: WPA2 is the implementation of security standard specified in final 802.11i. . It supports TKIP/CCMP encryption (default is CCMP) and PSK/RADIUS based authentication.

WPA + WPA2: This mode allows both WPA and WPA2 clients to connect simultaneously.

Encryption: Select the encryption method to use: TKIP, CCMP, or both.

Authentication: Type of authentication to use: RADIUS, PSK, or PSK + RADIUS.

WPA Password: Pre-Shared key for WPA/WPA2 PSK authentication. The clients also need to be configured with the same password.

WEP Index and Keys

Selecting WEP in the Security box requires selecting the type of authentication and specifying the static WEP key to be used in the computers or devices that wish to access this secured wireless network.

Authentication: Select between Open System or Shared Key schemes

Encryption: Select the encryption type: 64 WEP, 128 WEP, or 152 WEP. The larger size keys provide stronger encryption, thus making the key more difficult to crack (i.e. 64 WEP has a 40 bit key which is less secure than the 128 WEP which has a 104 bit key).

WEP Pass phrase: Choose any alphanumeric phrase (longer than 8 characters for optimal security) and click generate key to generate 4 unique WEP keys. Select one of the four to use as the static key that devices must have in order to use the wireless network.

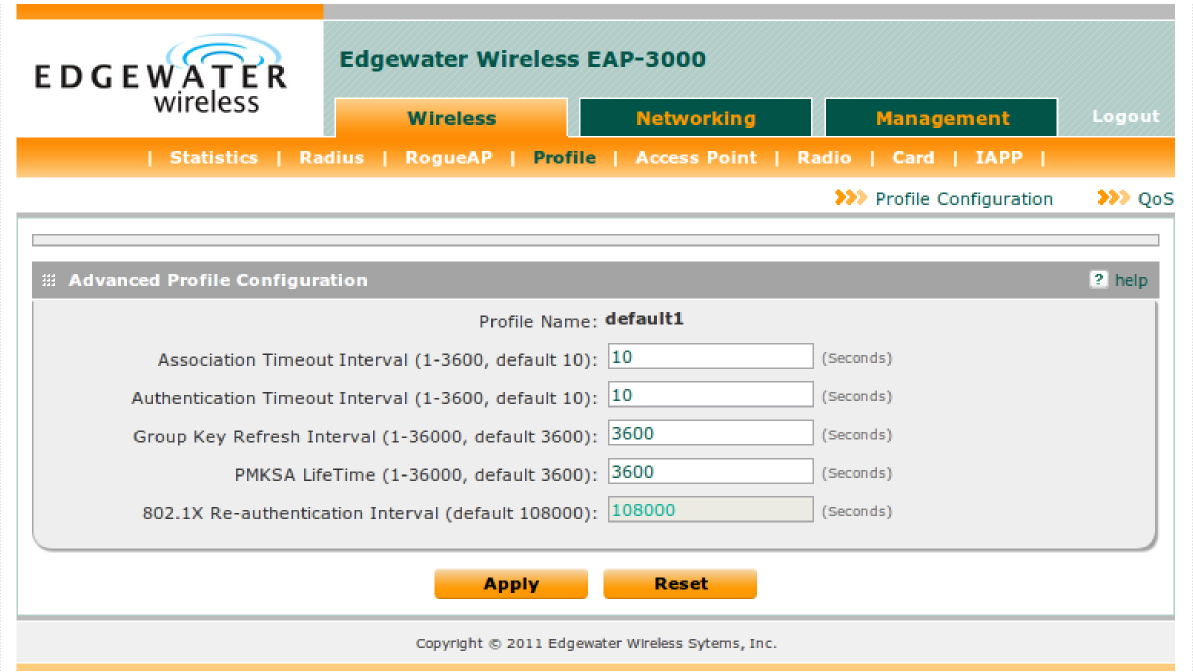
WEP Key 1-4: If WEP Pass phrase is not specified, a key can be entered directly in one of the WEP Key boxes. The length of key should be 5 ASCII characters (or 10 hex characters) for 64-bit WEP, 13 ASCII characters (or 26 hex characters) for 128-bit WEP, and 16 ASCII characters (or 32 hex characters) for 152-bit WEP

WEP Key Index: Based on which WEP key box is used, WEP key index is derived. Different clients can have different numbering scheme for index. For clients which have indexing starting with 0, WEP Key 1 to WEP Key 4 corresponds to index 0 to 3. Clients which have indexing starting with 1, WEP Key 1 to WEP Key 4 correspond to index 1 to 4.

Note: If the selected security type is OPEN then you will not be allowed to configure encryption and authentication.

Click Apply to save your changes.

Click Reset to revert to the previous settings.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Profile Configuration
QoS
Advanced Profile Configuration
? help
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Profile Name: **default1**

Association Timeout Interval (1-3600, default 10): 10 (Seconds)

Authentication Timeout Interval (1-3600, default 10): 10 (Seconds)

Group Key Refresh Interval (1-36000, default 3600): 3600 (Seconds)

PMKSA LifeTime (1-36000, default 3600): 3600 (Seconds)

802.1X Re-authentication Interval (default 108000): 108000 (Seconds)

3.7 Wireless -> Profile ->edit->Advanced Profile Configuration

This page allows you to change configuration parameters from their default settings.

Association Timeout Interval (Seconds): This specifies the timeout interval between authenticated and associated state of client. If client is not associated in this interval after the authentication, it is disconnected.

Authentication Timeout Interval (Seconds): This is the timeout interval for RADIUS (802.1X) authentication. If RADIUS authentication is not completed within this time after client is associated, it is disconnected.

Group Key Refresh Interval (Seconds): This specifies the timeout interval after which group keys are generated (only used if profile is configured with WPA or WPA2 security).

PMKSA Life Time (Seconds): WPA2 security standard has an option called Pairwise Master Key Security Association (PMKSA) caching which means that the master keys derived from successful RADIUS authentication are cached for some time to avoid long RADIUS authentication every time a client connects. This timeout interval specifies for how long this PMKSA is stored in the VAP. A client reconnecting within this interval (after successful RADIUS authentication) can skip the RADIUS authentication.

802.1X Re-authentication Interval: The timeout interval after which the VAP should re-authenticate with RADIUS server.

Click Apply to save your changes.

Click Reset to revert to the previous settings.

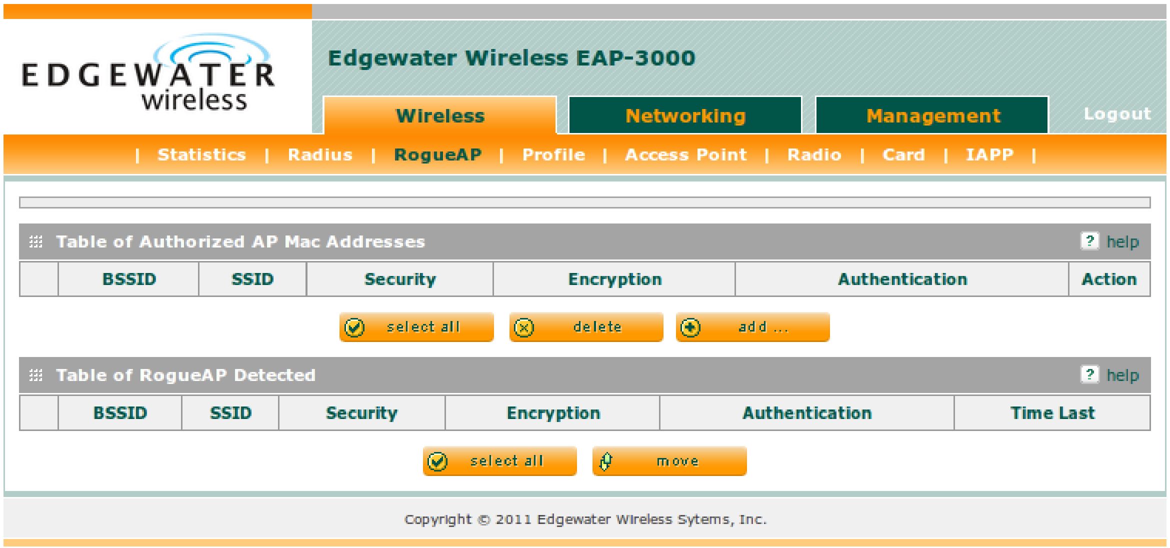

EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
help
select all
delete
add ...
help
select all
move

Table of Authorized AP Mac Addresses

	BSSID	SSID	Security	Encryption	Authentication	Action

Table of RogueAP Detected

	BSSID	SSID	Security	Encryption	Authentication	Time Last

Copyright © 2011 Edgewater Wireless Sytems, Inc.

3.8 Wireless -> RogueAP

This page summarizes the authorized and rogue APs configured for the system. A rogue AP is an AP that is not authorized to be running in the wireless area covered by this AP(s).

An Administrator can specify the list of authorized Access Points in the area in the "Table of Authorized AP MAC Addresses". Any AP which is not in this table is recorded in "Table of RogueAP Detected.

BSSID: The Basic Service Set Identifier (BSSID) of the AP

SSID: The Service Set Identifier (SSID) serviced by the AP

Security: Security used by the AP: None, WEP, WPA, WPA2, WPA+WPA2

Encryption: Encryption used by the AP: WEP, TKIP, CCMP, TKIP + CCMP.

Authentication: Type of WPA/WPA2 authentication used by AP: PSK, RADIUS, PSK+RADIUS

Time Last: This is the time in (seconds) when a rogue AP was detected.

Action/Edit: The edit button links to the Authorized AP Configuration page, allowing you to change the properties shown in the table for this AP.

The actions that can be taken on the Table of Authorized APs are:

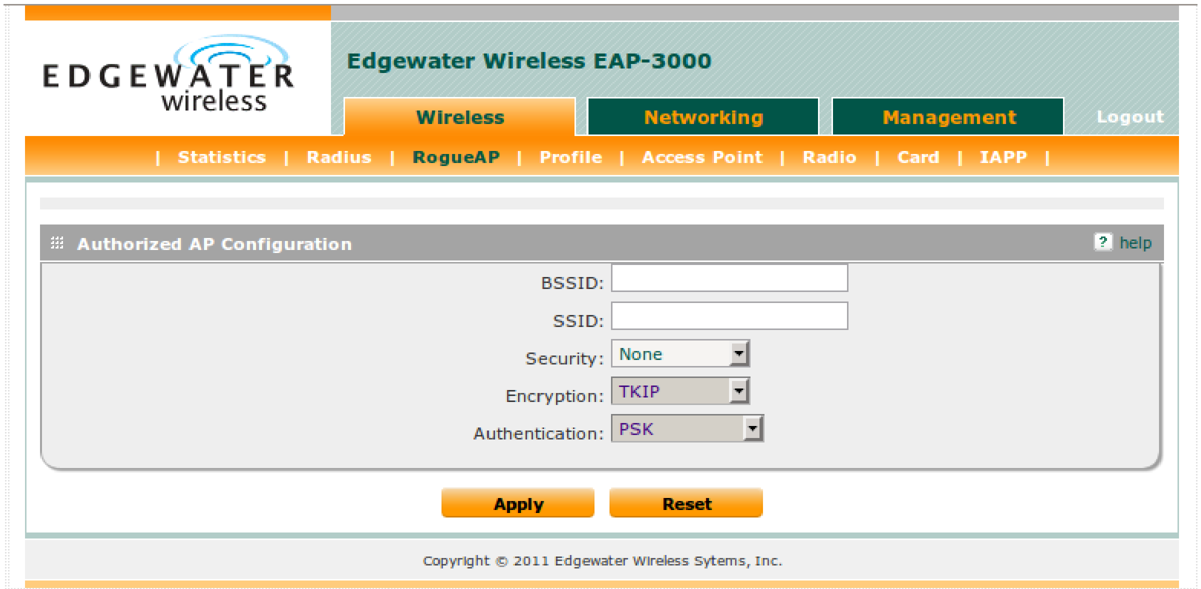
Select All: Select all the APs in the table

Delete: Delete the selected AP or APs

Add: Add a new authorized AP to the list

Move: Move an AP from “Table of Rogue AP Detected” to “Table of Authorized AP MAC Addresses”

3.9 Wireless -> RogueAP -> Authorized AP Configuration


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
? help
Apply
Reset

Authorized AP Configuration

BSSID:

SSID:

Security: None

Encryption: TKIP

Authentication: PSK

Copyright © 2011 Edgewater Wireless Sytems, Inc.

Use this page to add an AP to the Table of Authorized AP MAC Addresses.

BSSID: The BSSID of the AP

SSID: The Service Set Identifier serviced by AP

Security: Security used by AP: None, WEP, WPA, WPA2, WPA+WPA2

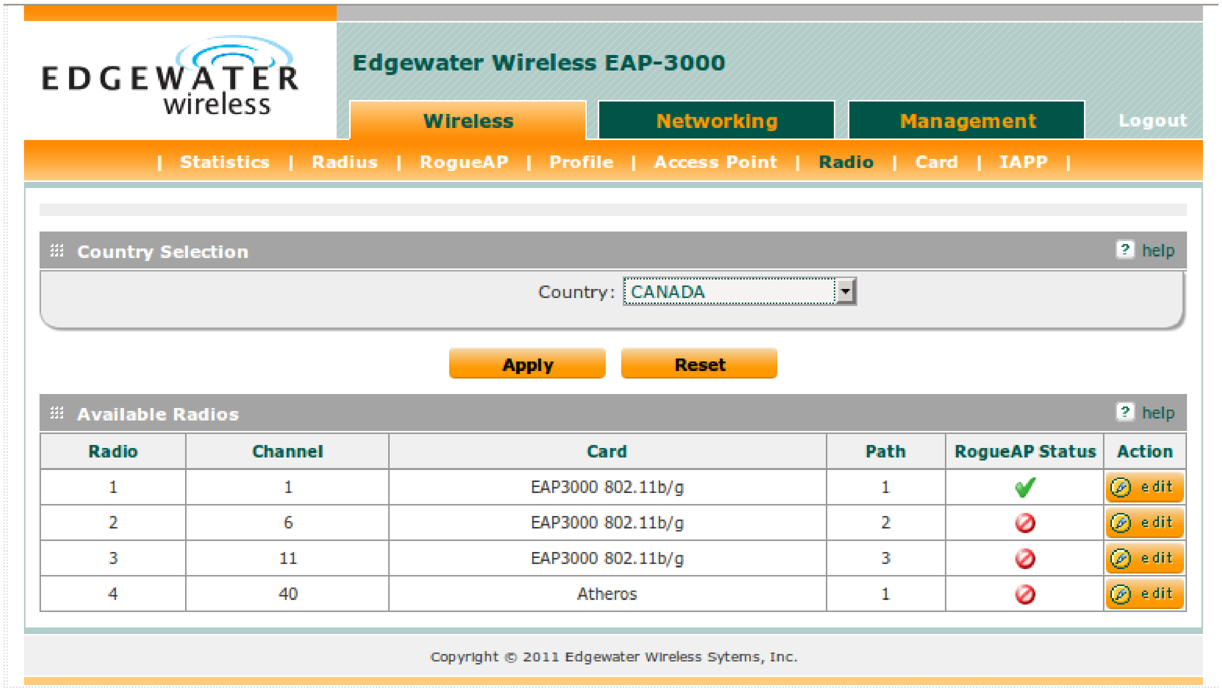
Encryption: Encryption used by AP: WEP, TKIP, CCMP, TKIP + CCMP.

Authentication: Type of WPA/WPA2 authentication used by AP: PSK, RADIUS, PSK+RADIUS

Click Apply to save your changes.

Click Reset to revert to the previous settings.

3.10 Wireless -> Radio


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Country Selection
? help
Apply
Reset
Available Radios
? help

Country: CANADA

Radio	Channel	Card	Path	RogueAP Status	Action
1	1	EAP3000 802.11b/g	1	✓	edit
2	6	EAP3000 802.11b/g	2	⊘	edit
3	11	EAP3000 802.11b/g	3	⊘	edit
4	40	Atheros	1	⊘	edit

Copyright © 2011 Edgewater Wireless Sytems, Inc.

This device supports multiple radios over 1 or 2 WLAN cards. The table here shows the list of available radios that a VAP may use.

