

# SkyPilot SkyExtender DualBand

Installation and Setup Guide



FCC Radio Frequency Interference Statement  
SkyExtender DualBand FCC Number: RV7-DBE1010

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 90 of the FCC Rules. These limits are designed to provide reasonable protection against interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed, and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment has been certified to comply with the limits for a class B computing device, pursuant to FCC Rules. In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

#### Maximum Permissible Exposure

In order to meet Industry Canada, FCC and other regulatory requirements for RF Exposure, the SkyGateway and SkyExtender units must be located a minimum of 21 cm (8 inches) from all persons. This distance is determined based upon the aforementioned 1 mW/cm<sup>2</sup> limit, measured data, and the following far-field peak power density equation:

$$d = \frac{0.282 \left[ 10^{((P+G)/20)} \right]}{\sqrt{S}}$$

where:  $d$  = MPE distance in cm

$P$  = Power in dBm (peak)

$G$  = Antenna Gain in dBi

$S$  = Power Density Limit in mW/cm<sup>2</sup> (1 mW/cm<sup>2</sup>)

Certified laboratory measurements indicate that the FCC's Power Density Limit of 1 mW/cm<sup>2</sup> is met at a distance of much less than 20 cm (8 inches). However the minimum distance for fixed or mobile transmitters is 20 cm even if calculations indicate the MPE distance is much less.

#### FCC 15.203 statement

Because this device uses standard RF connectors for the external removable antennas, professional installation is required.

#### IC RSS-210 statement

This device has been designed to operate with the external antennas for the 2.4 GHz band listed below, and having a maximum gain of 7.4 dBi. Antennas not included in this list or having a gain greater than 7.4 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

#### Approved antennas:

| Manufacturer | Model     |
|--------------|-----------|
| Comet        | SF245     |
| Comet        | SF245+12  |
| Comet        | SF245+12x |

# Contents

|   |    |
|---|----|
| About This Guide  | 5  |
| 1 Overview  | 7  |
| 2 Your SkyExtender DualBand kit                         | 9  |
| 3 Installing SkyExtender DualBand                       | 11 |
| 4 Configuring SkyExtender DualBand                      | 15 |
| 5 Configuration Tool Reference                          | 45 |
| A Connecting to the Access Point Command-Line Interface | 73 |
| B Manually Updating Access Point Software               | 79 |
| C WLAN Configuration Types                              | 81 |





## About This Guide

This guide provides directions for installing and setting up a SkyPilot™ SkyExtender™ DualBand, which can provide access point services for users of 802.1x wireless (Wi-Fi) networks.

This guide assumes administrator-level knowledge of IP networks and a familiarity with configuring wireless devices.



## Overview

SkyExtender DualBand is a dual-radio solution that combines SkyPilot's long-range, high-capacity 5 GHz mesh backhaul with a high-powered 802.11b/g access point that lets service providers and municipalities offer standard Wi-Fi services over great distances, for targeted hot zones or dense, ubiquitous coverage patterns.

### Features and benefits

With the ability to create multiple WLANs (wireless local area networks), each with its own VLAN and security policy, the SkyExtender DualBand can support several business models with a single service installation.

SkyExtender DualBand provides a unique opportunity for WISPs looking to combine scalable Wi-Fi capacity with the seamless coverage of a wireless mesh network.

SkyExtender DualBand nodes on a wireless mesh network offer a basis for multi-service networks capable of providing end-to-end security and quality of service for a variety of bandwidth-hungry applications and services, including VoIP and video surveillance solutions.

The auto-discovery and rapid provisioning features of a SkyPilot wireless mesh network can greatly reduce deployment and maintenance costs. Multiple topology options and network scalability create intriguing options for rapidly growing a metro Wi-Fi customer base.

## Default access point configuration

The SkyExtender DualBand access point is set up to provide Wi-Fi access right out of the box. The access point includes a preconfigured WLAN with the SSID (service set identifier) *SkyPilotDualBand*, providing WPA-PSK (Wi-Fi protected access – pre-shared key) protection. Users attempting to connect to the *SkyPilotDualBand* WLAN must provide a password (*publicpublic* by default).

The default configuration is provided for initial management and configuration of the SkyExtender DualBand access point via a wireless connection. You should always create an access point configuration before testing the device or making it available to customers.

**NOTE** A wireless network protected by WPA-PSK is vulnerable. To provide a more secure level of protection, configure the WLAN for WPA authentication in which each user is authenticated separately.



## Your SkyExtender DualBand Kit

The SkyPilot SkyExtender DualBand™ kit provides everything you need to install the device and configure it as both an extender for your wireless mesh network and an 802.11b/g Wi-Fi access point.

### Contents of kit

The SkyPilot SkyExtender DualBand kit includes:

- A SkyPilot SkyExtender DualBand.  
The SkyExtender DualBand integrates a SkyExtender with a high-powered Wi-Fi 802.11b/g access point.
- A pair of 2.4 GHz antennas.
- A PoE (Power over Ethernet) adapter for powering the SkyExtender DualBand.
- A custom console cable (RJ-45 to DB-9) for making a serial connection with the SkyExtender component of the SkyExtender DualBand.

### What you need for installation

Before starting installation, you need the following:

- A computer connected to the same network as the SkyExtender DualBand.
- A CAT-5 straight-through Ethernet cable for connecting the SkyExtender DualBand to a power source.
- MAC addresses for the SkyExtender DualBand and the WLANs you set up for the access point.

Each SkyExtender DualBand has 32 MAC addresses assigned to it. The MAC address of the SkyExtender's 5 GHz radio (as seen from the SkyGateway™) is printed on the label affixed to the base of the SkyExtender DualBand. The MAC address for the access point is 1 less than the MAC address of the SkyExtender's 5 GHz radio.

The MAC addresses reserved for use by WLAN SSIDs (basic SSIDs, or BSSIDs) begin with the MAC address on the label at the bottom of the SkyExtender DualBand minus-31.

MAC addresses use a base-16 (hexadecimal) system in which the letters A–F represent numbers 10–15. For example, if the MAC address of the SkyExtender DualBand is 00 0A DB 01 31 9F, the reserved addresses start with the MAC address 00 0A DB 01 31 80.

- Setup information for the access point:
  - A (case-sensitive) wireless SSID for each virtual WLAN Wi-Fi network
  - A unique IP address for the management of the access point if it's not connected to a DHCP server
  - A default gateway and subnet mask for the management network if the access point is not on the same subnet as your PC

**NOTE** Plan on configuring the SkyExtender DualBand before mounting it. Some steps, such as those requiring a serial cable, are easier if the access point is more accessible.

## Getting help

For technical assistance during the beta release period, contact SkyPilot support by logging in to customer support at [www.skypilot.com](http://www.skypilot.com).

## Installing SkyExtender DualBand

This chapter provides instructions for planning and performing the physical installation of the SkyExtender DualBand.

### Planning your installation

When choosing a site for the SkyExtender DualBand, consider the radio frequency (RF) environment and the physical layout of the area.

Trees, buildings, and hills can impede a wireless signal. When assessing a site, examine the overall topology of the wireless path for possible obstructions, existing or planned. The radio environment is dynamic and can deteriorate over time as structures appear or are relocated.

Plan on testing potential sites to determine the suitability of the link topology for target applications. Interference on your desired frequency results in overlapping signals, causing outages or intermittent drops in throughput.

Once you've identified a potential site, use a topographic map or path profile software to ensure that terrain or obstacles will not interfere with the links.

The site survey process should be an ongoing one. To verify that a site is relatively interference-free, make site audits every 6 to 12 months, scheduling regular maintenance visits to coincide with the site audits.

### Mounting and cabling

The section provides instructions for physically installing the SkyExtender DualBand.

**1 Mount the SkyExtender DualBand.**

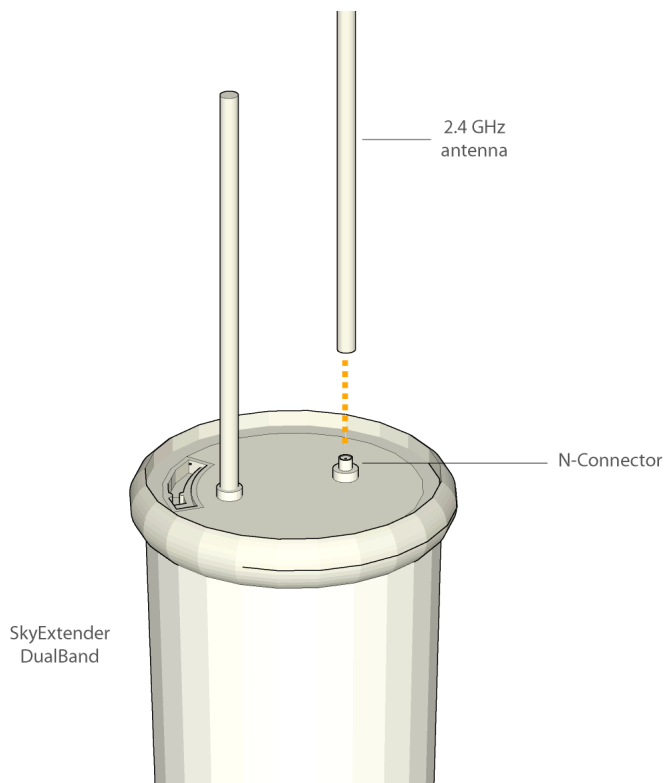
Follow the instructions provided in the *SkyPilot SkyGateway/SkyExtender Installation Guide*.

Make sure that you allow enough clearance for the 2.4 GHz antennas you'll attach to the bottom of the SkyExtender.

**2 Connect the 2.4 GHz antennas.**

The access point requires attachment of the two 2.4 GHz antennas included with the device. Screw the antennas onto the standard N connectors on the underside of the SkyExtender DualBand.