Country: Select the country that the AP is operating in from the drop-down selector.

Note: Ensure that the correct country code is selected in order to comply with your country's regulatory requirements. See Appendix A for regional regulatory compliance.

Radio: Depending on the WLAN card(s) used in this device, there are a maximum of 3 radios supported per card (EAP3000 802.11 b/g or 802.11a card) and maximum of 1 radio supported by Atheros 802.11a card; these are numerated 1 to 6 for the maximum of 2 WLAN cards.

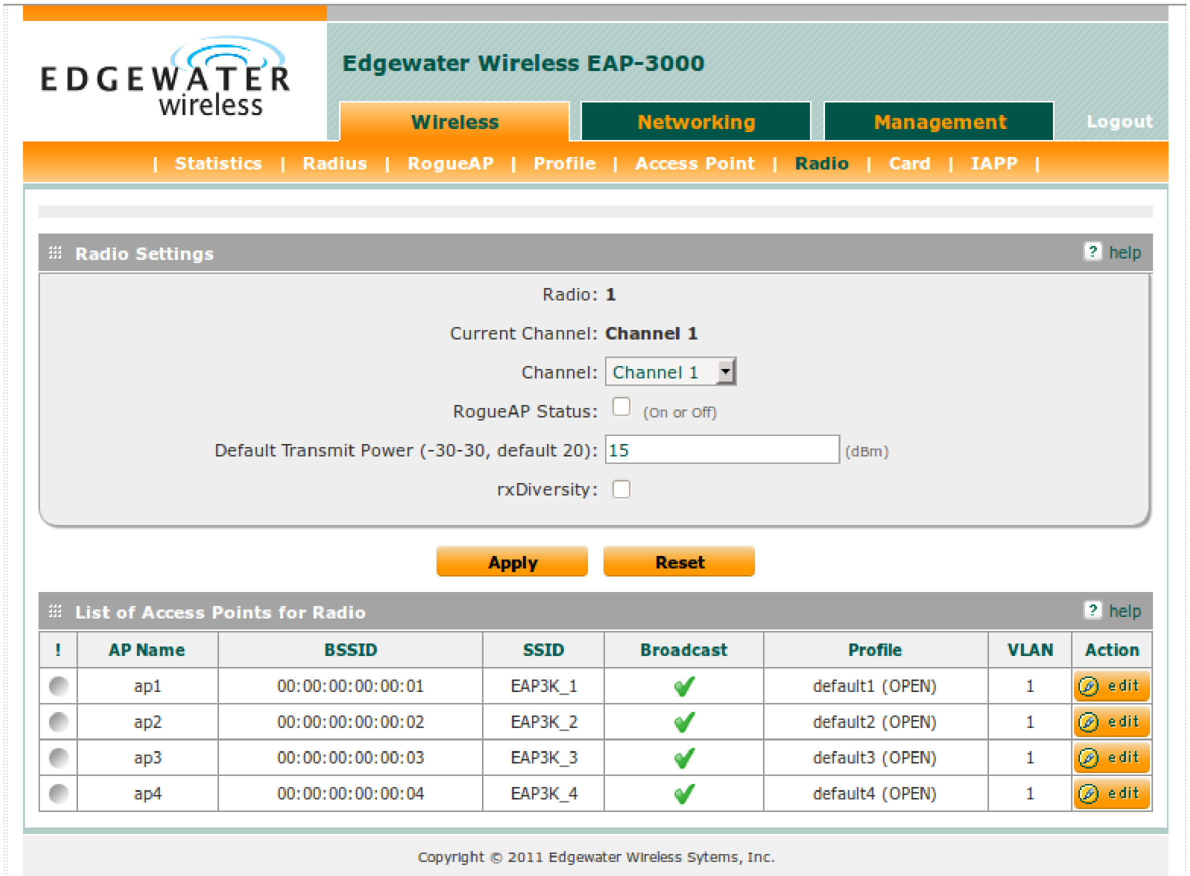
Channel: Current selected channel for the radio

Card: This field indicates which of the 2 cards the radio is using

Path: There are 3 possible paths on an EAP3000 card. Each radio is mapped to a unique path.

RogueAP Status: The green tick mark indicates that RogueAP detection is enabled on this radio; the red ‘cancel’ icon indicates the RogueAP detection is disabled on this radio

Action/Edit: The edit button links to the associated radio settings page.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Apply
Reset
help

Radio Settings

Radio: **1**

Current Channel: **Channel 1**

Channel: Channel 1

RogueAP Status: □ (On or Off)

Default Transmit Power (-30-30, default 20): 15 (dBm)

rxDiversity: □

List of Access Points for Radio

!	AP Name	BSSID	SSID	Broadcast	Profile	VLAN	Action
●	ap1	00:00:00:00:00:01	EAP3K_1	✓	default1 (OPEN)	1	edit
●	ap2	00:00:00:00:00:02	EAP3K_2	✓	default2 (OPEN)	1	edit
●	ap3	00:00:00:00:00:03	EAP3K_3	✓	default3 (OPEN)	1	edit
●	ap4	00:00:00:00:00:04	EAP3K_4	✓	default4 (OPEN)	1	edit

Copyright © 2011 Edgewater Wireless Sytems, Inc.

3.11 Wireless -> Radio ->edit

Radio Settings

Radio: This displays the radio that is currently being edited.

Current Channel: This displays the channel currently used by the radio when the channel is manually selected. If the channel is set automatically, this field displays "0" as the channel.

Channel: Select a channel from the list of channels or choose “auto” to let system determine the best channel to use.

RogueAP status: Select this check box to enable RogueAP detection on this radio.

Default Transmit Power: Enter a value in dBm as the default transmitted power level for all APs that use this radio. The range is -30dBm to 30dBm with a default of 20dBm

rxDiversity: Enable receive diversity. This is only applicable when multiple receive antennae are used

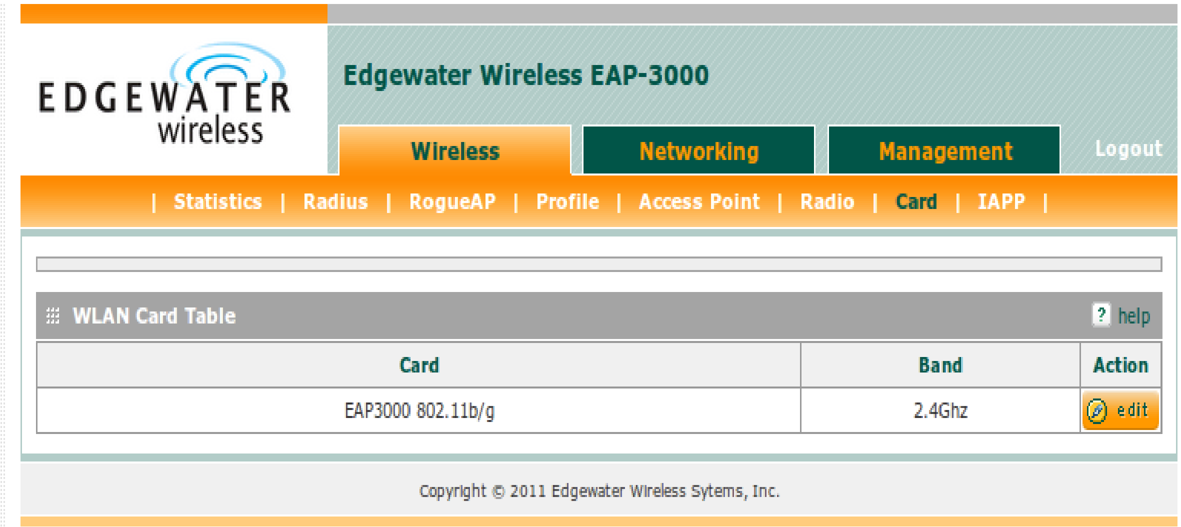
Click Apply to save your changes.

Click Reset to revert to the previous settings.

List of Access Points for Radio

This table displays all the VAP's that are configured for a particular radio. The actions that can be taken on the List of Access Points for Radio is:

Edit: Allows the configuration of a VAP on the current radio


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
? help

WLAN Card Table

Card	Band	Action
EAP3000 802.11b/g	2.4Ghz	edit

Copyright © 2011 Edgewater Wireless Sytems, Inc.

3.12 Wireless -> Card

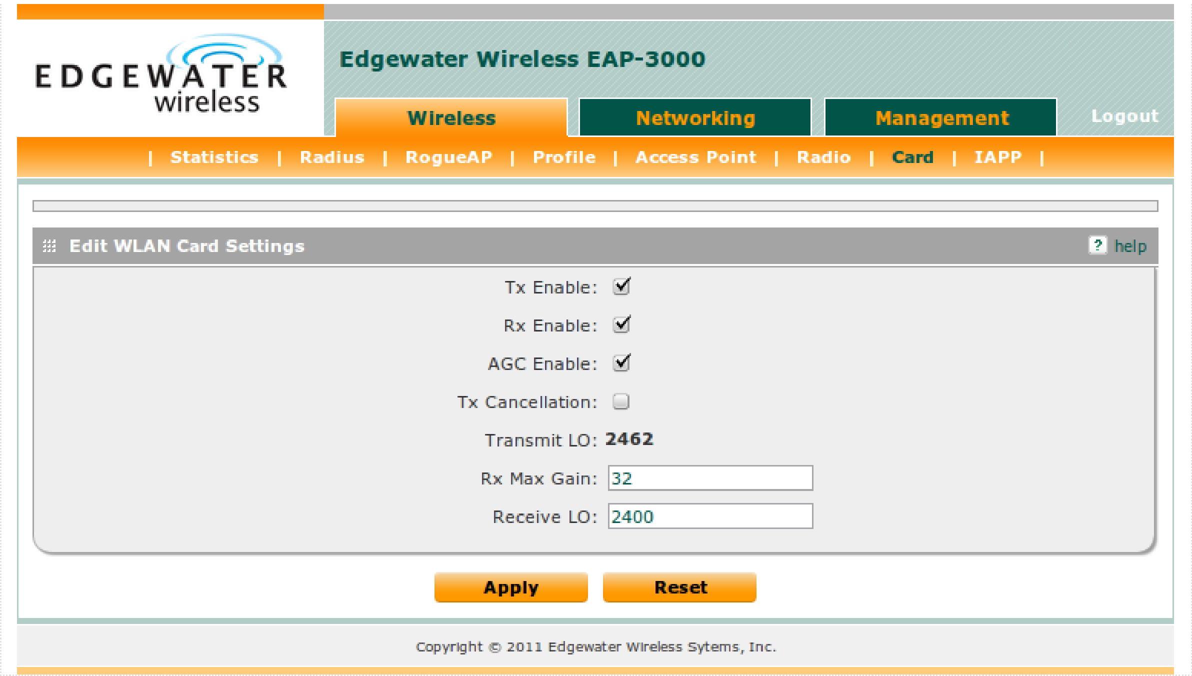
This page lists the number and type of wireless cards present in the system

List of the Card/Cards currently installed in the AP

The frequency band used by the associated wireless card

Action: The edit button links to the associated card’s settings page.

3.13 Wireless -> Card -> edit


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Edit WLAN Card Settings
? help
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Tx Enable: ☑

Rx Enable: ☑

AGC Enable: ☑

Tx Cancellation: ☐

Transmit LO: 2462

Rx Max Gain: 32

Receive LO: 2400

This page allows the administrator to change parameters pertaining to the wireless card.

WARNING: Changing these parameters can render the Access Point inoperable.

Tx Enable: De-select this check box to disable transmit

Rx Enable: De-select this check box to disable receive

AGC Enable: select to allow this card to adjust its gain settings depending on the connection with the client (automatic gain control)

Tx Cancellation: select to enable Crosstalk

Transmit LO: Displays the frequency of the Local Transmit Oscillator

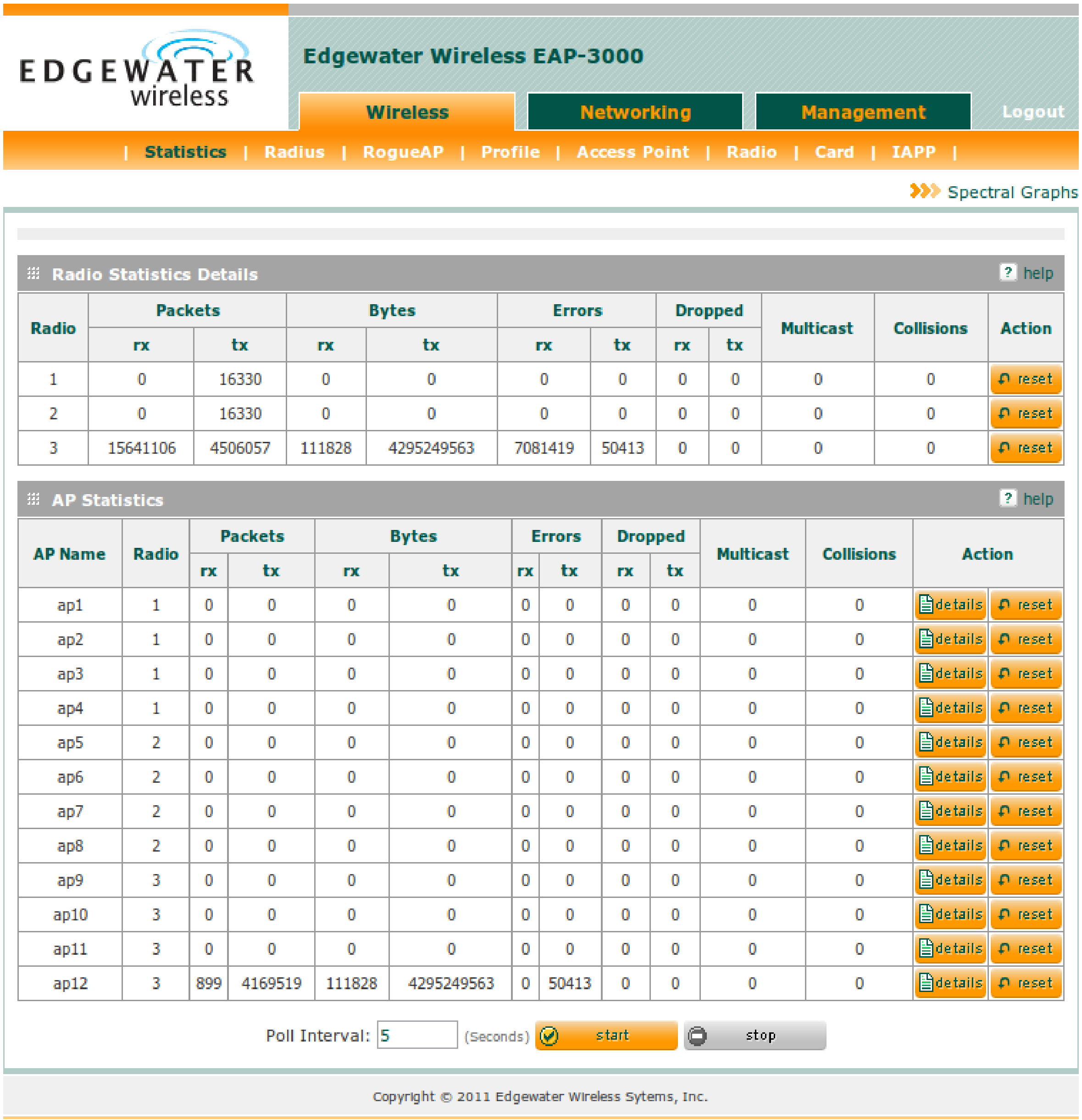
Rx Max Gain: This is the maximum gain that can be applied to the received data

Receive LO: Displays the frequency of the Local Receive Oscillator

Click Apply to save your changes.

Click Reset to revert to the previous settings.