Figure 1. Attaching the antennas

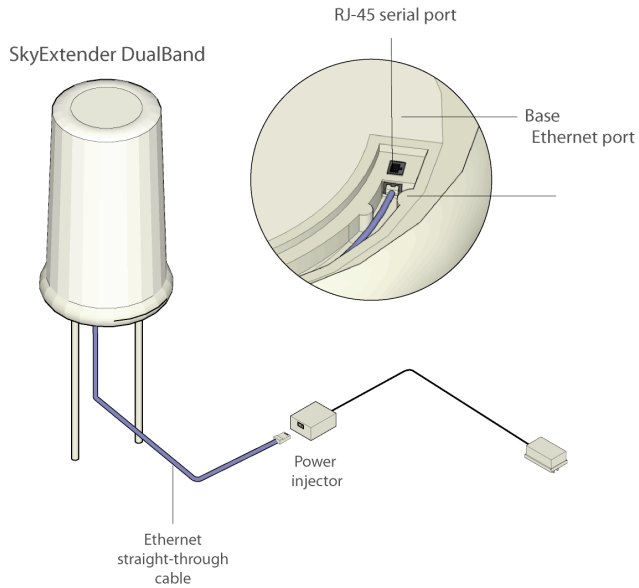


### 3 Connect the SkyExtender DualBand to the power supply.

Connect the Ethernet straight-through cable (provided) between the power injector and the Ethernet port on the base of the SkyExtender DualBand.

Plug the AC adapter into the power injector.

Figure 2. Providing power to the SkyExtender DualBand



**NOTE** The external Ethernet port on the SkyExtender DualBand is limited to providing power to the device; it cannot handle data traffic. Do not attempt to connect the power injector to a network switch or other device.

## Powering on

When power is supplied to the SkyExtender DualBand, it starts a routine power-on sequence that you can monitor by observing the pair of LED lights on the underside of the device.

While the device is initializing and searching for a GPS signal, both LED lights blink four times in a repeating cycle.

When the Link LED turns steady green and the Activity LED is off, the SkyExtender DualBand is initialized and listening for hello signals from other devices. When both LEDs are steady, the SkyExtender DualBand is successfully connected to the wireless network.

The sequence takes about 15 minutes while waiting to acquire a GPS signal. (The SkyExtender DualBand must have access to a GPS signal to complete the sequence.)

## Configuring SkyExtender DualBand

After installing the SkyExtender DualBand, you need to provide both the SkyExtender and access point components of the device with configuration information that they need for network operations.

This chapter tells you how to use the SkyPilot EMS software to configure the SkyExtender DualBand for both mesh networking and Wi-Fi operation.

### Before you begin

Before starting configuration, make sure the SkyExtender DualBand is powered on and capable of receiving a signal from a SkyGateway or SkyExtender.

Additionally, make sure the EMS software is installed (both on a central server and a client) and set up for configuring SkyPilot devices.

After getting a configuration from the provisioning server, the SkyExtender DualBand will establish a link to the SkyGateway (or to another SkyExtender) and use DHCP to retrieve an IP address and instructions for downloading configuration information stored on the server.

Detailed procedures for using EMS software are provided in the *SkyPilot Network Administration Guide* available on the *SkyPilot Network Software* CD or the SkyPilot website at [www.skypilot.com](http://www.skypilot.com).

### *Automatic configuration versus manual configuration*

The SkyExtender and access point contained in the SkyExtender require network configurations to operate on the wireless mesh network. SkyPilot gives you a

choice of two modes for provisioning devices with configurations: **automatic** or **manual**.

Automatic provisioning requires the use of SkyPilot EMS software to create configurations that an unattended central server can distribute to devices on the wireless mesh network. Although automatic provisioning requires more setup time than manual provisioning, it greatly simplifies the administration of a growing network.

Usually performed in the field, manual provisioning permits the configuration of only a single device at a time, creating the minimum settings required for a wireless link and storing them in the device's flash (nonvolatile) memory.

For more information on provisioning modes, see *Getting Started with the SkyPilot Network*, provided on the *SkyPilot Network Software CD*.

## Choosing a WLAN configuration

Before starting configuration, decide on the type of Wi-Fi network you want to configure at the access point location.

Most WLAN deployments use one of two common types of WLAN configuration:

- An open (unprotected) Wi-Fi network, which does not authenticate users or which depends on authentication by a backend system such as a captive portal
- A Wi-Fi protected access (WPA) network, which uses standards-based client authentication and encryption

**NOTE** A WPA network requires a Radius server for authenticating users; see the next section for information on setting up the server.

As you follow the steps for configuring the SkyExtender DualBand, the procedures will direct you to the appropriate section depending on your type of configuration.



## Setting up a Radius server for authenticating users

If you plan configure your SkyExtender DualBand access point for WPA, you must first configure a Radius server with the following:

- The IP address and shared secret of the SkyExtender DualBand access point.
- EAP-PEAP/MSCHAPv2 and EAP-TTLS/PAP or MSCHAPv2 (not EAP-TLS) suitable for WPA. Your Radius supplier can provide instructions.
- A Users database with user names and passwords. You may also need to identify a proxy Radius if you're delegating some domains to other service providers.

## Preparing software images

The next steps for automatic configuration of the SkyExtender DualBand start with preparing the software images, as described in this section, and continue with the procedures described in the remaining sections of this chapter. For information related to manual configuration, turn to Chapter 5, "Using the Access Point Configuration Tool."

Before you use the EMS software to set up automatic configuration of the SkyExtender DualBand, make sure the most current software images are available to the EMS client software. (You can identify software images by the prefixes and version numbers in their names—for example, *SkyGate.2.0.14.bin*, *SkyConn.2.0.14.bin*, *SkyExt.2.0.14.bin*, and *SkyExtDB.2.0.14.bin*.)

To provide the EMS software with access to the software images, copy the images to the directory `/var/ftp/pub/images/` on the provisioning server.

## Starting the EMS client

After confirming that the current software images are in the appropriate directory, you can run the EMS client software and start setting up automatic configuration of the SkyExtender DualBand.

You'll run the EMS client software from a computer on the wireless mesh network and use SkyProvision™ to set up a node profile for the SkyExtender DualBand.

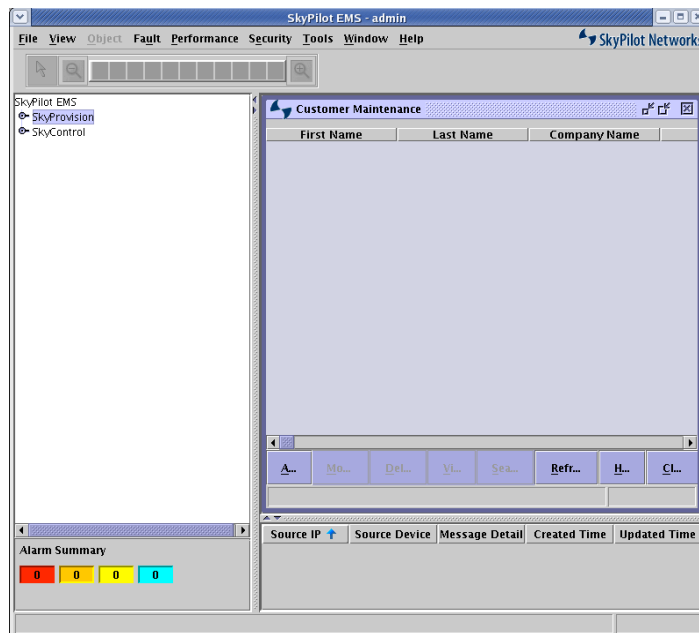
To start the EMS client software:

- 1 From the client computer, open the `C:\SkyPilot\EMS\bin\` directory.
- 2 Double-click the `startsemsclient.bat` application icon.
- 3 At the prompt, enter the user name and password.

The default user name is `admin`; the default password is `admin`.

The application starts, displaying the main menu.

Figure 3. EMS client window



The taskbar on the left side of the window expands to show options for using the EMS applications: SkyProvision and SkyControl™.

## Adding software images

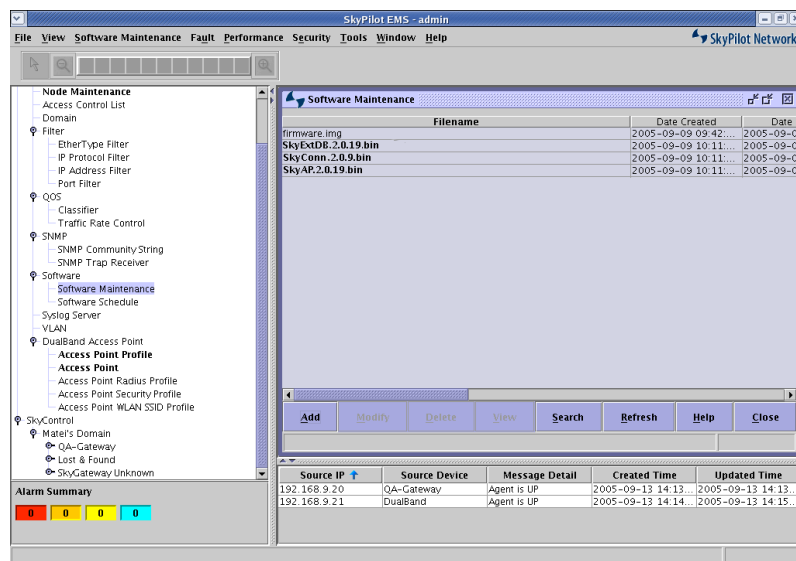
Using the SkyProvision application, you can view the software images that the provisioning server will use to configure the new device and then add any as needed.

### 1 Open the SkyProvision Software Maintenance pane.

In the taskbar, double-click *SkyProvision* > *Software* > *Software Maintenance*—that is, click the expansion icon next to *SkyProvision* to view all the application options, click the expansion icon next to the *Software* option, and then double-click *Software Maintenance* under that option.

The Software Maintenance pane appears, listing currently loaded software images.

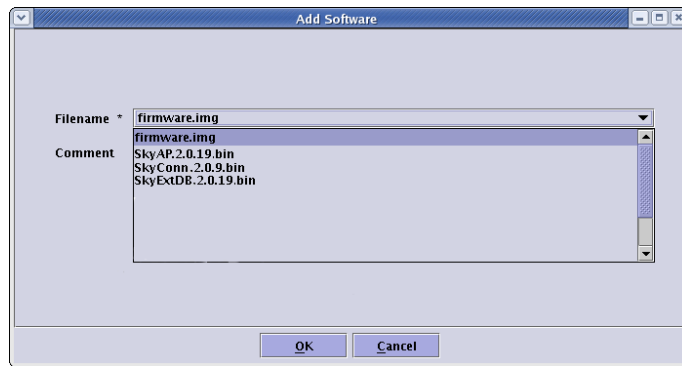
Figure 4. Software Maintenance list



### 2 If necessary, add one or more software images.

Click the **Add** button below the Software Maintenance list to open the Add Software dialog box.

Figure 5. Add Software dialog box



Select a software image from the list and click *OK*.

The selected image now appears in the Software Maintenance list.

Repeat step 2 to add additional software images.

## Specifying a domain

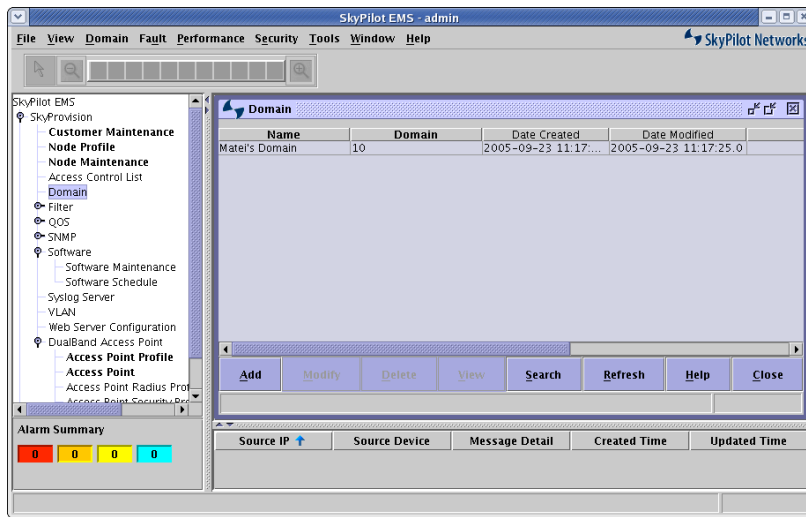
After adding any software images as necessary, you need to specify a domain for the SkyExtender DualBand that's consistent with the domain assigned to the SkyGateway operating as a hub for the wireless mesh network.

### 1 Open the SkyProvision Domain pane.

In the taskbar, double-click *SkyProvision > Domain*.

The Domain pane appears, listing currently active domains.

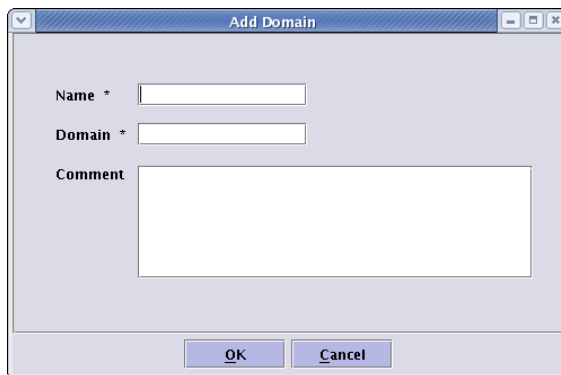
Figure 6. Domain list



## 2 Add a domain.

Click the *Add* button below the Domain list to open the Add Domain dialog box.

Figure 7. Add Domain dialog box



Enter a domain name and number, and then click *OK*. (The *Comment* field is optional.)

The domain now appears in the Domain list.

## Creating a node profile

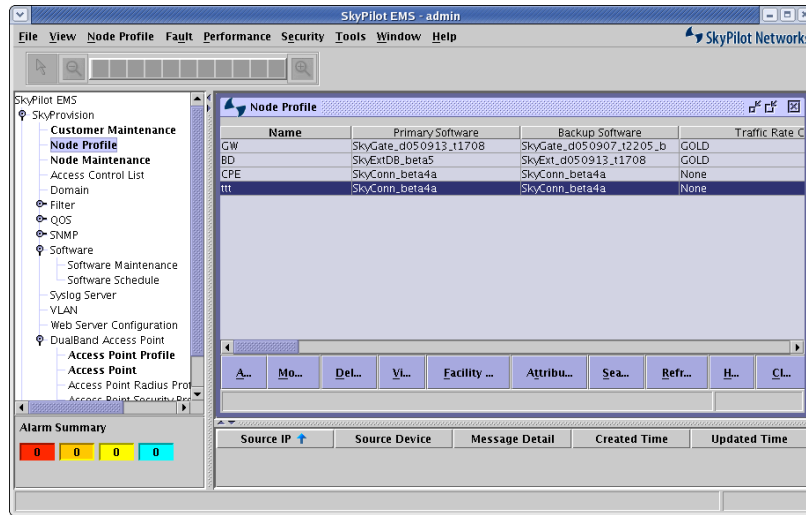
After confirming the availability of software images and the correct domain, your next step is to create a node profile for the SkyExtender DualBand.

### 1 Open the Node Profile pane.

In the taskbar, double-click *SkyProvision* > *Node Profile*.

The Node Profile pane appears, listing existing node profiles.

Figure 8. Node Profile list



### 2 Add a new node profile.

Click the *Add* button below the Node Profile list to display the Add Node Profile dialog box. (In this dialog box and similar ones, asterisks identify required fields.)

Figure 9. Add Node Profile dialog box

The 'Add Node Profile' dialog box is a standard Windows-style window with a title bar. It contains a list of configuration options on the left side, each with a corresponding input field or dropdown menu. The options are: Name (text box), Primary Software (dropdown menu with 'SkyConn\_beta4a' selected and a 'Swap' button), Backup Software (dropdown menu with 'SkyConn\_beta4a' selected), Traffic Rate Control (dropdown menu with 'None' selected and a 'Detail' button), Domain (dropdown menu with 'All' selected), Timezone (dropdown menu with 'American Samoa, Midway Is., Niue Is., Samoainsert(GMT-11)' selected), Frequency Region (dropdown menu with 'Default' selected), Frequency (dropdown menu with '5725' selected), Frequency Dwell Time (text box), Ethernet (dropdown menu with 'Enable' selected), SNMP (dropdown menu with 'Read-write' selected), Password (text box), Re-Enter Password (text box), Telnet Timeout (text box), Filter (dropdown menu with 'Disable' selected), EtherType Filter (dropdown menu with 'Allow' selected), IP Protocol Filter (dropdown menu with 'Allow' selected), and IP Address Destination (dropdown menu with 'Allow' selected). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Use the provided fields and pull-down menus to specify general operating parameters for the profile, including a profile name, software images, domain, Ethernet status, and operating frequency.

Click *OK* to save the settings.

The new node profile now appears in the Node Profile list.

## Creating a node

After creating the node profile, you can specify the SkyExtender DualBand as a new node on the wireless mesh network.

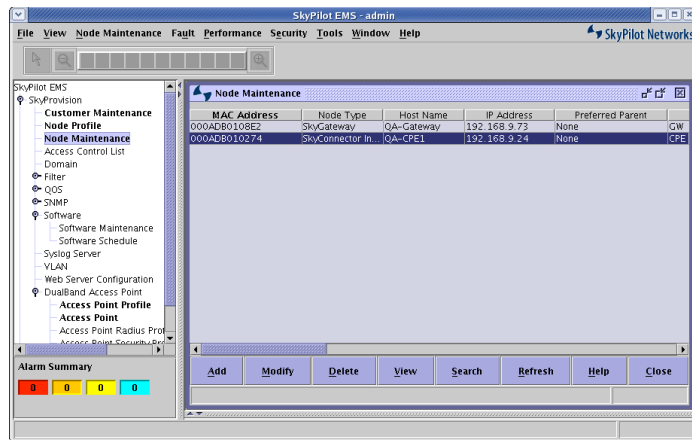
When you create a node and identify it as a SkyExtender DualBand, access point options become available in the EMS client taskbar.

### 1 Open the Node Maintenance pane.

In the taskbar, double-click *SkyProvision > Node Maintenance*.

The Node Maintenance pane appears, listing existing nodes by MAC address and node type. Figure 10 shows an example.

Figure 10. Node Maintenance list



**2** Add a new node.

Click the *Add* button below the Node Maintenance list to display the Add Node dialog box. (Asterisks identify required fields.)



Figure 11. Add Node dialog box

The 'Add Node' dialog box is a standard Windows-style window with a title bar and three control buttons (minimize, maximize, close). The main area contains the following fields and controls:

- MAC Address\***: A field with six boxes separated by colons, intended for entering a MAC address.
- Node Type\***: A dropdown menu currently showing 'SkyConnector Indoor'. A list of options is visible: SkyConnector Indoor, SkyConnector Outdoor, SkyExtender, SkyGateway, and SkyExtender DualBand.
- Host Name**: A text input field.
- IP Address\***: A text input field.
- Preferred Parent**: A sub-dialog box containing:
  - MAC Address**: A dropdown menu set to 'None'.
  - Host Name**: A text input field.
- Node Profile\***: A dropdown menu set to 'None', with a 'Detail' button to its right.
- Address 1**: A text input field.
- Address 2**: A text input field.
- City**: A text input field.
- State/Province**: A text input field.
- Postal Code**: A text input field.
- Country**: A dropdown menu set to 'None', with a 'Detail' button to its right.
- Customer**: A dropdown menu set to 'None', with a 'Detail' button to its right.
- Comment**: A large text area for additional information.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Use the *MAC Address* fields to enter the SkyExtender DualBand MAC address, which is printed on a label affixed to the base of the device.