3.14 Wireless -> Statistics



Edgewater Wireless EAP-3000

Radio Statistics Details

Radio	Packets		Bytes		Errors		Dropped		Multicast	Collisions	Action
	rx	tx	rx	tx	rx	tx	rx	tx			
1	0	16330	0	0	0	0	0	0	0	0	reset
2	0	16330	0	0	0	0	0	0	0	0	reset
3	15641106	4506057	111828	4295249563	7081419	50413	0	0	0	0	reset

AP Statistics

AP Name	Radio	Packets		Bytes		Errors		Dropped		Multicast	Collisions	Action
		rx	tx	rx	tx	rx	tx	rx	tx			
ap1	1	0	0	0	0	0	0	0	0	0	0	details reset
ap2	1	0	0	0	0	0	0	0	0	0	0	details reset
ap3	1	0	0	0	0	0	0	0	0	0	0	details reset
ap4	1	0	0	0	0	0	0	0	0	0	0	details reset
ap5	2	0	0	0	0	0	0	0	0	0	0	details reset
ap6	2	0	0	0	0	0	0	0	0	0	0	details reset
ap7	2	0	0	0	0	0	0	0	0	0	0	details reset
ap8	2	0	0	0	0	0	0	0	0	0	0	details reset
ap9	3	0	0	0	0	0	0	0	0	0	0	details reset
ap10	3	0	0	0	0	0	0	0	0	0	0	details reset
ap11	3	0	0	0	0	0	0	0	0	0	0	details reset
ap12	3	899	4169519	111828	4295249563	0	50413	0	0	0	0	details reset

Poll Interval: 5 (Seconds)

Copyright © 2011 Edgewater Wireless Sytems, Inc.

This page shows a cumulative total of relevant wireless statistics for the VAPs and radios; the counter is reset when the device is rebooted.

Radio Statistics Details

This table displays transmit/receive data for each radio.

Packets: the number of transmitted/received wireless packets

Bytes: the number of transmitted/received bytes of information

Errors: the number of transmitted/received packet errors reported to the radio

Dropped: the number of transmitted/received packets dropped between the radio and client

Multi-cast: the number of multi-cast packets sent over this radio

Collisions: the number of packet collisions reported to the radio

Action/reset: Clicking on reset will clear all the statistics for the selected radio.

AP Statistics Details

This table displays transmit/receive data for each VAP.

Packets: the number of transmitted/received wireless packets

Bytes: the number of transmitted/received bytes of information

Errors: the number of transmitted/received packet errors reported to the AP

Dropped: the number of transmitted/received packet dropped by the AP

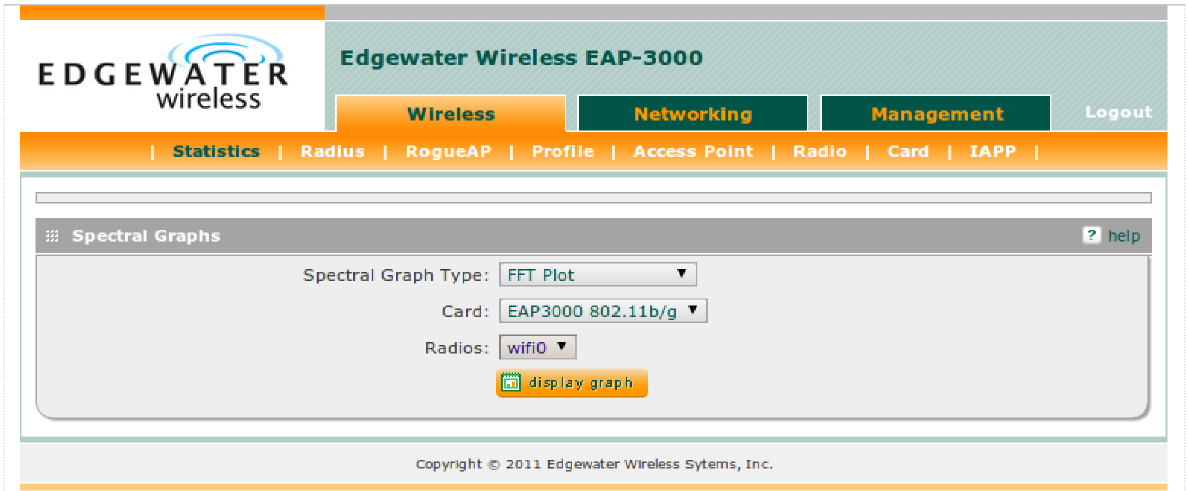
Multi-cast: the number of multi-cast packets sent over this AP

Collisions: the number of packet collisions reported to the AP

Action/Details: Clicking on details will open a pop-up window showing a detail list of parameters and associated values for the selected VAP. These stats are cumulative and reset when the device is rebooted.

Action/reset: Clicking on reset will clear the statistics for the selected VAP.

3.15 Wireless -> Statistics -> Spectral Graphs


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Spectral Graphs
help
display graph
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Spectral Graph Type: FFT Plot

Card: EAP3000 802.11b/g

Radios: wifi0

The Graphical FFT and Spectrogram feature aid visualization of the radio frequency spectrum in real-time. Its main uses are identification of sources of interference during initial deployment as well as during regular operation. Traditional 802.11 scanning devices identify the spectrum by scanning and retrieving SSID information from beacon frames. However, they fail the identification if the signal is too weak, too noisy or not 802.11 (microwave, alarm systems, audio and video distribution systems, for example). The Graphical FFT and Spectrogram avoids those problems by visualizing the raw frequency spectrum which is not bound to any particular protocol.

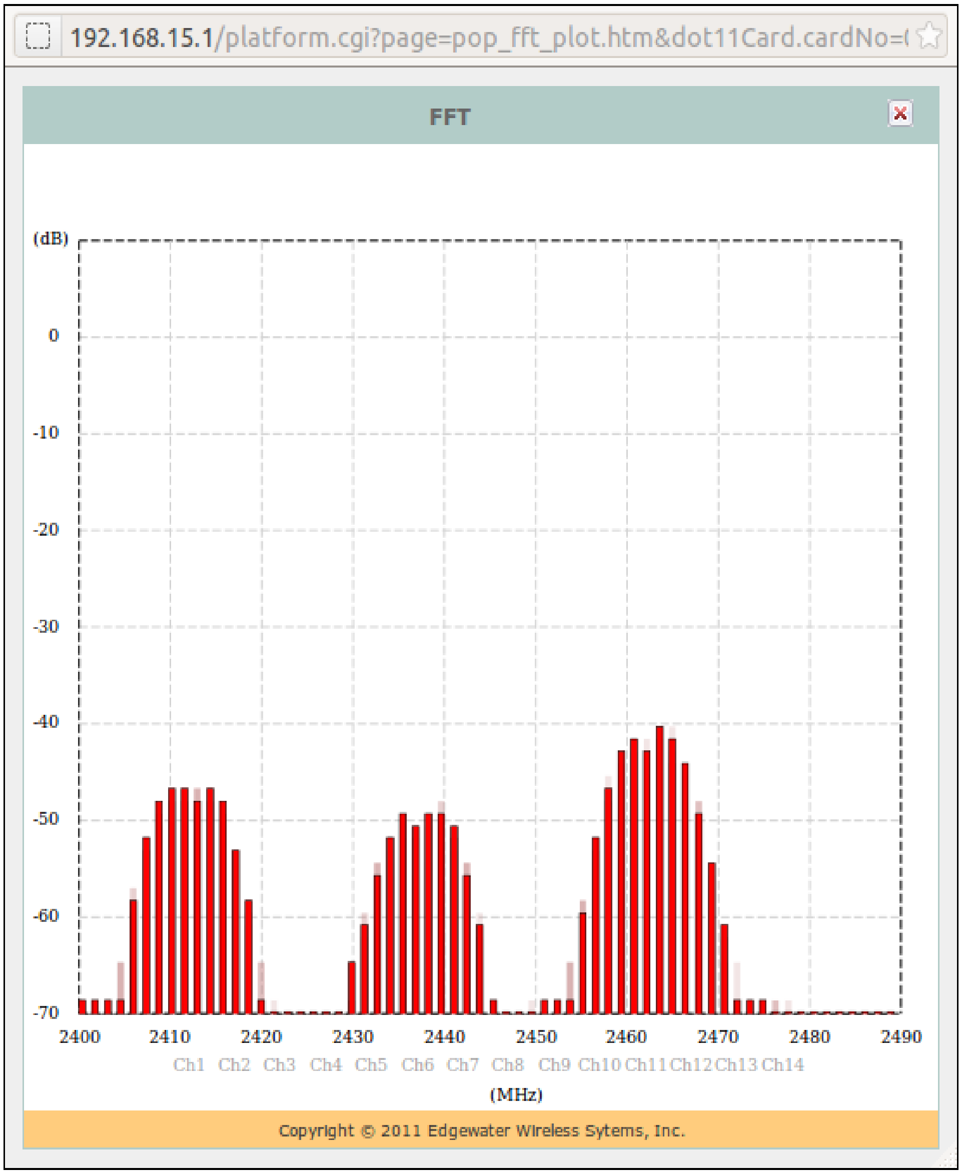
Spectral Graphs

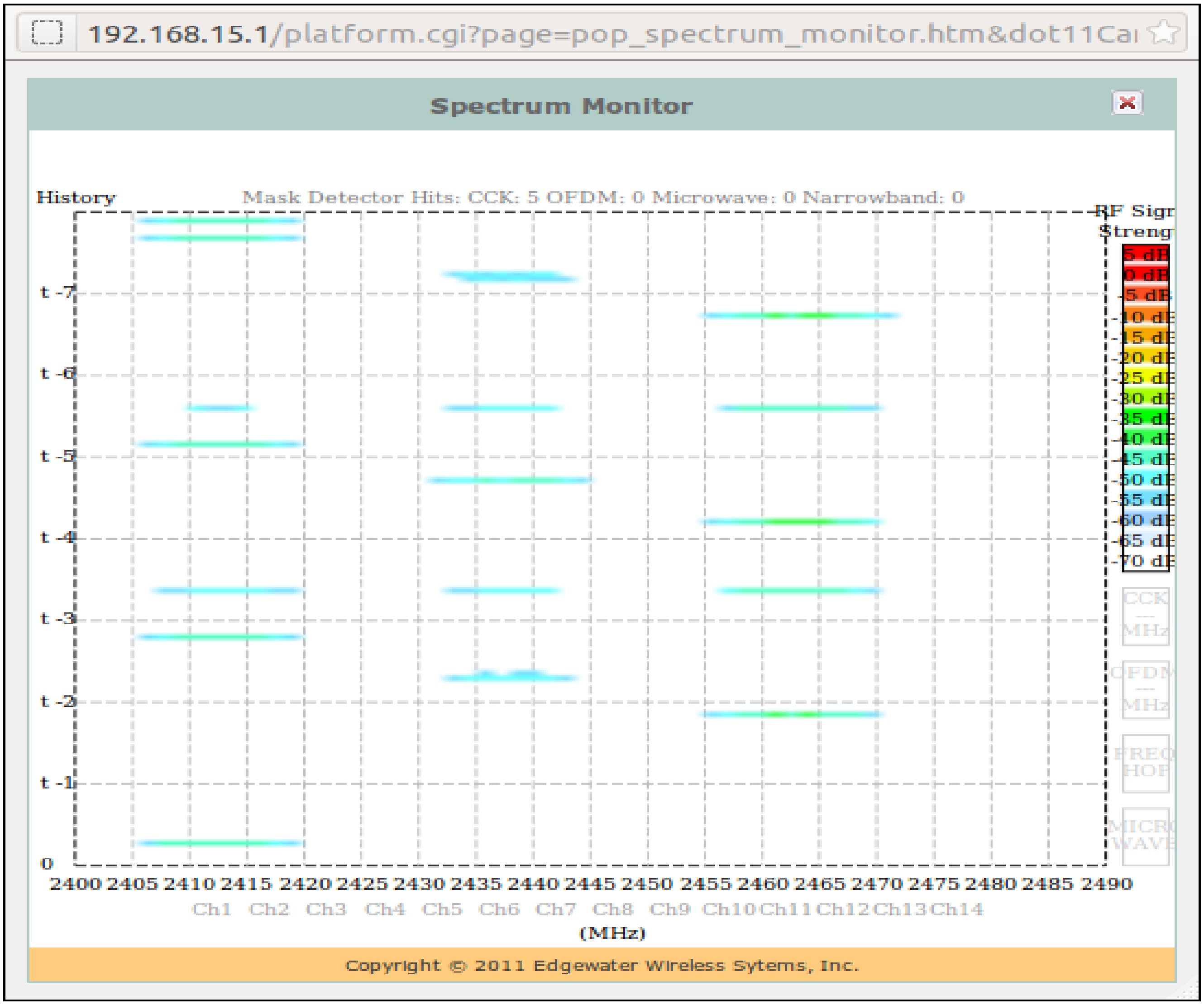
Spectral Graph Type: This AP supports 2 types of graphs to display: FFT Plot and Spectrum Monitor.

Card: Choose the radio card (if more than 1 on the AP) for which to display the selected graphs.

Click Display Graph to launch a window with the desired spectral graph. To display the FFT and spectrum monitor graphs ensure that pop-up blocker is disabled in your browser.

3.16 Wireless -> Statistics -> Spectral Graphs -> FFT Plot


192.168.15.1/platform.cgi?page=pop_fft_plot.htm&dot11Card.cardNo=(
FFT
(dB)
0
-10
-20
-30
-40
-50
-60
-70
2400
2410
2420
2430
2440
2450
2460
2470
2480
2490
Ch1
Ch2
Ch3
Ch4
Ch5
Ch6
Ch7
Ch8
Ch9
Ch10
Ch11
Ch12
Ch13
Ch14
(MHz)
Copyright © 2011 Edgewater Wireless Sytems, Inc.



192.168.15.1/platform.cgi?page=pop_spectrum_monitor.htm&dot11Ca

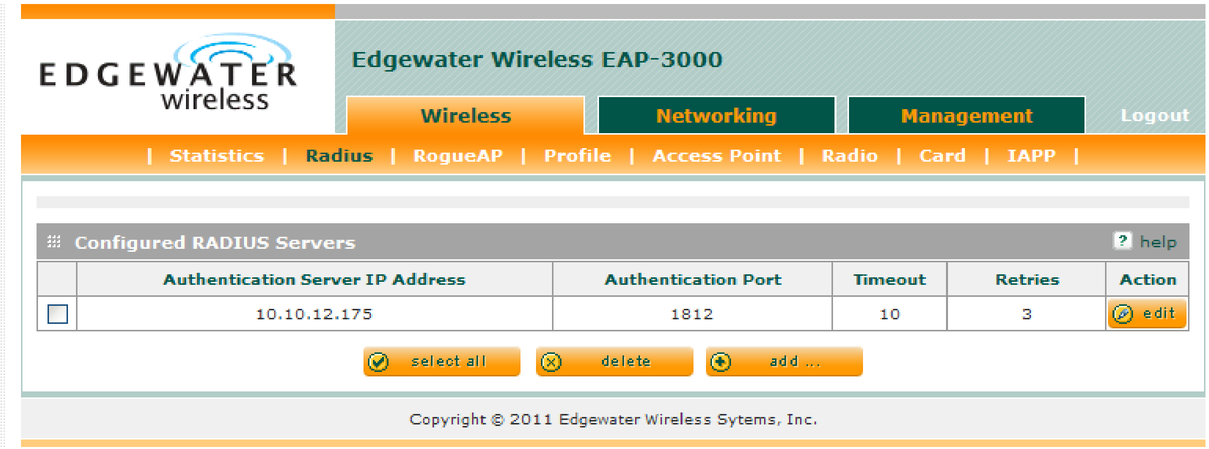
Spectrum Monitor

Mask Detector Hits: CCK: 5 OFDM: 0 Microwave: 0 Narrowband: 0

Copyright © 2011 Edgewater Wireless Sytems, Inc.

3.17 Wireless -> Statistics -> Spectral Graphs -> Spectrum Monitor

3.18 Wireless -> Radius


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Configured RADIUS Servers
help
select all
delete
add ...

	Authentication Server IP Address	Authentication Port	Timeout	Retries	Action
□	10.10.12.175	1812	10	3	edit

Copyright © 2011 Edgewater Wireless Sytems, Inc.

A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server already exists, it can be used for authenticating users that want to connect to the wireless network provided by this device. When multiple RADIUS servers are configured they are accessed in the same order as in the table. If first RADIUS server is not accessible, then the system tries to contact the next RADIUS server.