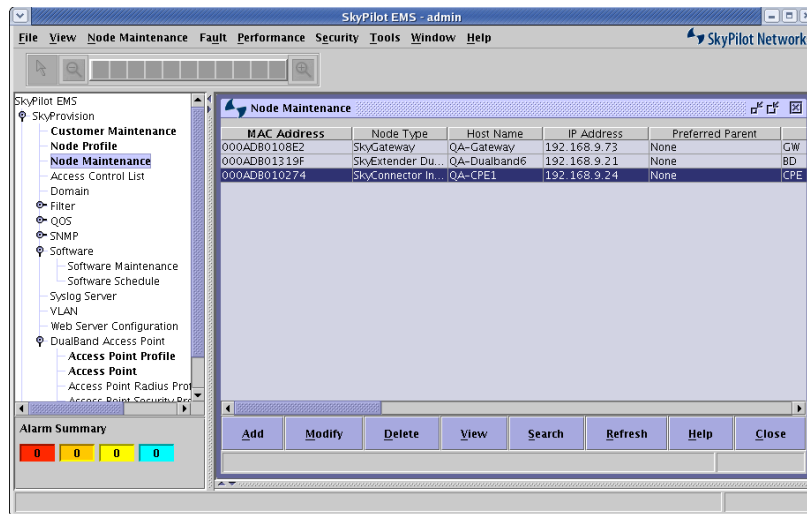
From the *Node Type* pull-down menu, choose *SkyExtender DualBand*.

From the *Node Profile* pull-down menu, choose a node profile.

Add any other information you want to include in the node description and click *OK*.

The new node now appears in the Node Maintenance list. Figure 12 shows an example.

Figure 12. Node Maintenance list with SkyExtender DualBand node



Because you specified the new node as a SkyExtender DualBand, access point options for the device are now available in the taskbar.

See the *SkyPilot Network Administration Guide* provided on the *SkyPilot Networks Software CD* for more information on using the EMS application to configure SkyExtender DualBand for network operations on a SkyPilot wireless mesh network.

## Creating an access point security profile

Now you can start creating profiles for the access point component of the SkyExtender DualBand, beginning with a security profile for Telnet communications with the access point.

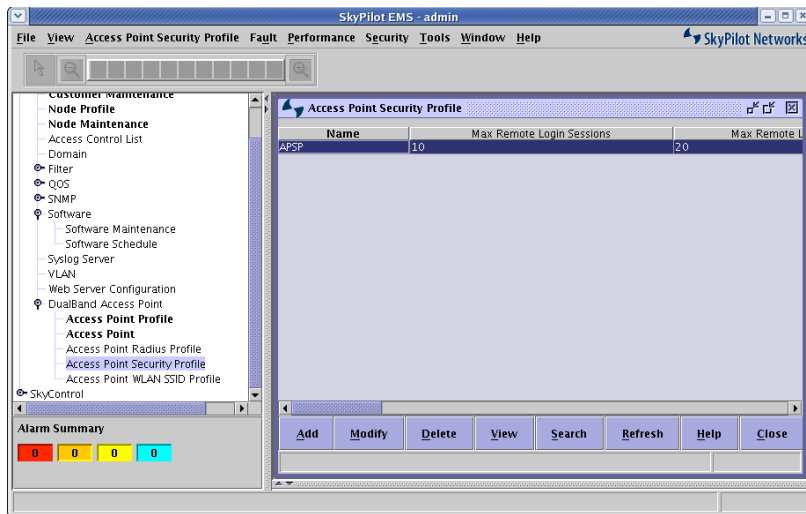
In this procedure, you'll create a security profile for remote communications with the access point via Telnet.

### 1 View the access point security profiles.

In the taskbar, double-click *SkyProvision > DualBand Access Point > Access Point Security Profile*.

The information pane lists any existing access point security profiles.

Figure 13. Access Point Security Profile list



If the pane lists a profile that you want to use, go to step 3.

If you need to create a profile, go to step 2.

## 2 Add a new access point security profile.

Click the **Add** button below the profile list to display the Add Access Point Security Profile dialog box. (Asterisks identify required fields.)

Figure 14. Add Access Point Security Profile dialog box

The dialog box titled "Add Access Point Security Profile" contains the following fields and options:

- Name \*
- Max Remote Login Sessions
- Max Remote Login Timeout
- Telnet Server \* (Dropdown menu: Enable)
- Admin Telnet Password
- Confirm Password
- Peer to Peer (Dropdown menu: Disable)
- Management From Wireless Clients \* (Dropdown menu: Enable)
- Syslog \* (Dropdown menu: Disable)
- Syslog Server (IP address field: . . . .)
- Comment (Text area)
- OK button
- Cancel button

Use the provided fields and pull-down menus to give the profile a name, specify login session parameters, enable a Telnet server, and choose logging and management options.

Click **OK** to save the profile, which now appears in the list of access point security profiles.

Your next step depends on the type of Wi-Fi access you want to provide with the 1SkyExtender DualBand:

- If you're configuring the WLAN for WPA (Wi-Fi protected access), go to the next section.
- If you're configuring the WLAN for open (unprotected) access, you don't need a Radius profile to complete the access point configuration, so skip to the section "Creating a WLAN SSID profile for open configuration" on page 31.

## Creating a Radius profile (WPA)

If you're creating an access point configuration for WPA, you'll need a Radius profile, which provides information about the Radius server the WLAN will use to

authenticate users. If the profile does not exist, you must create it before you can complete configuration of the access point for WPA.

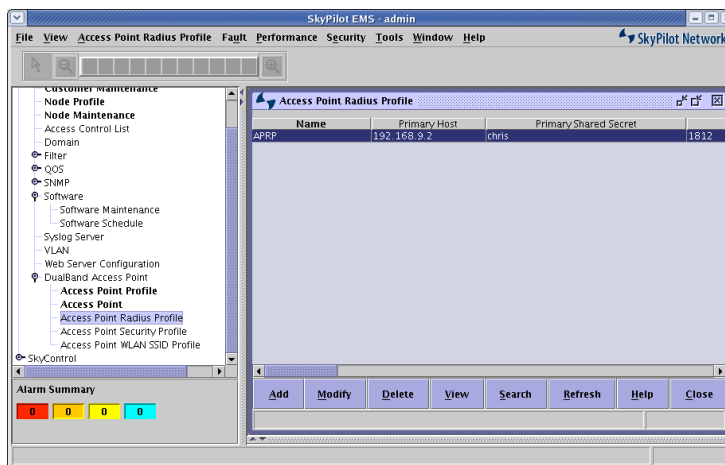
**NOTE** The configuration of a Radius server for authenticating Wi-Fi users varies, depending on the vendor solution, and is outside the scope of this document.

**1** View existing Radius profiles.

In the taskbar, double-click *SkyProvision* > *DualBand Access Point* > *Access Point Radius Profile*.

The information pane displays any existing access point Radius profiles. Figure 15 shows an example.

Figure 15. Access Point Radius Profile list



If the pane displays an access point Radius profile that you can use, skip to the section "Creating a WLAN SSID profile for WPA" on page 34.

If you need to create an access point Radius profile, continue with step 2.

**2** Add a new Radius profile.

Click the *Add* button below the profile list to display the Add Access Point Radius Profile dialog box. (Asterisks identify required fields.)

Figure 16. Add Access Point Radius Profile dialog box

The screenshot shows a dialog box titled "Add Access Point Radius Profile". It contains the following fields and values:

- Name \* (empty text box)
- Primary Host \* (IP address input fields: . . .)
- Primary Shared Secret \* (empty text box)
- Primary Authentication Port \* (1812)
- Primary Accounting Port \* (1813)
- Secondary Host (IP address input fields: . . .)
- Secondary Shared Secret (empty text box)
- Secondary Authentication Port \* (1812)
- Secondary Accounting Port \* (1813)
- Comment (empty text area)

At the bottom of the dialog box are "OK" and "Cancel" buttons.

Use the provided fields and pull-down menus to give the profile a name, enter the IP address of the primary host, provide a shared secret, and identify authentication and accounting ports.

In the *Primary Host* fields, enter the primary Radius server IP address.

Use the *Primary Shared Secret* field to supply the shared secret string specified in the Radius server's client configuration.

Modify the *Primary Authentication Port* and *Primary Accounting Port* assignments if they're different from the standard defaults.

If you have access to a secondary Radius server, fill in the *Secondary Host*, *Secondary Shared Secret*, *Secondary Authentication Port*, and *Secondary Accounting Port* fields for that server as well.

Click *OK* to save the profile.

The new profile now appears in the list of access point Radius profiles.

To continue configuring the WLAN for WPA, skip to the section "Creating a WLAN SSID profile for WPA" on page 34.

## Creating a WLAN SSID profile for open configuration

An open (unprotected) configuration allows anyone with Wi-Fi capability to connect to the wireless network via the SkyExtender DualBand access point.

An open configuration doesn't include any mechanism for authenticating users at the network layer, thereby making it easy for users to connect to the WLAN.

There are obvious security concerns for an open configuration. The network is more vulnerable to unauthorized access and malicious actions (including denial-of-service attacks) than WPA-secured networks.

For more information about open WLAN configuration and other types of WLAN configuration, see Appendix C, "WLAN Configuration Types."