Configured RADIUS Servers

This table displays the list of configured RADIUS servers.

Authentication Server IP Address: IP address of RADIUS authentication server

Authentication Port: RADIUS authentication server port to send the RADIUS messages.

Timeout: The time (in seconds) the device waits for a response from the RADIUS server

Retries: The number of tries the Access Point will make to the RADIUS server before giving up.

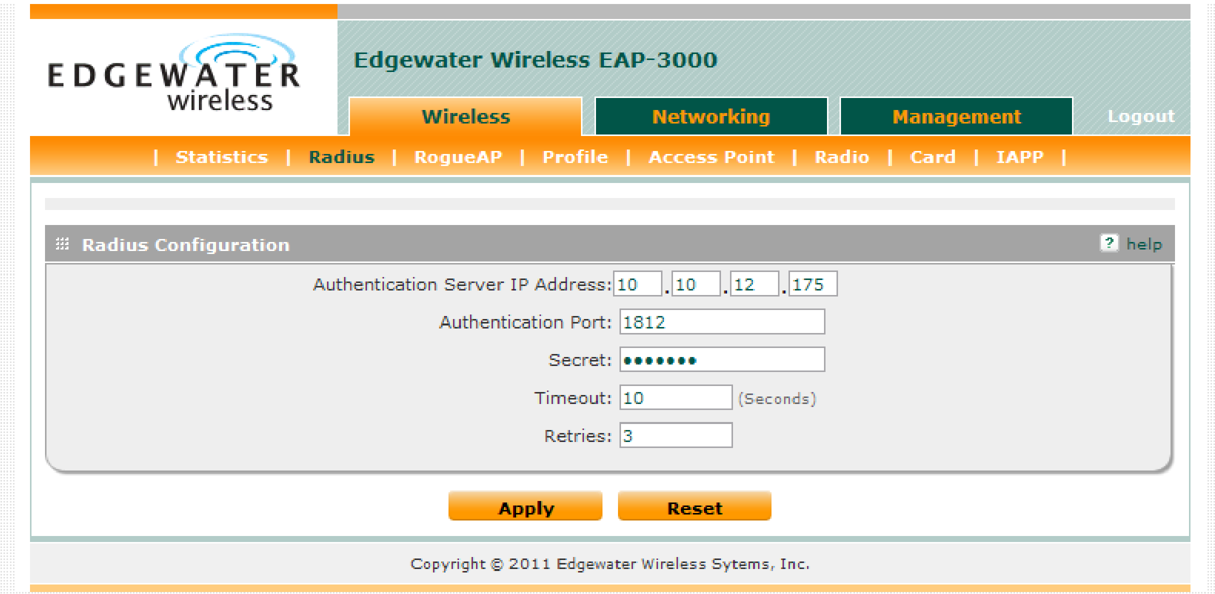
Action/Edit: The edit button links to the associated RADIUS Configuration page.

The actions that can be taken on RADIUS servers are:

Select All: Select all the RADIUS servers in the table

Delete: Deletes the selected RADIUS servers

Add: Add a new RADIUS server


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
help
Apply
Reset

Radius Configuration

Authentication Server IP Address: 10 . 10 . 12 . 175

Authentication Port: 1812

Secret: •••••••

Timeout: 10 (Seconds)

Retries: 3

Copyright © 2011 Edgewater Wireless Sytems, Inc.

3.19 Wireless -> Radius->edit

RADIUS Configuration

This table displays the configurable parameters of the RADIUS server.

Authentication Server IP Address: IP address of RADIUS authentication server

Authentication Port: RADIUS authentication server port to send the RADIUS messages.

Secret: The password to the RADIUS server

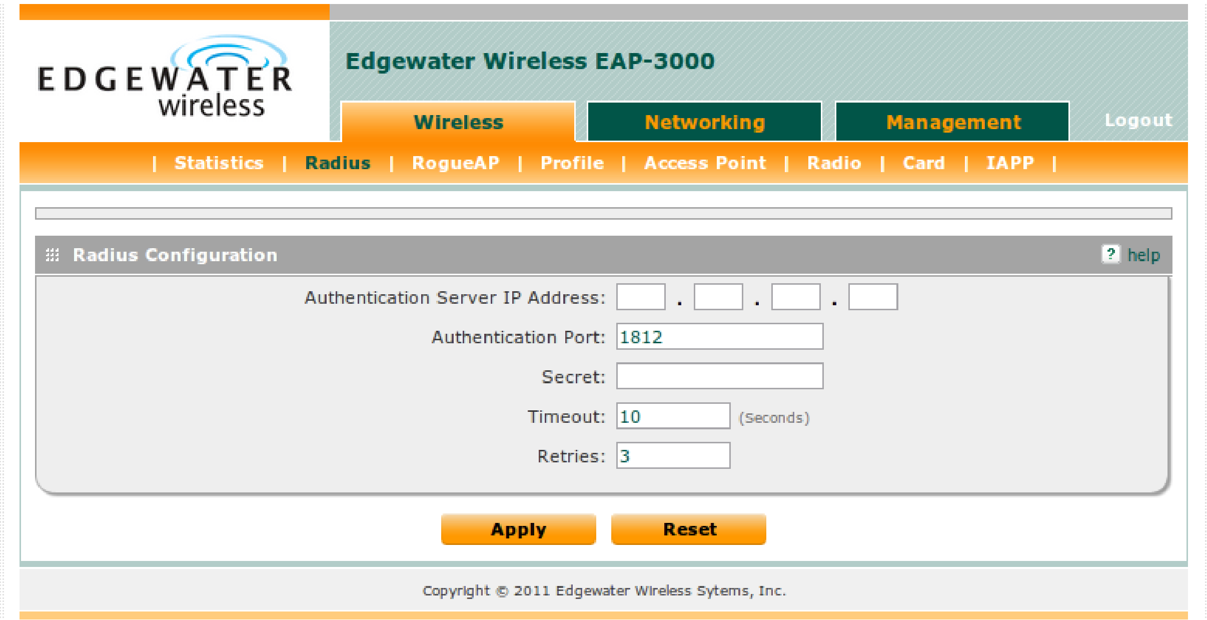
Timeout: The time (in seconds) the device waits for a response from the RADIUS server

Retries: The number of tries the Access Point will make to the RADIUS server before giving up.

Click Apply to save your changes.

Click Reset to revert to the previous settings.

3.20 Wireless -> Radius -> Add


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Statistics | Radius | RogueAP | Profile | Access Point | Radio | Card | IAPP |
Radius Configuration
? help
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Authentication Server IP Address: ___ . ___ . ___ . ___

Authentication Port: 1812

Secret:

Timeout: 10 (Seconds)

Retries: 3

RADIUS Configuration

This page allows the user to configure a new RADIUS server to be used for authentication.

Authentication Server IP Address: IP address of RADIUS authentication server

Authentication Port: RADIUS authentication server port to send the RADIUS messages.

Secret: The password to the RADIUS server

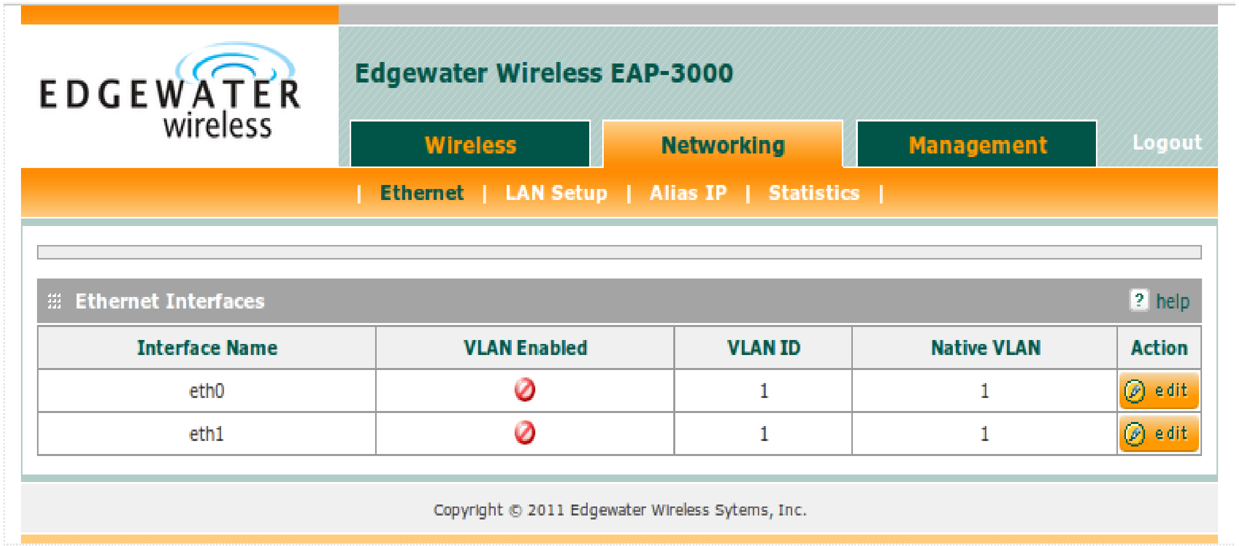
Time out period: Set the amount of time in seconds, the Access Point should wait for a response from the RADIUS server.

Maximum Retry Count: This determines the number of tries the Access Point will make to the RADIUS server before giving up.

Click Apply to save the settings.

Click Reset to revert to the previous settings.

4 Networking


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Ethernet | LAN Setup | Alias IP | Statistics |
? help

Ethernet Interfaces

Interface Name	VLAN Enabled	VLAN ID	Native VLAN	Action
eth0	⊘	1	1	edit
eth1	⊘	1	1	edit

Copyright © 2011 Edgewater Wireless Sytems, Inc.

4.1 Networking -> Ethernet

This device has two Ethernet interfaces, eth0 and eth1. Both eth0 and eth1 Ethernet interfaces and all the wireless interfaces are bridged under a virtual interface called "bdg". This allows wireless clients to access the local area network (LAN) via the Ethernet ports.

Ethernet Interfaces

This table displays the available Ethernet interfaces on the Access Point.

Interface Name: Name of the Ethernet interface (eth0, eth1)

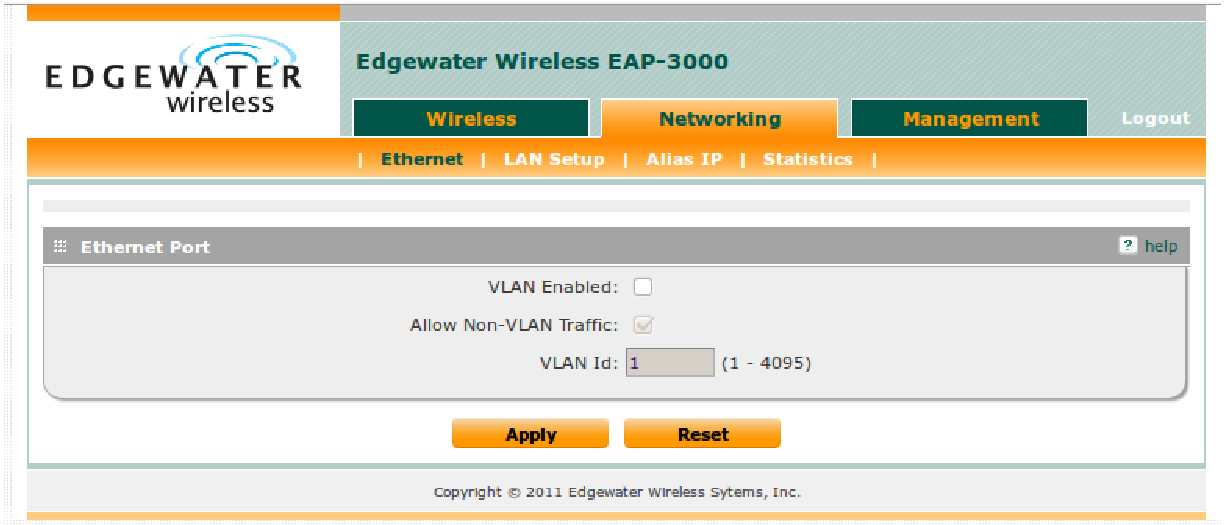
VLAN Enabled: A green check mark indicates that VLAN is enabled on the interface, a red cancel icon indicates that VLAN is not enabled on the interface.

VLAN ID: The ID (1 – 4095) of the configured VLAN for the interface

Native VLAN: Native VLAN is the default VLAN tag to be added to the incoming non-VLAN tagged traffic. The VLAN ID assigned to a VAP may be considered as the Native VLAN although Native VLAN is not a provision-able attribute for the VAPs.

Action/Edit: The edit button links to the Ethernet Port configuration page.

4.2 Networking -> Ethernet->edit


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Ethernet | LAN Setup | Alias IP | Statistics |
Ethernet Port
help

VLAN Enabled: □

Allow Non-VLAN Traffic: ☑

VLAN Id: 1 (1 - 4095)

Copyright © 2011 Edgewater Wireless Sytems, Inc.

The Virtual Local Area Network (VLAN) feature makes use of the 802.1Q header of the Ethernet frames to identify individual traffic groups. For the EAP3000, the key advantage of the VLAN feature is that it allows for the segregation of data traffic into VLAN groups. A VLAN group consists of EAP3000 interfaces which have VLAN enabled and have been assigned the same VLAN identifier (VLAN ID). Two EAP3000 interfaces must belong to the same VLAN group (and with VLAN enabled) for data traffic to flow between them.

Another advantage of the EAP3000 VLAN feature is the restriction of access to the EAP3000 Management Entity to that of the Management VLAN ID. The Management VLAN ID is the VLAN ID assigned to the VLAN trunk port, eth0. The EAP3000 Management Entity is responsible for the control of the EAP3000 system. It is the termination point of the web GUI and CLI sessions on an EAP3000. The VLAN feature helps protect the EAP3000 from unauthorized accesses.

A VLAN ID is a value between 1 and 4095. If an Ethernet frame is VLAN tagged, the given VLAN ID is in the 802.11Q header of the Ethernet frame. The default VLAN ID is 1 for all the EAP3000 interfaces.

Each interface of the EAP3000, namely Ethernet interfaces eth0, eth1 and all the Virtual Access Points (VAPs) can be assigned a single VLAN ID. The assigned VLAN ID is meaningful only if VLAN is enabled for the given interface.

A VLAN ID can be assigned to multiple interfaces (interface eth0, eth1 and the VAPs) allowing data traffic to flow amongst the interfaces. In the case of an interface having a unique VLAN ID, the traffic will flow between the particular interface and the VLAN Trunk Port (i.e., Ethernet interface eth0) provided VLAN is enabled on Ethernet interface eth0; if VLAN is disabled on Ethernet interface eth0, then an interface having a unique VLAN ID will become isolated (i.e., not able to inter-work with another interface on the EAP3000).

The Management VLAN ID is the VLAN ID assigned to the VLAN Trunk Port, eth0. The Management VLAN ID is meaningful only if VLAN is enabled on eth0. Other interfaces may be assigned the same Management VLAN ID as well.

If VLAN ID is enabled on the VLAN Trunk Port (interface eth0), for VLAN tagged traffic arriving from one of the EAP3000 interfaces (eth0, eth1 and VAPs), only those carrying the Management VLAN ID tagged can access the EAP3000 Management Entity. Non-VLAN traffic between interfaces eth0 and eth1 to the EAP3000 Management Entity are allowed. Non-VLAN traffic between VAP interfaces and the EAP3000 Management Entity are disallowed.

Ethernet Port

This page allows the user to enable VLAN on the selected Ethernet interface. If the VLAN Enabled check box is selected it will allow the configuration of Allow Non-VLAN Traffic and also configuration of the VLAN ID.

VLAN enabled: Click the check box to enable VLAN for the selected interface.