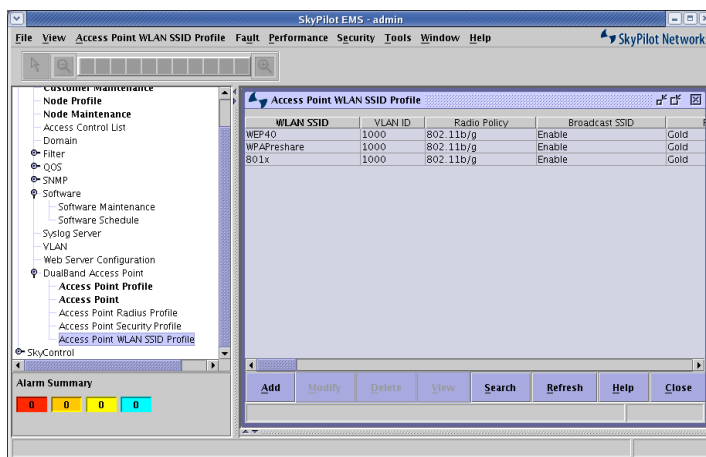
Follow these steps to create a profile that configures a WLAN for open access:

### 1 View the access point WLAN SSID profiles.

In the taskbar, double-click *SkyProvision* > *DualBand Access Point* > *Access Point WLAN SSID Profile*.

The information pane lists any existing WLAN SSID profiles. Figure 17 shows an example.

Figure 17. Access Point WLAN SSID Profile list



If the pane lists an access point WLAN SSID profile that you can use to configure an open access Wi-Fi network, skip to the section “Creating an access point profile” on page 38.

If you need to create an access point WLAN SSID profile, continue with step 2.

## 2 Add a new WLAN SSID profile.

Click the *Add* button below the profile list to display the Add Access Point WLAN SSID Profile dialog box. (Asterisks identify required fields.)

Figure 18. Add Access Point WLAN SSID Profile dialog box (top half)

| Field                  | Value     |
|------------------------|-----------|
| WLAN SSID *            |           |
| VLAN ID *              |           |
| Radio Policy *         | 802.11b/g |
| Broadcast SSID *       | Enable    |
| Prioritization *       | Gold      |
| SSID Status *          | Active    |
| <b>Security</b>        |           |
| Security Policy *      | None      |
| WEP Key Size           | 40        |
| WEP Encryption Key     |           |
| WEP Allow Shared Key   | Enable    |
| 802.1x Key Size        | 40        |
| 802.1x Rekeying Period |           |
| WPA Pre-Shared Key     | Enable    |
| WPA Passphrase         |           |

Enter a unique name for the WLAN in the *WLAN SSID* field. (You cannot create multiple SSIDs with the same name.)

To direct all traffic on the WLAN to a particular VLAN, enter an ID number in the *VLAN ID* field. (If you aren't using VLANs, enter 0 in this field.)

**NOTE** If you're setting up multiple WLAN SSIDs with different security policies or multiple IP address spaces, the use of VLANs is highly recommended.

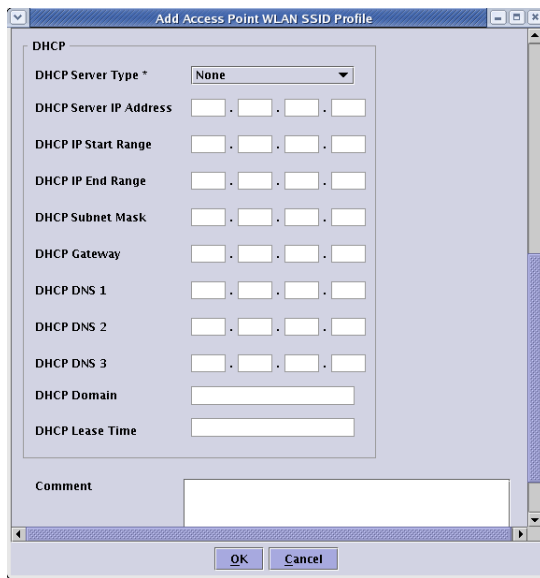


To make the WLAN visible to users searching for wireless networks, choose **Enable** from the **Broadcast SSID** pull-down menu. (This should be enabled in almost all instances.)

Make the WLAN operational by choosing **Active** from the **SSID Status** pull-down menu. If **Active** is not chosen, the access point won't announce the SSID or respond to requests by clients to associate with the WLAN.

Make the WLAN an open network by choosing **None** from the **Security Policy** pull-down menu.

Figure 19. Add Access Point WLAN SSID Profile dialog box (bottom half)

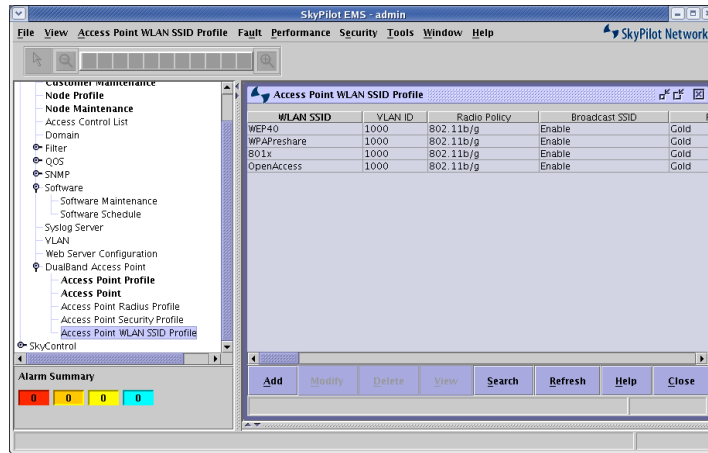


Choose **None** from the **DHCP Server Type** pull-down menu unless you plan to use the access point as the DHCP server. Making the access point a DHCP server is practical for only very small networks. Typically, you'll want to have access to a DHCP server through the wireless mesh network.

Click **OK** to save the WLAN SSID profile.

The new profile now appears in the list of WLAN SSID profiles. Figure 20 shows an example.

Figure 20. Access Point WLAN SSID Profile list with new profile



Repeat step 2 to add additional WLAN SSID profiles.

With a WLAN SSID profile for open access available, complete the access point configuration by going to the section “Creating an access point profile” on page 38.

## Creating a WLAN SSID profile for WPA

A Wi-Fi protected access (WPA) configuration for the SkyExtender DualBand authenticates Wi-Fi network users via a Radius server.

WPA uses the IEEE 802.1x and IETF EAP protocols to give users a secure connection with both the access point and the Radius server, allowing the exchange of credentials (*userName@domain* and *password*) and keys for encrypting all traffic between the client and the access point—even after authentication.

For more information on WLAN WPA configuration and other types of WLAN configuration, see Appendix C, “WLAN Configuration Types.”

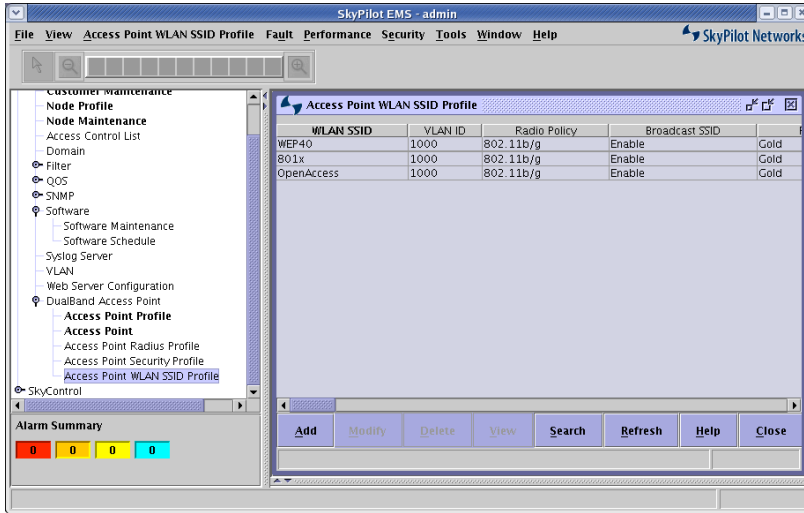
Follow these steps to create a profile that configures a WLAN for WPA:

- 1 View the access point WLAN SSID profiles.

In the taskbar, double-click *SkyProvision* > *DualBand Access Point* > *Access Point WLAN SID Profile*.

The information pane displays any existing WLAN SSID profiles. Figure 21 shows an example.

Figure 21. Access Point WLAN SSID Profile list



If the pane lists an access point WLAN SSID profile that you can use to configure a protected access Wi-Fi network, skip to the next section.

If you need to create an access point WLAN SSID profile, continue with step 2.

## 2 Add a new WLAN SSID profile.

Click the **Add** button below the profile list to display the Add Access Point WLAN SSID Profile dialog box. (Asterisks identify required fields.)

Figure 22. Add Access Point WLAN SSID Profile dialog box (top half)

The screenshot shows the 'Add Access Point WLAN SSID Profile' dialog box. It has a title bar with the text 'Add Access Point WLAN SSID Profile'. The dialog is divided into several sections. The top section contains the following fields and dropdowns: 'WLAN SSID \*' (text input), 'VLAN ID \*' (text input), 'Radio Policy \*' (dropdown menu with '802.11b/g' selected), 'Broadcast SSID \*' (dropdown menu with 'Enable' selected), 'Prioritization \*' (dropdown menu with 'Gold' selected), and 'SSID Status \*' (dropdown menu with 'Active' selected). Below this is a 'Security' section with a 'Security Policy \*' dropdown menu (set to 'None'). Under 'Security Policy \*', there are several sub-sections: 'WEP' (with 'WEP Key Size' dropdown set to '40', 'WEP Encryption Key' text input, and 'WEP Allow Shared Key' dropdown set to 'Enable'), '802.1x' (with '802.1x Key Size' dropdown set to '40' and '802.1x Rekeying Period' text input), and 'WPA' (with 'WPA Pre-Shared Key' dropdown set to 'Enable' and 'WPA Passphrase' text input).

Enter a unique name for the WLAN in the *WLAN SSID* field. (You cannot create multiple SSIDs with the same name.)

To direct all traffic on the WLAN to a particular VLAN, enter an ID number in the *VLAN ID* field. (If you aren't using VLANs, enter 0 in this field.)

**NOTE** If you're setting up multiple WLAN SSIDs with different security policies or multiple IP address spaces, the use of VLANs is highly recommended.

To make the WLAN visible to users searching for wireless networks, choose *Enable* from the *Broadcast SSID* pull-down menu. (This should be enabled in almost all instances.)

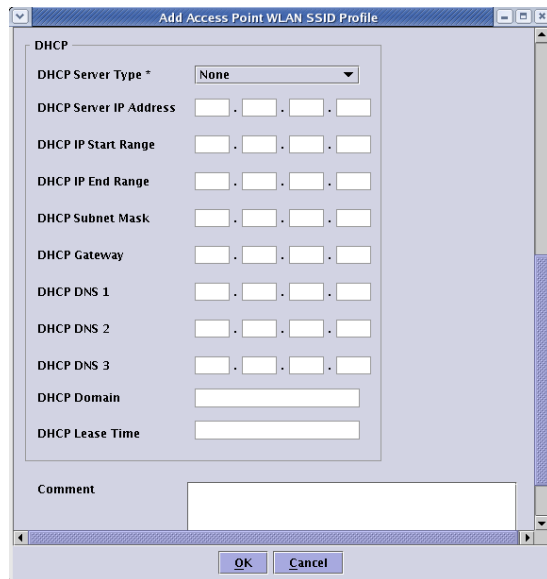
Make the VLAN operational by choosing *Active* from the *SSID Status* pull-down menu. If *Active* is not chosen, the access point won't announce the SSID or respond to requests by clients to associate with the WLAN.

Specify WPA protection by choosing *WPA* from the *Security Policy* pull-down menu.

Choose additional security settings in the *Security* area. (Do not enable *Pre-Shared Key*.)

**NOTE** Typically, you won't use a pre-shared key (PSK) for public access networks. If you want to employ encryption and key management mechanisms that are more stringent than WEP (Wired Equivalent Privacy), use Radius-based WPA instead of WPA-PSK.

Figure 23. Add Access Point WLAN SSID Profile dialog box (bottom half)

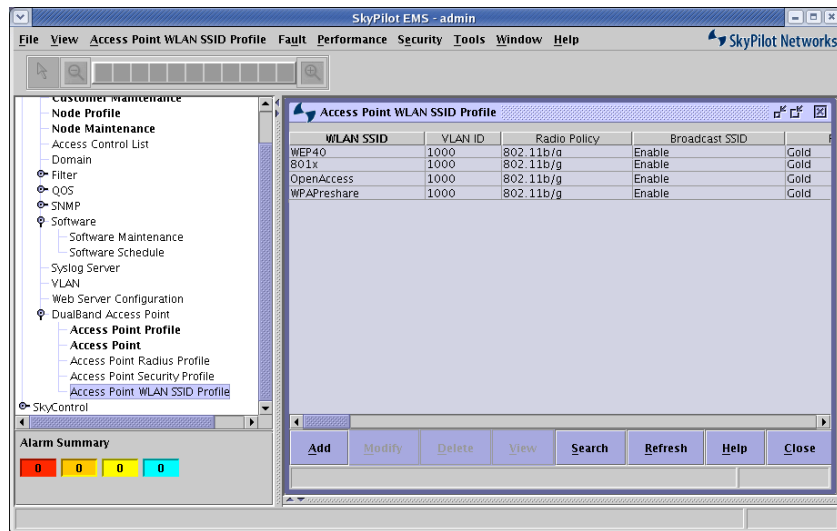


Choose *None* from the *DHCP Server Type* menu unless you plan to use the access point as the DHCP server. Making the access point a DHCP server is practical for only very small networks. Typically, you'll want to have access to a DHCP server through the wireless mesh network.

Click *OK* to save the WLAN SSID profile.

The new profile now appears in the list of WLAN SSID profiles. Figure 24 shows an example.

Figure 24. Access Point WLAN SSID Profile list with new profile



Repeat step 2 to add additional WLAN SSID profiles.

## Creating an access point profile

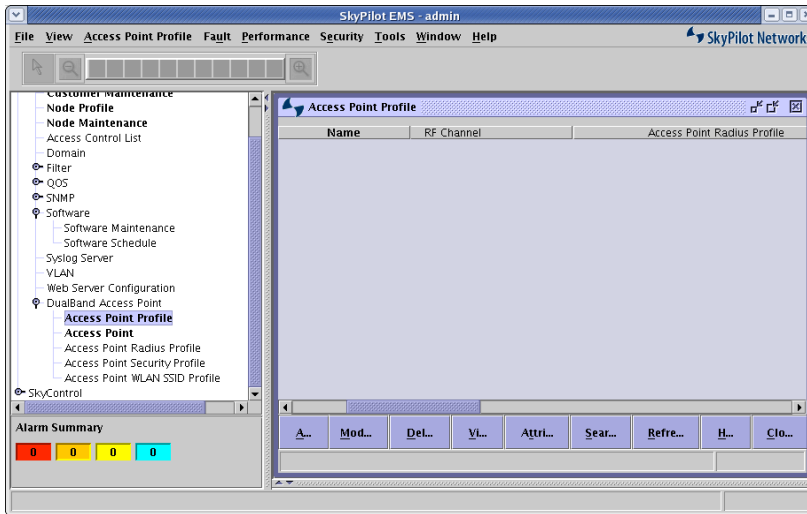
Complete the access point configuration by creating an access point profile.

### 1 Open the Access Point Profile pane.

In the taskbar, double-click *SkyProvision > DualBand Access Point > Access Point Profile*.

The Access Point Profile pane appears, listing any existing access point profiles.

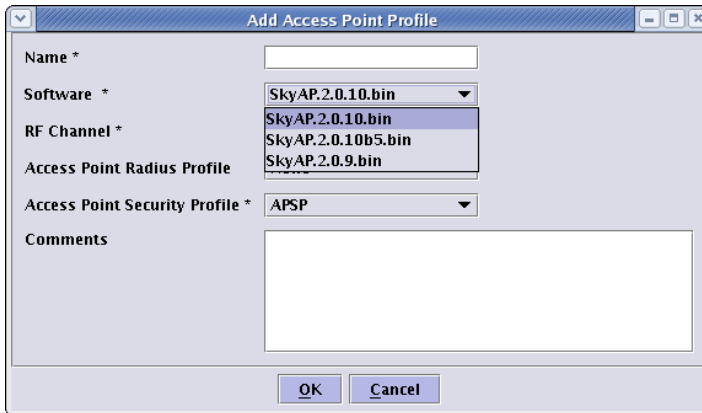
Figure 25. Access Point Profile list (empty)



2 Add a new access point profile.

Click the *Add* button below the Access Point Profile list to display the Add Access Point Profile dialog box. (Asterisks identify required fields.)

Figure 26. Add Access Point Profile dialog box

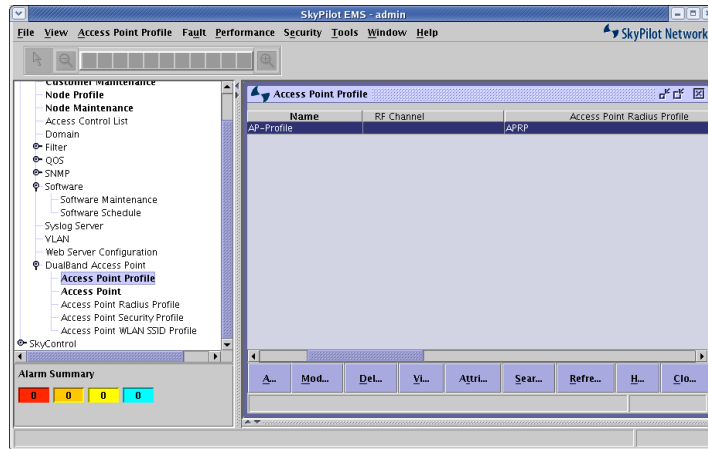


Use the provided fields and pull-down menus to give the profile a name, choose a software image, choose an access point security profile, and (if using WPA) specify an access point Radius profile.

Click **OK** to save the settings.

The new profile now appears in the Access Point Profile list.

Figure 27. Access Point Profile list with new profile



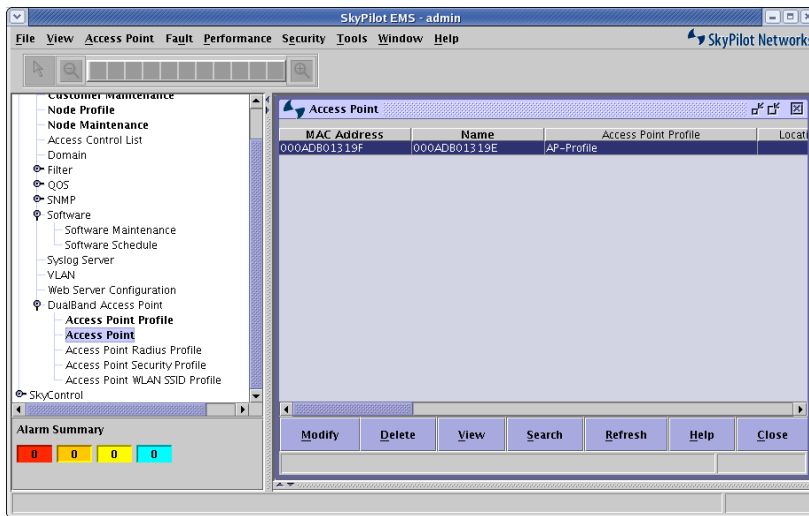
## Viewing the access point nodes

SkyProvision automatically creates the access point node from the access point profile you supplied. View the node by double-clicking *SkyProvision > DualBand Access Point > Access Point* in the taskbar.