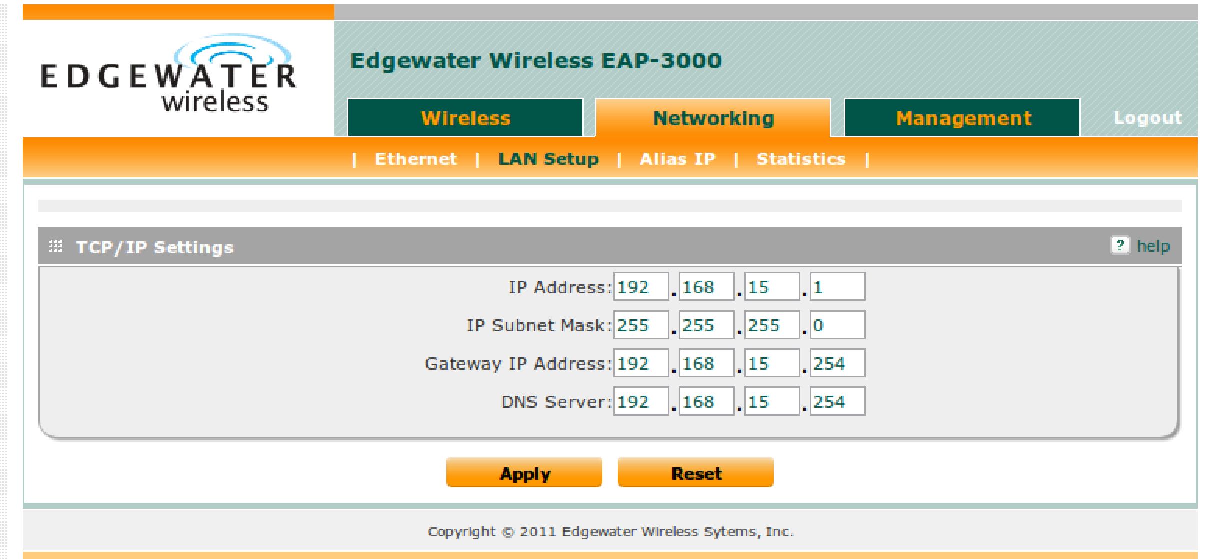
Allow Non-VLAN Traffic: Click the check box to allow non-VLAN traffic on the selected interface.

VLAN ID: set the chosen VLAN ID to the VLAN for the selected interface.

Click Apply to save the settings.

Click Reset to revert to the previous settings.

4.3 Networking-> Ethernet -> LAN Setup


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Ethernet | LAN Setup | Alias IP | Statistics |
TCP/IP Settings
? help
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

IP Address: 192 . 168 . 15 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 192 . 168 . 15 . 254

DNS Server: 192 . 168 . 15 . 254

This page allows the administrator to configure the IP addresses to manage this Access Point.

TCP/IP Settings

IP Address: The static IP address of this device

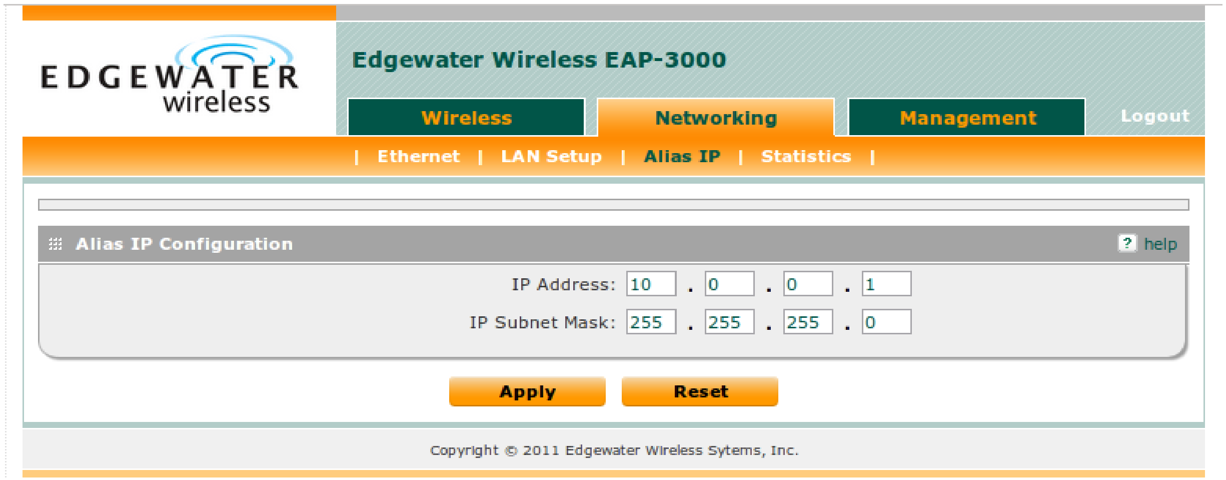
Subnet Mask: IPv4 Subnet Mask

Gateway IP Address: IP address of the gateway. This is usually provided by the ISP or your network administrator.

Domain name servers (DNS): DNS server IP address to convert the Internet name (such as www.google.com) to an IP address.

Click Apply to save the settings.

Click Reset to revert to the previous settings.



IP Address: 10 . 0 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

Copyright © 2011 Edgewater Wireless Sytems, Inc.

4.4 Networking-> Alias IP

This page allows the administrator to configure the alias IP address for the Access Point.

The Alias IP is a secondary IP address that can be used to access the management interface.

Alias IP Configuration

IP Address: The static IP address of this device

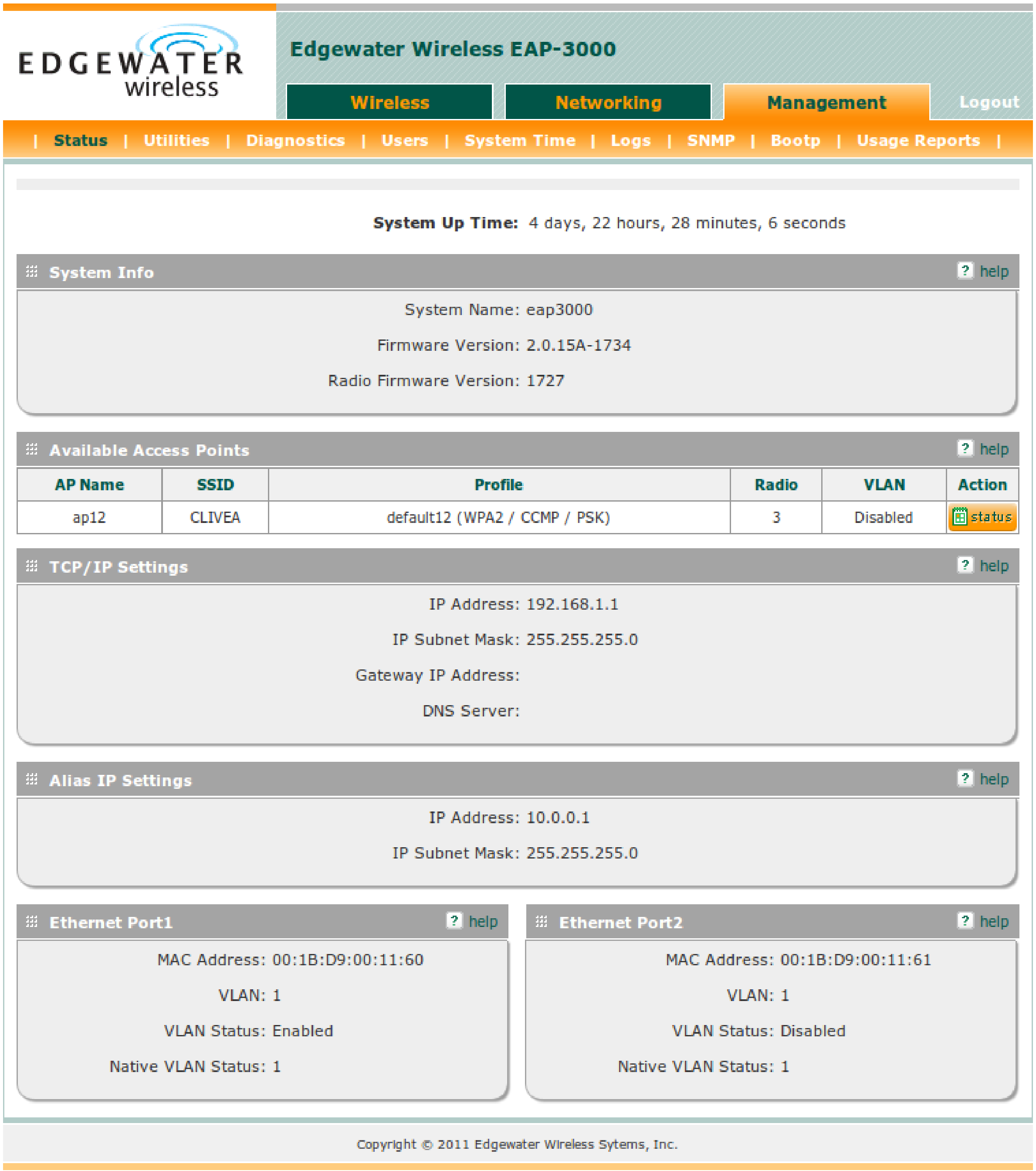
IP Subnet Mask: IPv4 Subnet Mask

Click Apply to save the settings.

Click Reset to revert to the previous settings.

5 Management

5.1 Management ->Status


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
help
status

System Up Time: 4 days, 22 hours, 28 minutes, 6 seconds

System Info

System Name: eap3000

Firmware Version: 2.0.15A-1734

Radio Firmware Version: 1727

Available Access Points

AP Name	SSID	Profile	Radio	VLAN	Action
ap12	CLIVEA	default12 (WPA2 / CCMP / PSK)	3	Disabled	status

TCP/IP Settings

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Gateway IP Address:

DNS Server:

Alias IP Settings

IP Address: 10.0.0.1

IP Subnet Mask: 255.255.255.0

Ethernet Port1

MAC Address: 00:1B:D9:00:11:60

VLAN: 1

VLAN Status: Enabled

Native VLAN Status: 1

Ethernet Port2

MAC Address: 00:1B:D9:00:11:61

VLAN: 1

VLAN Status: Disabled

Native VLAN Status: 1

Copyright © 2011 Edgewater Wireless Sytems, Inc.

This page displays current status of the device, including the configured VAPs, as well as other system information.

System Up Time: This is the time that the device has been on-line since its last reboot.

System Info

This section displays some basic the information about the system, including the System Name and the Firmware Versions.

System Name: Displays the name of the Access Point (eap3000)

Firmware Version: This is the version number of the firmware currently used by this device. By default, this AP device will boot from this version. This will change when the device firmware is upgraded.

Radio Firmware Version: Displays the version of the firmware currently running on the Radio card.

Available Access Points

The Available Access Points table displays the list of active VAPs for this device (from the AP table in the Access Points menu). From this summary list, status and parameters of each AP are available for display.

AP Name: This is the identifier which uniquely identifies the VAP in the list of configured VAPs.

SSID: The SSID (service set identifier) is the name of the wireless network serviced by this VAP; it is configured on the Profile page and later associated with AP by selecting it from the profile drop down box. Note that a given wireless profile can be common to multiple VAPs, and so the SSID is not unique to a VAP. In order for the computers or devices to communicate via this wireless network serviced by this VAP, all devices must select the same SSID from the list of wireless networks in the area.

Profile: This field has a brief description of the security, encryption and authentication combination assigned to the VAP. A Profile is not necessarily unique to a VAP; rather this grouping of wireless settings can be used on more than one VAP at the same time.

Radio: The physical radio on which this VAP is running on.

VLAN: The AP can be part of a logical network defined by the VLAN id; this allows devices connected to the VLAN through this AP to exchange data with one another as in a LAN.

Action/Status: The status button links to the statistics page for this VAP, displaying traffic information for the VAP and an overview of the connected clients. Note that this is the same page as Wireless->Access Point->Status.

TCP/IP Settings

This area displays the TCP/IP settings for the main Ethernet interface.

IP Address: The static IP address of this device

IP Subnet Mask: IPv4 Subnet Mask

Gateway IP Address: IP address of the gateway. This is usually provided by the ISP or your network administrator.

Domain name servers (DNS): DNS server IP address to convert the Internet name (such as www.google.com) to an IP address.

Alias IP Settings

This area displays the TCP/IP settings for the secondary Ethernet interface.

IP Address: The static IP address of this device

IP Subnet Mask: IPv4 Subnet Mask

Ethernet Port 1

This section displays information about Ethernet port 1.

MAC Address: MAC address for this port.

VLAN: This is the ID of the VLAN group to which this port belongs, if any.

VLAN Status: Status of VLAN on this port (Enabled or Disabled).

Allow Non-VLAN Traffic Status: This is a status indication of whether non-VLAN traffic is allowed through th port. 1 is displayed if non-VLAN traffic is allowed. 0 is displayed otherwise.

Ethernet Port 2

This section displays information about Ethernet port 2.

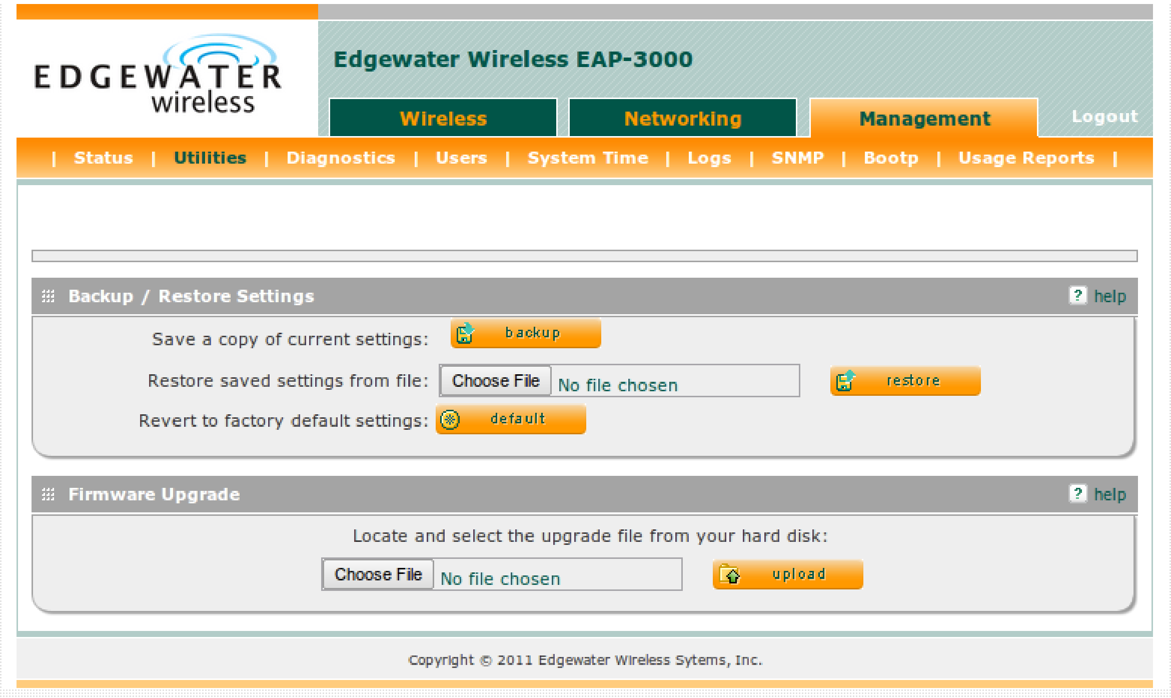
MAC Address: The LAN side configured MAC address for this port.

VLAN: This is the ID of the VLAN group to which this port belongs, if any.

VLAN Status: Status of VLAN on this port (Enabled or Disabled).

Allow Non-VLAN Traffic Status: This is a status indication of whether non-VLAN traffic is allowed through th port. 1 is displayed if non-VLAN traffic is allowed. 0 is displayed otherwise.

5.2 Management -> Utilities


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
help
backup
Choose File
restore
default
help
Choose File
upload

Backup / Restore Settings

Save a copy of current settings:

Restore saved settings from file: No file chosen

Revert to factory default settings:

Firmware Upgrade

Locate and select the upgrade file from your hard disk:

No file chosen

Copyright © 2011 Edgewater Wireless Sytems, Inc.

This page allows the user to save a backup copy of the device’s settings and restore them at a later time. You can also erase the settings completely and restore the factory defaults.

The Firmware Upgrade section is used to upgrade the device to a different firmware version.

IMPORTANT!

Restoring a saved configuration or resetting to defaults will remove your current settings. Configured VAPs, Profiles, RogueAP settings and all other settings will be lost. Please backup your settings. Settings cannot be retrieved unless they have been backed up.