The Access Point pane appears, listing any existing access points. Figure 28 shows an example.



Figure 28. Access Point list



For each access point, SkyProvision shows current information, including the MAC address, name, profile assignment, and creation date.

## Verifying the new node

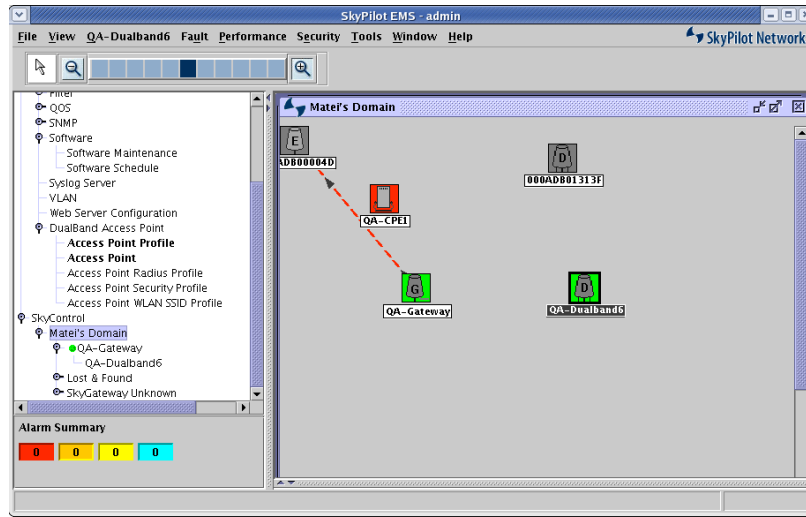
To verify that the newly configured SkyExtender DualBand is configured as a network node, use the SkyControl application to view a graphical representation of the device as part of the domain to which you assigned it.

### 1 View the node in the domain map.

In the taskbar, click the expansion icon next to *SkyControl* to view all the application options, and then double-click the name of the domain to which you assigned the new SkyExtender DualBand.

A domain view pane opens, displaying a graphical representation of the domain, including your new device. Figure 29 shows an example.

Figure 29. SkyControl domain view



2 View the device details.

Double-click the SkyExtender DualBand icon to display a Device Details window for the device. The window displays current settings for the device, including its MAC address, IP address, and network status. Figure 30 shows an example.

Figure 30. Device Details window



- 3 Click *Close*.

## Provisioning the SkyExtender DualBand

The access point configuration you created in SkyProvision is automatically sent to the SkyExtender DualBand the next time the device is polled by the network.

For more information on using SkyControl to set polling intervals and other provisioning parameters, see the *SkyPilot Network Administration Guide*.



## Using the Access Point Configuration Tool

This chapter explains how to manually configure a SkyExtender DualBand access point with the Web-based configuration tool on board in the access point. Manual configuration using an on-board configuration tool is provided as an alternative to automatic configuration via the provisioning server and SkyPilot EMS software.

You'll learn how to connect to the tool and use it to set operating and access parameters for the Wi-Fi network. The chapter also offers descriptions of tool pages, fields, and buttons you can use to modify and monitor the configuration.

### Setting up your connection

Before using the configuration tool to create a manual configuration for the SkyExtender DualBand access point, you must first set up access to the device. You have two options for setting up access: establishing a connection from the wireless mesh network available through the SkyExtender component of the SkyExtender DualBand, or connecting to the access point directly via a Wi-Fi connection.

#### *Checking VLAN status*

When setting up your connection to the SkyExtender DualBand access, make sure no VLAN currently operates on the DHCP server, host computer, and the SkyGateway. Or, if you already have a management VLAN for your SkyExtenders—that is, the DHCP server—verify that the host computer is on the same VLAN.

If you set a management VLAN for the SkyExtender component of the SkyExtender DualBand via the EMS client or a manual configuration, the SkyExtender DualBand access point automatically uses the same VLAN as the SkyExtender component to manage access point communications. If no management VLAN is set for the SkyExtender component, you cannot set up a management VLAN for only the access point component.

### *Setting up access via the SkyPilot wireless mesh network*

To use the configuration tool from the wireless mesh network, verify that your installation meets these requirements:

- The SkyExtender component of SkyExtender DualBand has established a wireless connection with the SkyGateway serving as the network hub, or to another SkyExtender connecting to the SkyGateway.
- A DHCP server is connected to the SkyGateway and is set up to distribute IP addresses across the wireless mesh network.

To connect to the access point from a host computer on the SkyPilot wireless mesh network:

**1 Confirm that the SkyExtender DualBand is configured correctly and connected to the SkyPilot wireless mesh network.**

Confirm the connection by pinging the IP address of the SkyExtender DualBand EXT radio, which is also the standard SkyExtender IP address.

**2 Get the IP address of the SkyExtender DualBand access point.**

You'll find the IP address of the access point in the DHCP server log that's based on the MAC address of the access point. The access point's MAC address is always 1 less than the MAC address of the SkyExtender DualBand, which is visible on the label affixed to the bottom of the device.

**NOTE** MAC addresses use a base-16 (hexadecimal) system in which the letters A–F represent numbers 10–15. For example, if the MAC address of the SkyExtender DualBand is 00 0A DB 01 31 9F, the MAC address of the access point will be 00 0A DB 01 31 9E.

You'll use this IP address to connect to the access point over the SkyPilot wireless mesh network.

**NOTE** You can also configure the DHCP server to provide a specific address based on the MAC address of the access point—that is, 1 less than the MAC address that's visible on the label affixed to the bottom of the SkyExtender DualBand.

**3** Confirm that you can communicate with the access point within the SkyExtender DualBand.

Ping the address you identified in step 2.

If you can successfully ping the IP address of the access point, go to the section "Starting the configuration tool" on page 49 for instructions on opening the Web-based configuration tool.

If you can't ping the IP address, follow the instructions in Appendix A, "Connecting to the Access Point Command-Line Interface," to connect to the access point via a serial console, and then confirm the IP address assignment from the console.

If a management VLAN operates on the DHCP server, your host computer, and the access point, confirm that it's the same VLAN as the one configured for use by the SkyExtender component of the SkyExtender DualBand. If it's not the same management VLAN or there is no VLAN set up for the SkyExtender component, disable the VLAN and reattempt pinging the IP address of the access point.

### *Setting up access via a local Wi-Fi connection*

An alternative method is to initially manage the SkyExtender DualBand access point from a computer with a direct Wi-Fi connection to the SkyExtender DualBand access point.

To connect to the SkyExtender DualBand access point through a Wi-Fi connection, you need a Wi-Fi/WPA-PSK capable computer that's within operating range of the access point and a Web browser application.

**NOTE** The SkyExtender DualBand does not have to be connected to a SkyPilot mesh network while you're configuring it for access point operations via an 802.11b/g wireless connection.

If the SkyExtender DualBand is also connected to the wireless mesh network and is receiving an IP address from a DHCP server, you'll have to view the DHCP log to identify the IP address.

To connect to the access point from the Wi-Fi network:

- 1 Set up your host computer's 802.11b/g interface to connect to the SSID *SkyPilotDualBand*, the default WLAN configured for the SkyExtender DualBand access point.**

The default WLAN *SkyPilotDualBand* employs a WPA-PSK protection scheme that uses a public key (password) of *publicpublic* to control access. You're prompted for this key when you connect to the SSID from your computer.

- 2 Set an IP address for your computer's 802.11b/g interface.**

If the SkyExtender DualBand is not connected to a DHCP server via the SkyPilot mesh network, enter the IP address *192.168.0.9* and apply the setting.

If the SkyExtender DualBand is connected to a SkyPilot mesh network and receiving an IP address from a DHCP server, use an IP address that's within the address space the DHCP server is using for device assignments.

- 3 Confirm that your computer can communicate with the SkyExtender DualBand access point.**

Ping the IP address of the access point, either the default *192.168.0.3* or the address assigned to it by a DHCP server. (This is same IP address you use to connect to the access point's Web-based configuration tool.)

If you can successfully ping the access point's IP address, go to the next section for instructions on starting the Web-based configuration tool.

If you cannot ping the IP address, you need to troubleshoot the problem before proceeding. See Appendix A, "Connecting to the Access Point



Command-Line Interface,” for instructions on verifying the address of the access point from a serial console.

## Starting the configuration tool

To run the configuration tool, you need the current address of the access point component of the SkyExtender DualBand. (The default IP address of the access point is **198.68.0.3**.)

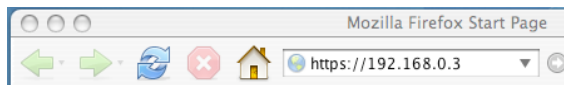
If the access point was assigned an IP address by a DHCP server, it must be within the address space the DHCP server uses to populate devices. (For more information on getting an IP address assigned by DHCP, see the previous section.)

To start the configuration tool:

- 1 Open a Web browser and enter the URL of the access point.

Figure 31 shows an example.

Figure 31. Entering the access point URL

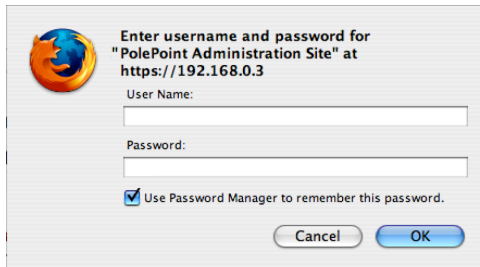


**NOTE** The access point uses the Secure Sockets Layer (SSL) for secure transmission across the Internet. By convention, a URL that requires an SSL connection begins with *https* instead of *http*.