When the settings restore operation or the firmware upgrade is in progress:

1. Do NOT close the browser window.

2. Do NOT go on-line.

3. Do NOT turn off or power-cycle the device.

4. Do NOT shutdown the computer that is connected to the management interface.

Backup / Restore Settings

To take a backup of the current settings:

Click Back Up.

You may be prompted to save a file with the extension ".cfg". Select a safe location on your computer and save the file.

The settings will be saved in this file.

To restore settings from a backup file:

Click Browse.

On your computer, locate and select the backup file you saved previously.

Click Restore.

A progress bar indicating the status of the restore operation will appear. The device will automatically restart after the Restore Settings operation has completed.

To revert to the factory default settings, click Default.

The device will restart automatically after resetting to the factory default settings. The factory default settings are as follows:

User Name: admin

Password: password

LAN Port 1 IP address: 192.168.1.1

Alias IP address: 10.0.0.1

Firmware Upgrade

New versions of firmware can be loaded onto the device in this section.

IMPORTANT!

A firmware upgrade may sometimes require a complete reconfiguration of the device. See the Release Notes which are included with the downloaded firmware file or go to the download page of the website for more information. Read the Release Notes for any information related to the upgrade before performing the upgrade operation.

To upgrade the Access Point software:

Click Browse.

Select the uncompressed firmware image file stored on your computer.

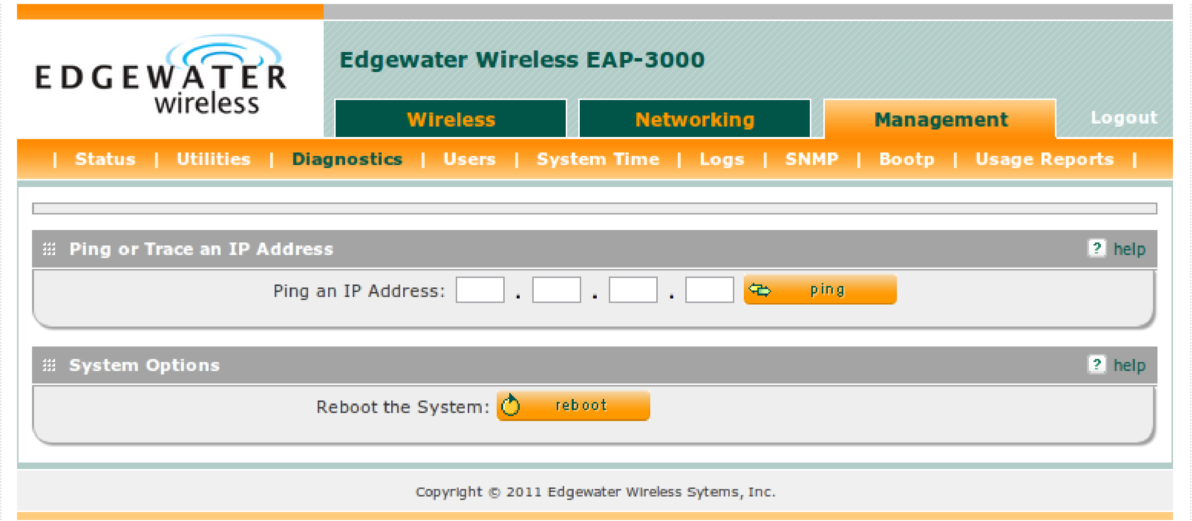
Click Upgrade. A progress bar will appear displaying the status of the upload.

The device will take several minutes to complete the upgrade.

Once the image upgrade is complete, the device will automatically restart.

After a successful upgrade, the Login page will display. After logging in, go to the Status page under the Management menu, to verify the firmware upgrade. The Firmware Version should be the same as the version selected for the upgrade.

If the upgrade was unsuccessful, see "Trouble Shooting" in the Reference Manual on the Resource CD.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
Ping or Trace an IP Address
? help
Ping an IP Address: . . .
ping
System Options
? help
Reboot the System:
reboot
Copyright © 2011 Edgewater Wireless Sytems, Inc.

5.3 Management -> Diagnostics

The diagnostics page allows the user to perform ping connectivity tests and system reboot.

Ping or Trace an IP Address

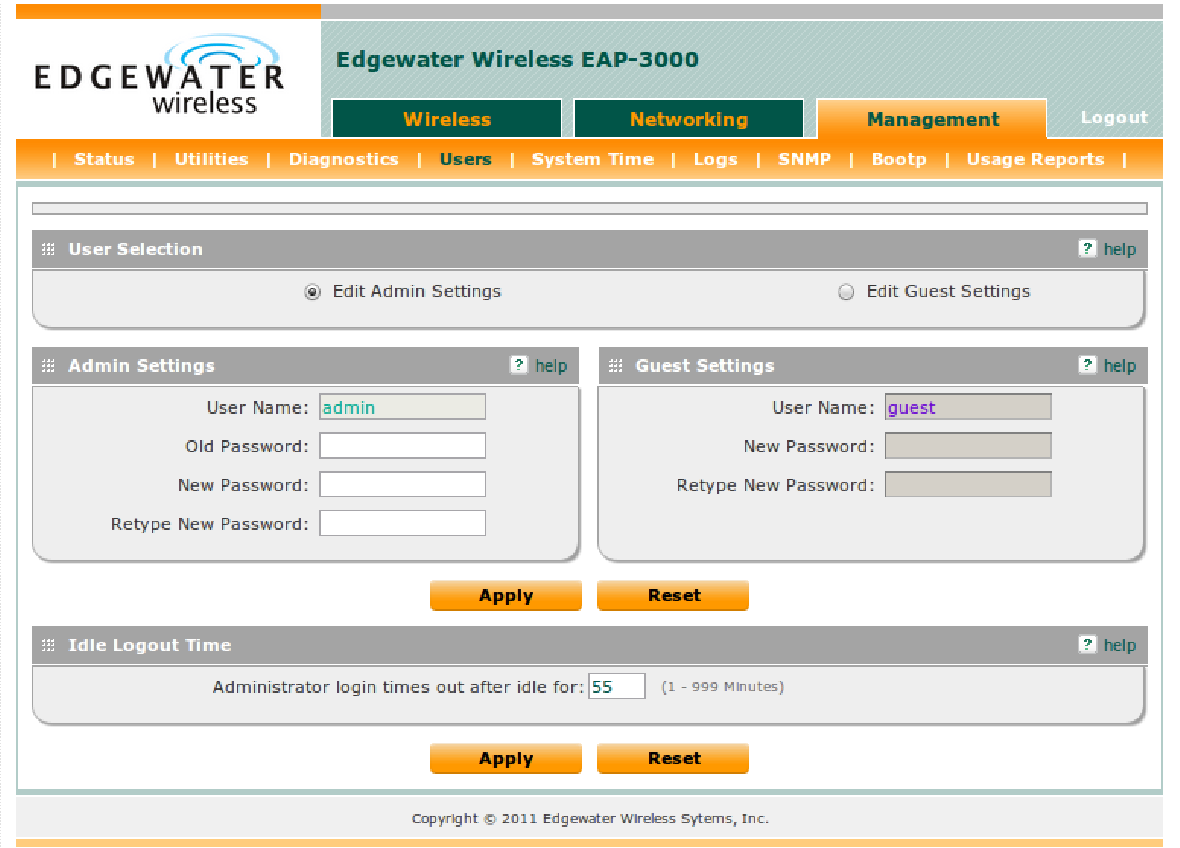
Ping: This utility can be used to test connectivity between this device and another device on the network connected to this system. Type in an IP address and click ping to send an ICMP echo request packet to the destination. If the destination IP address is active, you can see a response similar to “64 bytes from IP_Address: icmp……”. A “response timed out” message indicates that the destination is either not active or is blocking ping requests.

The results of the ping operation will be loaded in the current page. To return to the Diagnostics page, click on the back button of your browser.

System Options

Reboot the System: Click Reboot to restart the device from the web interface.

Note: All active connections to the AP and the connections going through the AP to the LAN will be disconnected while the restart is in progress.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
help
Apply
Reset

User Selection

● Edit Admin Settings ○ Edit Guest Settings

Admin Settings

User Name: admin
Old Password:
New Password:
Retype New Password:

Guest Settings

User Name: guest
New Password:
Retype New Password:

Idle Logout Time

Administrator login times out after idle for: 55 (1 - 999 Minutes)

Copyright © 2011 Edgewater Wireless Sytems, Inc.

5.4 Management -> Users

The Users page is used to change the system passwords for Administrator and Guest users. Only an administrator can make changes on this page.

Note: This password is used to login to the device and is NOT the same as the account password provided by your ISP.

User Selection

To change administrator credentials, click Edit Admin Settings. To change guest user settings, click Edit Guest Settings.

Admin Settings

This section allows you to change the settings for the account with administrator privileges. The following fields must be entered:

Old Password: Type in the current password.

New Password: Type in a new password

Retype New Password: Confirm the new password by re-entering it.

Guest Settings

This section allows you to change the settings of the guest user. The following fields must be entered:

New Password: Type in the new desired password.

Retype New Password: Confirm the new password by retyping it.

Click Apply to save your changes.

Click Reset to revert back to the previous settings.

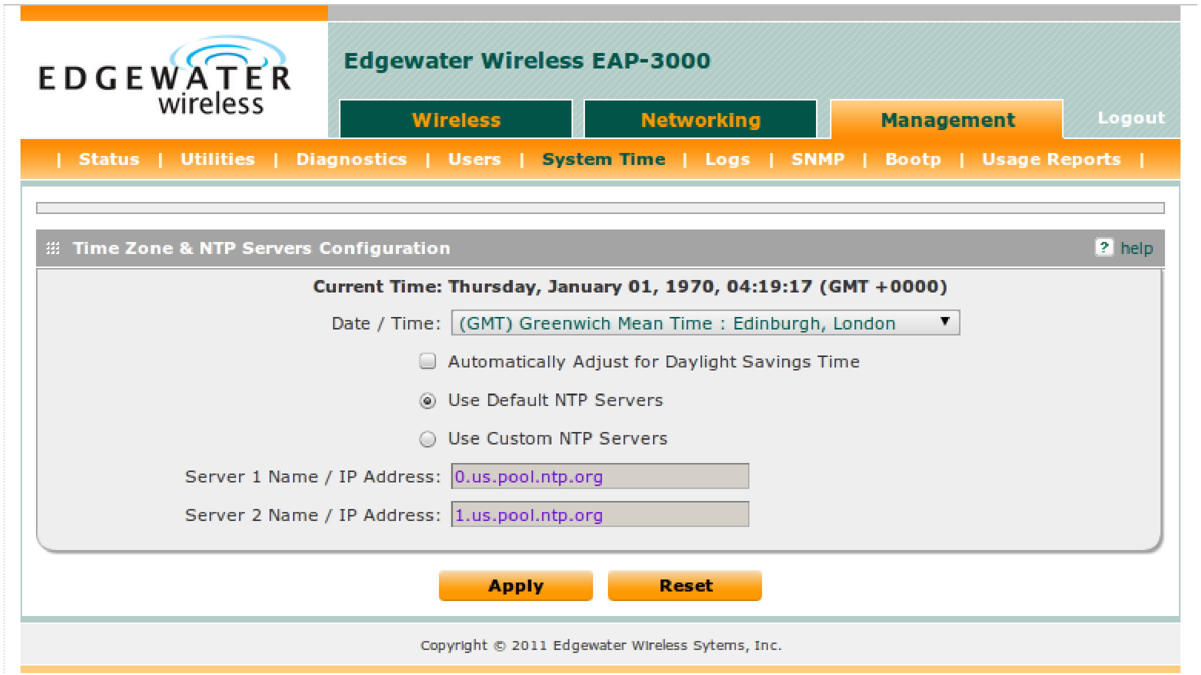
Idle Logout Time

For security reasons, the device will log you out of the web management interface after a period of inactivity. The factory default timeout is 5 minutes. To change the timeout period, type in a new value in the field labeled 'Administrator login times out after idle for' field.

Click Apply to save your changes.

Click Reset to revert back to the previous settings.

5.5 Management -> System Time


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
Time Zone & NTP Servers Configuration
? help
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Current Time: Thursday, January 01, 1970, 04:19:17 (GMT +0000)

Date / Time: (GMT) Greenwich Mean Time : Edinburgh, London ▼

□ Automatically Adjust for Daylight Savings Time

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: 0.us.pool.ntp.org

Server 2 Name / IP Address: 1.us.pool.ntp.org

This page allows for the configuration of the Time Zone and Network Time Protocol servers.

Time Zones & NTP Servers Configuration

Date / Time: Select your Local Time Zone.

Automatically Adujust for Daylight Savings Time: If the selected Time Zone uses Daylight Savings Time (DST) then select this option to have the Access Point automatically adjust for DST.

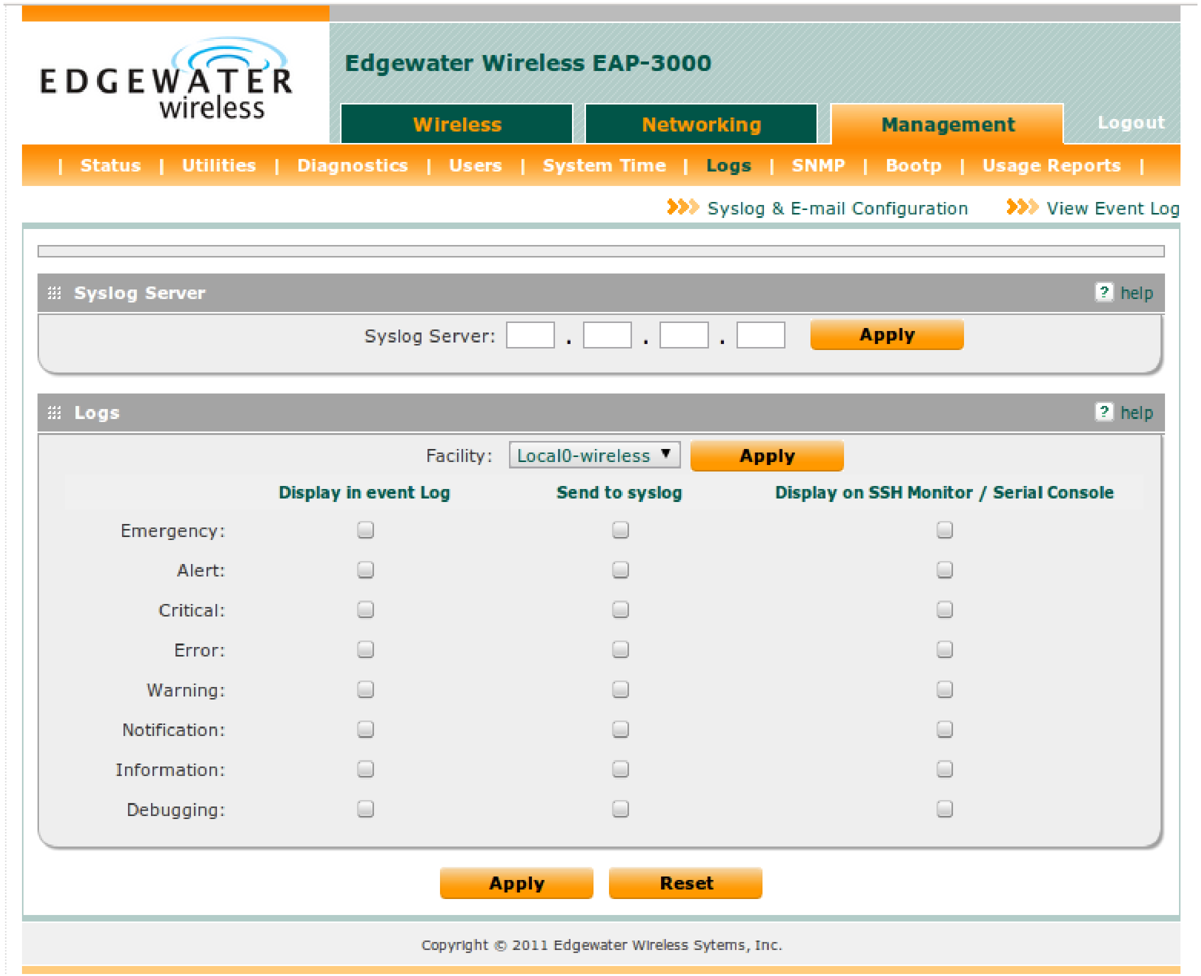
Use Default NTP Servers: If this is enabled, then time is updated regularly by contacting preconfigured default public NTP Servers on the Internet.

Use Custom NTP Servers: If you prefer to use a particular NTP server, enable this and enter the name or IP address of an NTP Server in the Server 1 Name/IP Address field. If required, you can also enter the address of another NTP server in the Server 2 Name/IP Address field.

Click Apply to save your changes.

Click Reset to revert to the previous settings.

Management -> Logs


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
Syslog & E-mail Configuration
View Event Log
Syslog Server
help
Apply
Logs
help
Apply
Apply
Reset

Syslog Server: ___ . ___ . ___ . ___

Facility: Local0-wireless

	Display in event Log	Send to syslog	Display on SSH Monitor / Serial Console
Emergency:	□	□	□
Alert:	□	□	□
Critical:	□	□	□
Error:	□	□	□
Warning:	□	□	□
Notification:	□	□	□
Information:	□	□	□
Debugging:	□	□	□

Copyright © 2011 Edgewater Wireless Sytems, Inc.

This page allows for the configuration of the Logging subsystem. There are a variety of events that can be captured and logged for review. These logs can be sent to a server or emailed as configured.

Syslog Server

Syslog Server: Enter the IP address of the syslog server. The logs will be sent to the server with this IP address.

Click Apply to save your changes.

Facility: The Facility drop-down allows you to select the type of functionality from which to generate logs: Kernel, Local0-wireless, or System.

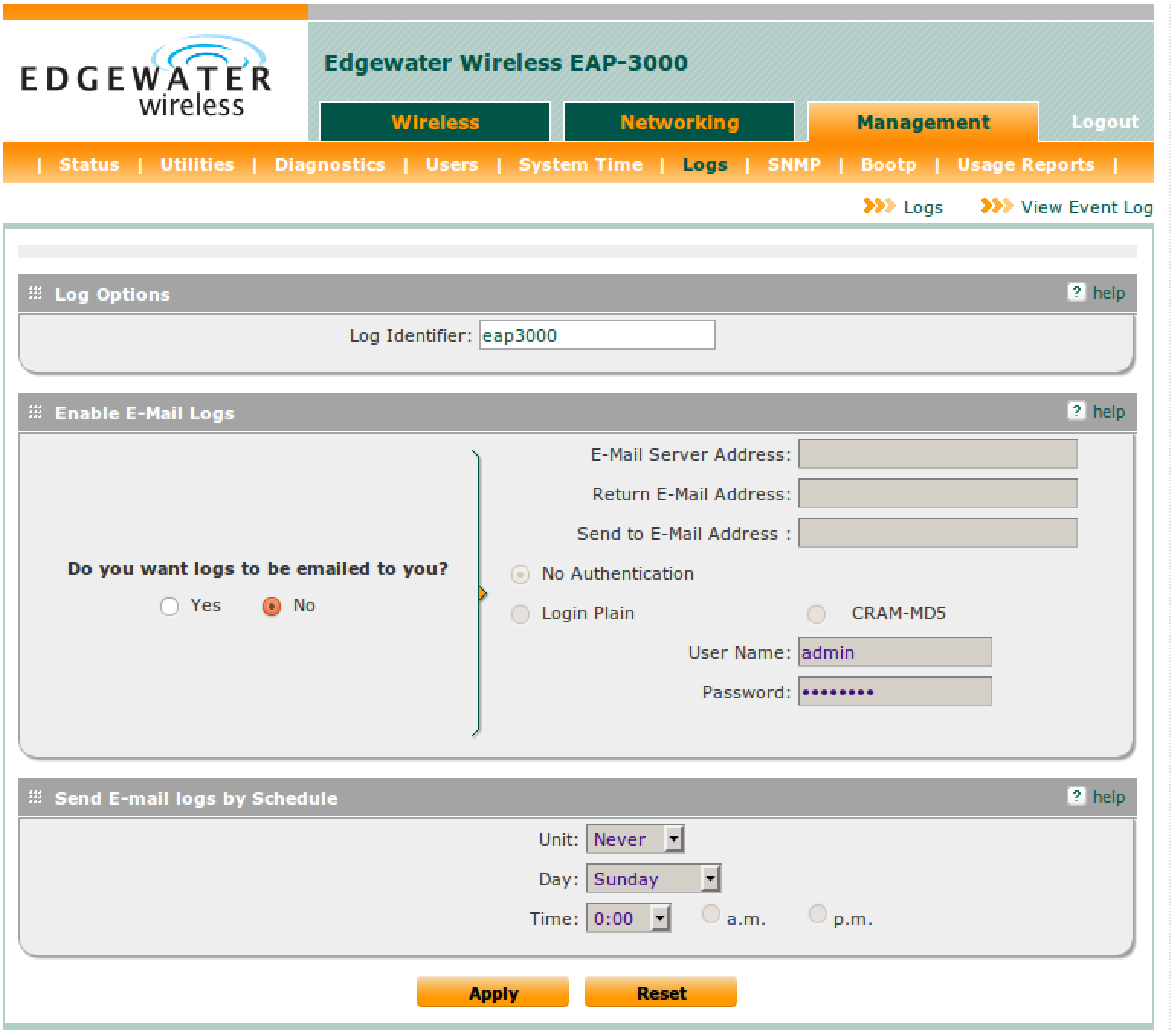
Click Apply to save your changes.

Events that can be logged: Select from Emergency, Alert, Critical, Error, Warning, Notification, Information, and Debugging.

For each of these events, you may select how to receive notification: Display in event Log, Notify via SNMP TRAP, Send to Syslog, Display on SSH monitor / Serial Console.

Click Apply to save your changes.

Click Reset to revert to the previous settings.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
Logs
View Event Log
help
Apply
Reset

Log Options

Log Identifier: eap3000

Enable E-Mail Logs

Do you want logs to be emailed to you?

○ Yes ● No

E-Mail Server Address:

Return E-Mail Address:

Send to E-Mail Address :

● No Authentication

○ Login Plain ○ CRAM-MD5

User Name: admin

Password: ••••••••

Send E-mail logs by Schedule

Unit: Never

Day: Sunday

Time: 0:00 ○ a.m. ○ p.m.

5.6 Management -> Logs -> Syslog & Email Configuration

The device can be configured to log and e-mail the selected events in the Logs page to a specified e-mail address or a SysLog server.

Log Options

Log Identifier: Every logged message will contain a prefix for easier identification of the source of the message. The log identifier will be prefixed to both, e-mail and Syslog messages.

Enable E-mail Logs

This section is used to configure e-mail settings for sending logs.

E-Mail Logs is disabled by default. Select the Yes radio box to enable e-mail logs.

E-mail Server address: Enter the IP address or Internet Name of the SMTP server. The device will connect to this server to send the e-mail logs.

Return E-mail Address: Type the e-mail address where the replies from the SMTP server are to be sent; for example, failure messages.

Send To E-mail Address: Type the e-mail address where the logs and alerts are to be sent.

Authentication with SMTP server: If the SMTP server requires authentication before accepting connections, select either Login Plain or CRAM-MD5 and enter the User Name and Password to be used for authentication. To disable authentication, select the No Authentication radio box.

Send E-mail logs by Schedule

To receive e-mail logs according to a schedule, select the appropriate schedule. To enable scheduling, configure the e-mail settings in the Enable E-Mail Logs section. To disable sending logs, select Never.

Unit: Select the period of time that you need to send the log: Hourly, Daily, or Weekly. To disable sending of logs, select Never.

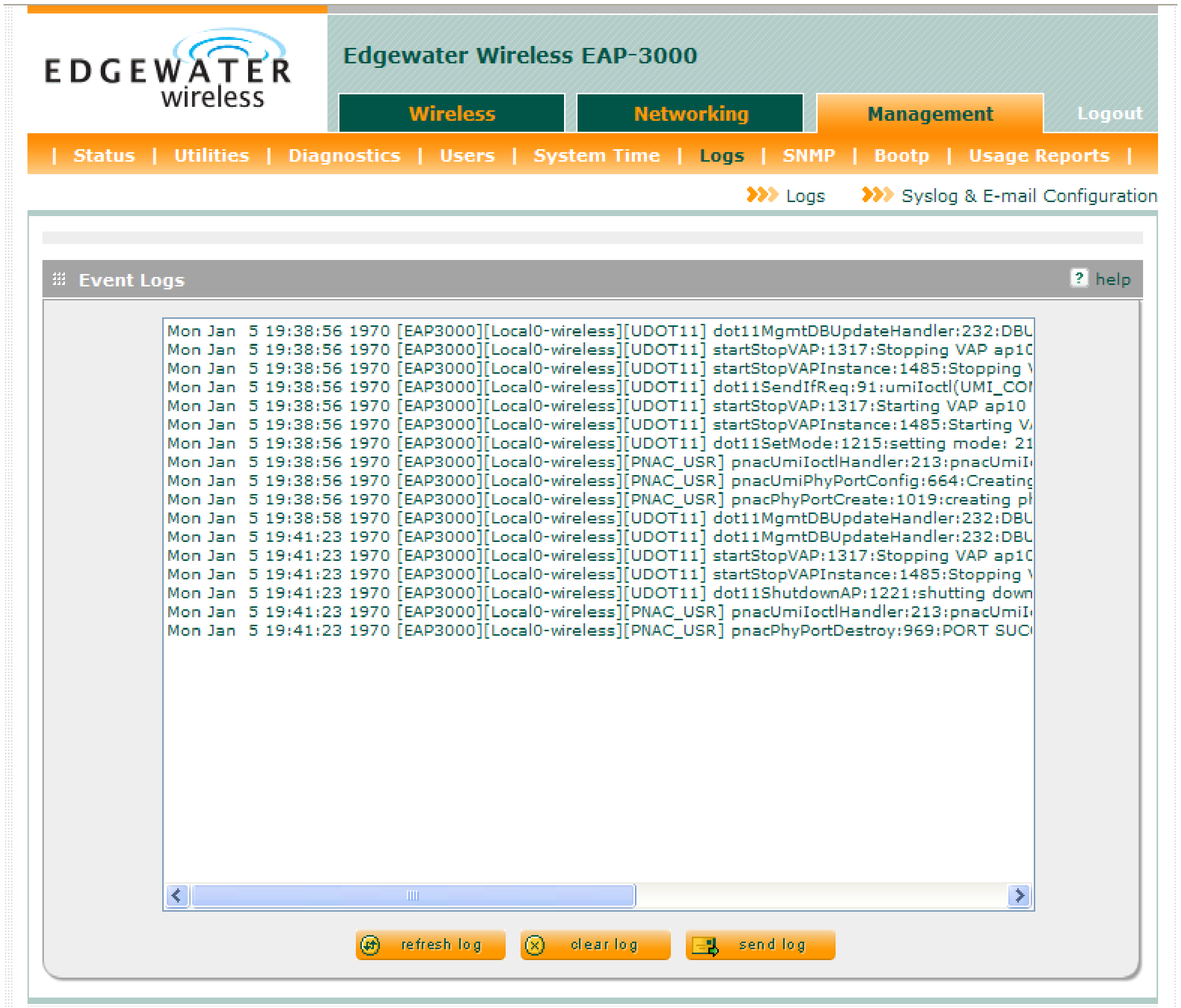
This option is useful when you do not want to receive logs by e-mail, but want to keep e-mail options configured so that you can use the Send Log function from the View Logs page.

Day: If Weekly is selected, choose the day of the week.

Time: Select the time when logs should be sent.

Click Apply to save your changes.

Click Reset to revert to the previous settings.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
Logs
Syslog & E-mail Configuration
Event Logs
help
refresh log
clear log
send log

```
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] dot11MgmtDBUpdateHandler:232:DBU
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] startStopVAP:1317:Stopping VAP ap10
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] startStopVAPInstance:1485:Stopping V
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] dot11SendIfReq:91:umiIoctl(UMI_CON
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] startStopVAP:1317:Starting VAP ap10
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] startStopVAPInstance:1485:Starting V
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][UDOT11] dot11SetMode:1215:setting mode: 21
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][PNAC_USR] pnacUmiIoctlHandler:213:pnacUmiI
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][PNAC_USR] pnacUmiPhyPortConfig:664:Creating
Mon Jan  5 19:38:56 1970 [EAP3000][Local0-wireless][PNAC_USR] pnacPhyPortCreate:1019:creating ph
Mon Jan  5 19:38:58 1970 [EAP3000][Local0-wireless][UDOT11] dot11MgmtDBUpdateHandler:232:DBU
Mon Jan  5 19:41:23 1970 [EAP3000][Local0-wireless][UDOT11] dot11MgmtDBUpdateHandler:232:DBU
Mon Jan  5 19:41:23 1970 [EAP3000][Local0-wireless][UDOT11] startStopVAP:1317:Stopping VAP ap10
Mon Jan  5 19:41:23 1970 [EAP3000][Local0-wireless][UDOT11] startStopVAPInstance:1485:Stopping V
Mon Jan  5 19:41:23 1970 [EAP3000][Local0-wireless][UDOT11] dot11ShutdownAP:1221:shutting down
Mon Jan  5 19:41:23 1970 [EAP3000][Local0-wireless][PNAC_USR] pnacUmiIoctlHandler:213:pnacUmiI
Mon Jan  5 19:41:23 1970 [EAP3000][Local0-wireless][PNAC_USR] pnacPhyPortDestroy:969:PORT SUC
```

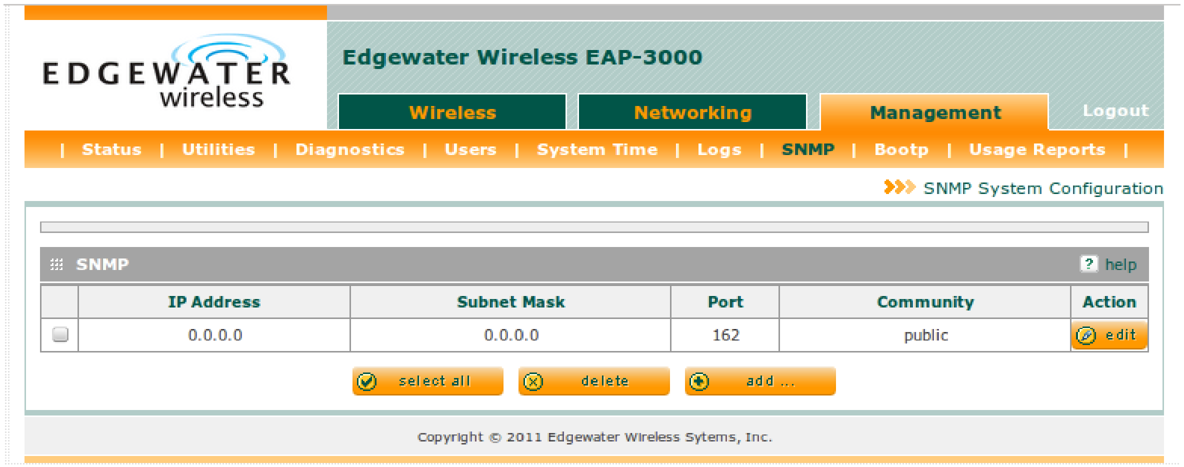
5.7 Management -> Logs -> View Event Log

Event Logs

This section displays the logs from various events that were configured to display in event log.

Click refresh log to refresh the log display area.
Click clear log to clear the log display area.
Click send log to send log to the configured email address.

5.8 Management -> SNMP


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
SNMP System Configuration
SNMP
help
select all
delete
add ...
Copyright © 2011 Edgewater Wireless Sytems, Inc.

	IP Address	Subnet Mask	Port	Community	Action
□	0.0.0.0	0.0.0.0	162	public	edit

SNMP

Simple Network Management Protocol (SNMP) lets you monitor and manage your device from an SNMP Manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. This device supports the SNMPv2c protocol version and can send traps to a specified community.

IP Address: This field is used to specify either a specific IP or a network address. When a network address is specified, all systems in that network have SNMP management access to the device. However, no traps can be sent to any of the machines, since broadcasting of traps is not supported. If traps are to be sent to a specific machine, then this field requires the specific IP address of that machine.

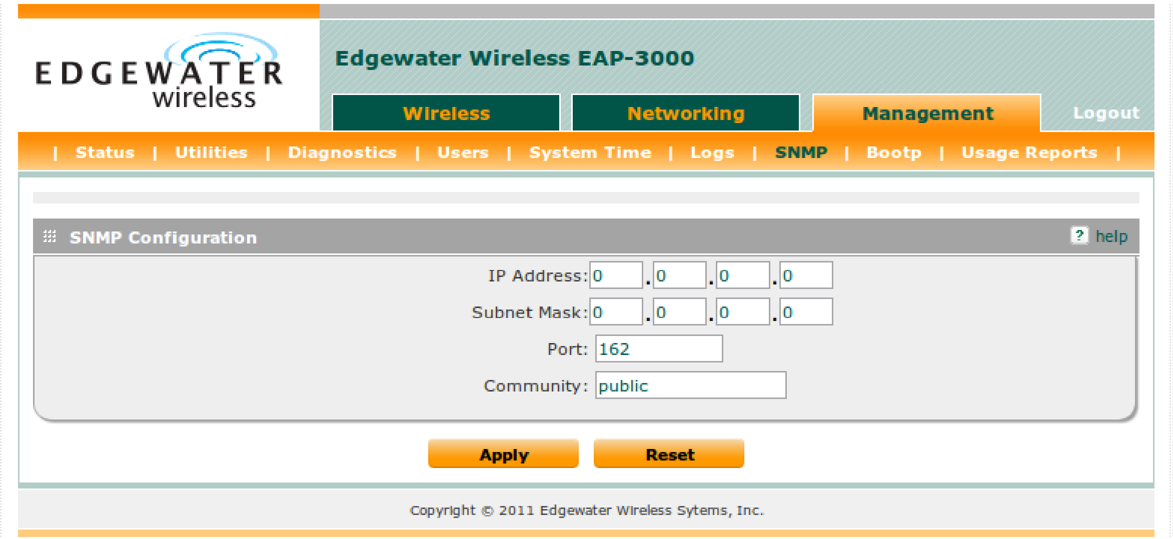
Subnet Mask: This field is used in conjunction with the 'IP Address' field to specify the network to which SNMP management access is restricted.

Port: This field is meant to specify the port of the SNMP agent to which traps will be sent. It does not impose any restrictions on SNMP manager access to the device.

Community: This field specifies the community to which the agent belongs, as well as the community to which traps will be sent. Most agents are configured to listen for traps in the Public community.

Action: The edit button links to the SNMP configuration page.

5.9 Management -> SNMP->edit



EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
SNMP Configuration
help
Apply
Reset
Copyright © 2011 Edgewater Wireless Sytems, Inc.

IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Port: 162
Community: public

SNMP Configuration
This table lets you configure and control the SNMP agents which can access the box and also the agents which can receive trap messages. The following fields are present in the table:
The following are present in the table:

IP Address: This field can be used to specify either a specific IP or a network address. When a network address is specified, all systems in that network have SNMP management access to the device. However, no traps can be sent to any of the machines, since broadcasting of traps is not supported. If traps are to be sent to a specific machine, then this field requires the specific IP address of that machine.

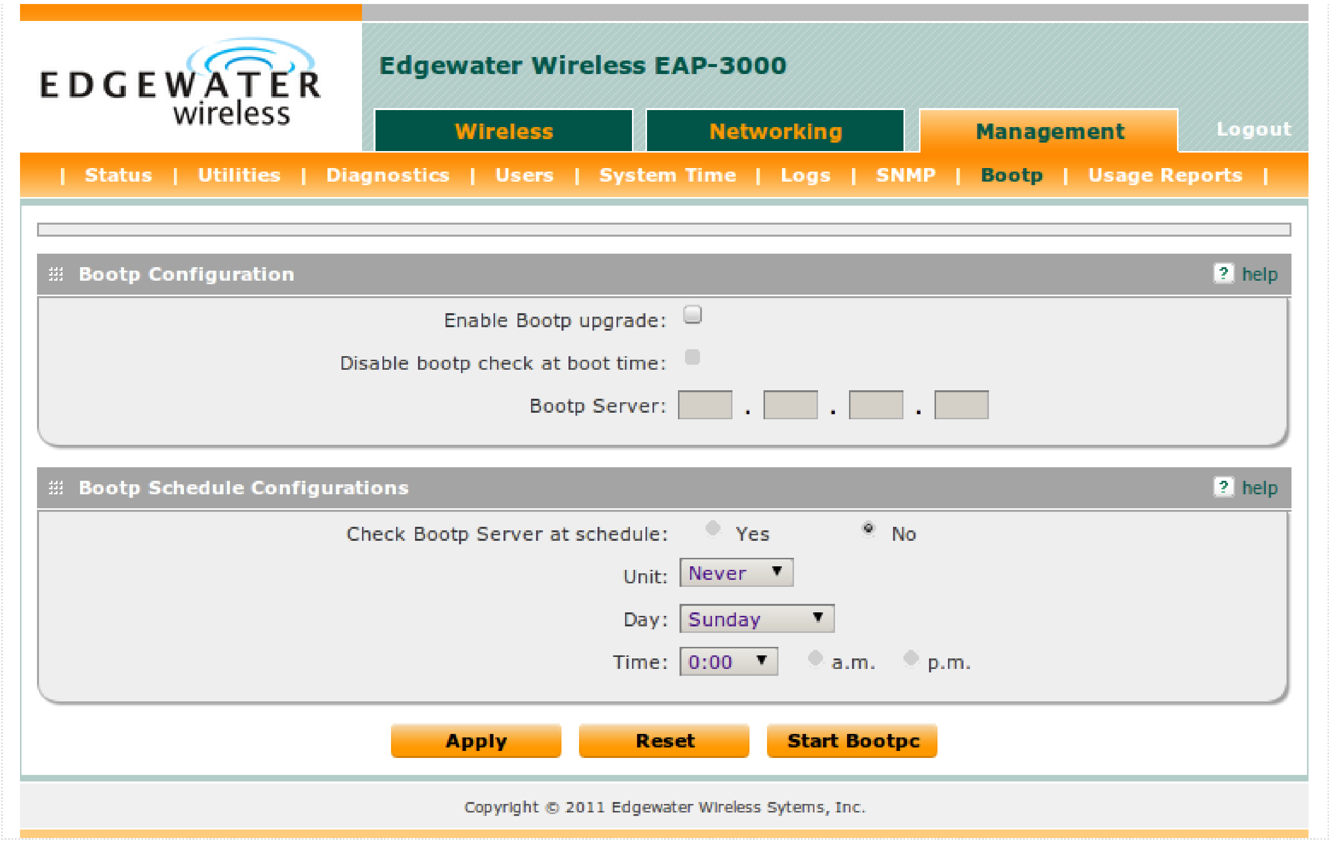
Subnet Mask: This field is used in conjunction with the 'IP Address' field to specify the network to which SNMP management access is restricted.

Port: This field is meant to specify the port of the SNMP agent to which traps will be sent. It does not impose any restrictions on SNMP manager access to the device.

Community: This field specifies the community to which the agent belongs, as well as the community to which traps will be sent. Most agents are configured to listen for traps in the Public community.

Click on Add to create this new configuration.
Click on Edit to modify or change the selected configuration.
Select All: Select all the entries in the table.
Delete: Delete selected entries from the table.
Note: Note: Global access to the device is allowed in either of the two cases:
a. The 'IP Address' /'Subnet Mask' fields are configured as 0.0.0.0/0.0.0.0
b. No entry exists in the configuration table.
Please configure a specific host/network if you need to restrict access to
the device.

5.10 Management -> Bootp


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
help
help
Apply
Reset
Start Bootpc
Copyright © 2011 Edgewater Wireless Sytems, Inc.

Bootp Configuration

Enable Bootp upgrade: □

Disable bootp check at boot time: □

Bootp Server: . . .

Bootp Schedule Configurations

Check Bootp Server at schedule: ○ Yes ● No

Unit: Never

Day: Sunday

Time: 0:00 ○ a.m. ○ p.m.

The Bootstrap Protocol (Bootp) allows a system to boot with the image(Firmware) stored on the Bootp server. EAP3000 uses Bootp protocol to get the firmware file name. This firmware filename on the Bootp server is compared against that currently running firmware version on the AP; an upgrade takes place only if the firmware version differs. The firmware image on the Bootp server is expected to be in a standard format: SYSNAME-X.Y.Z-B.img, where SYSNAME is the system name,configurable via the SNMP configuration page. X.Y.Z is the 3 digit firmware version number (major, minor, maintenance) and B is the build number

.

Bootp Configuration

Enable Bootp upgrade: Select this check box to enable the bootstrap protocol upgrade feature of this AP. Disabling this check box will prevent bootp operation on this device.

Disable bootp check at boot time: By default this AP does not check for an upgrade image in the bootp server during boot up (i.e. this check box is selected). To enable checking of firmware during bootup, de-select this box.

Bootp Server: This is the IPv4 address of the bootp server. If this is not specified, AP broadcasts the bootp requests on the LAN.

Bootp Schedule Configuration

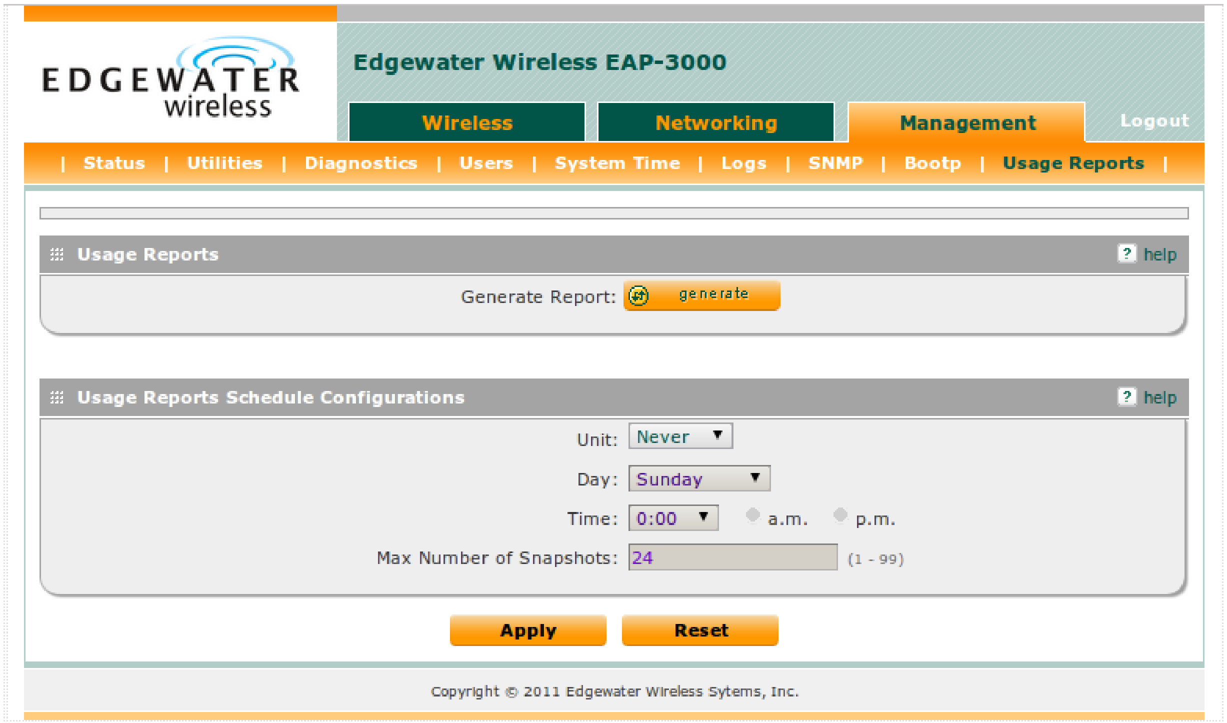
Enabling this feature allows this AP to check for firmware upgrades on the bootp host server at pre-defined intervals.

Unit: Select the frequency of checking with the bootp host: never, hourly, daily or weekly. To disable the bootp schedule, select Never.

Day: If the schedule is defined on a weekly basis, choose the day to perform the check.

Time: If the schedule is set to a weekly or daily check, choose the hour (and am/pm) to perform the check with the bootp host.

Click Apply to save your changes.
Click Reset to revert to the previous settings.
Click Start Bootpc to start the Bootp upgrade immediately.


EDGEWATER wireless
Edgewater Wireless EAP-3000
Wireless
Networking
Management
Logout
| Status | Utilities | Diagnostics | Users | System Time | Logs | SNMP | Bootp | Usage Reports |
? help
generate
? help
Apply
Reset

Usage Reports

Generate Report: generate

Usage Reports Schedule Configurations

Unit: Never

Day: Sunday

Time: 0:00 ○ a.m. ○ p.m.

Max Number of Snapshots: 24 (1 - 99)

Copyright © 2011 Edgewater Wireless Sytems, Inc.

5.11 Management -> Usage Reports

Usage reports are snapshots of relevant traffic statistics over a defined period of time, with a defined interval between updates.

Usage Reports

Generate Report: Click Generate to extract relevant statistics to a comma separated value (CSV) file available to download to the host or view using spreadsheet software.

Usage Report Schedule Configuration

Here you can set the frequency of intervals between collecting data for the usage report.

Unit: select the frequency of updating the report: never, hourly, daily or weekly. To disable sending usage report schedule, select Never.

Day: If the schedule is defined on a weekly basis, choose the day to update the report.

Time: If the schedule is set to a weekly or daily check, choose the hour (and am/pm) to update the report.

Max Number of Snapshots: select the maximum number of entries for the usage report before the report is rolled over and past information is lost. This allows you to limit the size of the CSV file stored as well as limit the system resources allocated to gathering reporting data.

Note: Schedule needs to be enable for the Generate to work. the minimum report update interval is 1 hour. If the AP was recently rebooted, you must wait at least 1 hour to observe non-zero data in the usage report.

Click Apply to save your changes.

Click Reset to revert to the previous settings.

Appendix A

Channel Identifier	**Center Frequency (MHz)**	**Regulatory Domains**					
		Americas		**EMEA**		**Japan**	
		CCK	**OFDM**	**CCK**	**OFDM**	**CCK**	**OFDM**
1	2412	X	X	X	X	X	X
2	2417	X	X	X	X	X	X
3	2422	X	X	X	X	X	X
4	2427	X	X	X	X	X	X
5	2432	X	X	X	X	X	X
6	2437	X	X	X	X	X	X
7	2442	X	X	X	X	X	X
8	2447	X	X	X	X	X	X
9	2452	X	X	X	X	X	X
10	2457	X	X	X	X	X	X
11	2462	X	X	X	X	X	X
12	2467	-	-	X	X	X	X
13	2472	-	-	X	X	X	X
14	2484	-	-	-	-	X	-

Note: Mexico is a part of the Americas regulatory domain but channels 1 – 8 are reserved for indoor use only while channels 9 through 11 may be used for both indoor and outdoor use.

Appendix B: Regulatory Statement

This device must be professionally installed. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter within a host device, except as described in this user manual.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter (10165A-EAP3030) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (10165A-EAP3030) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

This equipment is certified to be used with the following types of antennas:

- Indoor Unit 2.4 GHz Pedal antenna, Alpha APA-M04 7 dBi
- Indoor Unit 2.4 GHz Patch antenna, ALLNET 2.4 GHz 10 dBi Flat Patch
- Indoor Unit 2.4 GHz Whip antenna, Nearson S151AH-2450 5 dBi
- Outdoor Unit 2.4 GHz Rod antennas: OD24M-9 (9 dBi), OD24M-7 (7 dBi) and OD24M-5 (5 dBi)
- Outdoor Unit 2.4 GHz Sector antenna, Laird Technologies SA24-120-16-WB 16 dBi
- Indoor/outdoor 5 GHz dipole antenna, Aristotle RFA-25-C2M2