Depending on your browser settings, a dialog box may appear that asks you to confirm certificate authority for the Web address. Click **OK** to proceed.

A prompt appears, asking you to enter a user name and password.

Figure 32. Prompt for user name and password



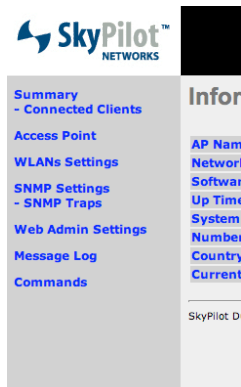
The screenshot shows a dialog box titled "Enter username and password for 'PolePoint Administration Site' at https://192.168.0.3". It features a globe icon on the left. The dialog contains two input fields: "User Name:" and "Password:". Below the password field is a checked checkbox labeled "Use Password Manager to remember this password." At the bottom, there are "Cancel" and "OK" buttons.

- 2 Log in by entering the default user name (*admin*) and password (*public*).

A summary page appears, displaying the current status of the access point. The next section shows an example and explains the information displayed.

The configuration tool provides a navigation bar on the left side. To navigate to a page, click the corresponding item in the bar. You create and modify configurations by using tool pages to enter data and select configuration options.

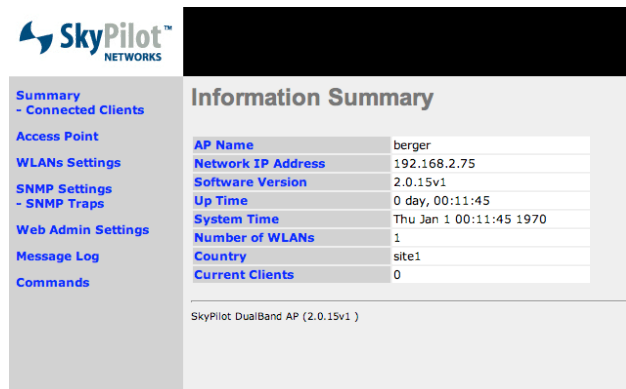
Figure 33. Configuration tool navigation bar



## Information Summary page

The Information Summary page is the first page you see when you log in to the configuration tool. It provides an overview of the access point's current status.

Figure 34. Information Summary page



| Parameter          | Value                   |
|--------------------|-------------------------|
| AP Name            | berger                  |
| Network IP Address | 192.168.2.75            |
| Software Version   | 2.0.15v1                |
| Up Time            | 0 day, 00:11:45         |
| System Time        | Thu Jan 1 00:11:45 1970 |
| Number of WLANs    | 1                       |
| Country            | site1                   |
| Current Clients    | 0                       |

SkyPilot DualBand AP (2.0.15v1 )

**AP Name.** The name assigned to the access point.

**Network IP Address.** The IP address of the access point, assigned by DHCP or provided as a static address. (The default is **192.168.0.3**.)

**Software Version.** The version of the software running on the access point.

**Up Time.** The amount of time since the access point was last booted.

**System Time.** The system date and time as set by NTP or, if not set by NTP, January 1, 1970 plus the amount of time since the access point was last booted (**Up Time**).

**Number of WLANs.** The number of WLANs configured and enabled.

**Country.** An arbitrary string specifying the physical location of the unit.

**Current Clients.** The number of clients associated with the access point.

## Access Point Configuration page

Clicking **Access Point** in the navigation bar takes you to the Access Point Configuration page. Use this page to view and modify the access point's global configuration parameters. These parameters apply to all the wireless networks that use the access point as a hub.

Figure 35. Access Point Configuration page

**Access Point Configuration**

Save Save to flash and activate

|                                |                                     |                                    |
|--------------------------------|-------------------------------------|------------------------------------|
| AP Name                        | berger                              |                                    |
| Location                       | site1                               |                                    |
| Server IP                      | 192.168.2.75                        | <input type="checkbox"/> From DHCP |
| Subnet Mask                    | 255.255.255.0                       |                                    |
| Default Gateway                | 192.168.2.1                         |                                    |
| DNS Server                     | 192.168.2.3                         |                                    |
| Provisioning                   | <input checked="" type="checkbox"/> |                                    |
| TFTP Server Address            |                                     |                                    |
| Management HTTP Server Address |                                     | Port 8000                          |
| VLAN ID                        | 0                                   |                                    |
| NTP Server                     | pool.ntp.org                        |                                    |

**Security Setting**

|                                  |   |                  |
|----------------------------------|---|------------------|
| SSH Server                       | <input checked="" type="checkbox"/> Enabled |                  |
| SSH Server Password              | *****                                       | User Name: root  |
| Telnet Server                    | <input checked="" type="checkbox"/> Enabled |                  |
| Telnet Server Password           | *****                                       | User Name: admin |
| Maximum Remote Session           | 0   |                  |
| Remote Session Idle Timeout      | 0   | minutes          |
| Peer to Peer                     | <input type="checkbox"/> Enabled            |                  |
| Management from Wireless Clients | <input checked="" type="checkbox"/> Enabled |                  |
| SysLog to Remote Server          | <input type="checkbox"/> Enabled            |                  |

After modifying the access point configuration settings, click the *Save* or *Save to flash and activate* button at the top or bottom of the page:

- Click *Save* to save your changes to volatile RAM on the access point. A message confirms the change in configuration.
- Click *Save to flash and activate* to save your changes to flash (nonvolatile) memory and instantly update the SkyExtender DualBand access point's active configuration. (You can also save all configuration changes to flash memory from the Configuration Management Commands page, as described in the section "Configuration Management Commands page" on page 72.)

### Names and addresses

Use the top area of the Access Point Configuration page to view and edit names and general address settings for the access point.

Figure 36. Name and address fields on Access Point Configuration page

The screenshot shows the 'Access Point Configuration' page with the following fields and values:

| Field                          | Value  |
|--------------------------------|--|
| AP Name                        | berger   |
| Location                       | site1  |
| Server IP                      | 192.168.2.75<br><input type="checkbox"/> From DHCP |
| Subnet Mask                    | 255.255.255.0                                      |
| Default Gateway                | 192.168.2.1  |
| DNS Server                     | 192.168.2.3  |
| Provisioning                   | <input checked="" type="checkbox"/>                |
| TFTP Server Address            |  |
| Management HTTP Server Address | Port 8000  |
| VLAN ID                        | 0  |
| NTP Server                     | pool.ntp.org                                       |

**AP Name.** A name to be given to the access point. (This name is for user convenience; it has no relation with the device address.)

**Location.** A location name for the access point. (The location name is also for user convenience; it has no effect on the device address.)

**Server IP.** An IP address to be used for managing the access point. It should be in the same network segment as the management IP address for the SkyExtender. Check **From DHCP** if the IP address is provided by a DHCP server. If **From DHCP** is checked, the other IP address fields are unavailable for editing; otherwise, you must enter static IP addresses in the empty address fields.

**Subnet Mask.** (Unavailable if **From DHCP** is checked) The IP subnet mask associated with the **Server IP** address.

**Default Gateway.** (Unavailable if **From DHCP** is checked) An IP gateway address for the network associated with the **Server IP** address.

**DNS Server.** (Optional) The address of a server providing DNS name resolution for that network.

**Provisioning.** Enables automatic configuration; should always be checked. If automatic configuration is not available, the access point will use the configuration currently stored in flash (nonvolatile) memory.

**TFTP Server Address.** Overrides Provisioning TFTP Server Address. (Leave blank for now.)

**Management HTTP Server Address.** Overrides Provisioning HTTP Server Address. (Leave blank for now.)

**VLAN ID.** A read-only field that automatically denotes the same VLAN as the SkyExtender's management VLAN. If there is no management VLAN, this field shows 0.

**NTP Server.** xxx.

### Security Setting area

Use the Security Setting area of the Access Point Configuration page to enable security services, provide passwords, and set up remote access of the access point.

Figure 37. Security Setting area of Access Point Configuration page

| Security Setting                 |   |
|----------------------------------|---|
| SSH Server                       | <input checked="" type="checkbox"/> Enabled         |
| SSH Server Password              | ***** User Name: <input type="text" value="root"/>  |
| Telnet Server                    | <input checked="" type="checkbox"/> Enabled         |
| Telnet Server Password           | ***** User Name: <input type="text" value="admin"/> |
| Maximum Remote Session           | <input type="text" value="0"/>                      |
| Remote Session Idle Timeout      | <input type="text" value="0"/> minutes              |
| Peer to Peer                     | <input type="checkbox"/> Enabled                    |
| Management from Wireless Clients | <input checked="" type="checkbox"/> Enabled         |
| SysLog to Remote Server          | <input type="checkbox"/> Enabled                    |

**SSH Server.** Check to enable the SSH server on the access point and permit remote access to the device command line via SSH.

**SSH Server Password.** (Available only if **SSH Server** is enabled) Use these fields to set an SSH user name and password.

**Telnet Server.** Check to enable the Telnet server for remote access of the access point command line.

**Telnet Server Password.** (Available only if **Telnet Server** is enabled) Use these fields to set a Telnet user name and password.

**Maximum Remote Session.** Use this field to enter the number of simultaneous remote SSH or Telnet sessions that are allowed. If the value is 0, unlimited sessions are allowed.

**Remote Session Idle Timeout.** Use this field to specify how long (in minutes) an SSH or Telnet session will stay connected without activity. If the value is 0, the idle timeout is unlimited.

**Peer to Peer.** Check to block Layer 2 broadcast and ARP traffic between wireless clients. Enable **Peer to Peer** in a public network if you want to prevent users from “sniffing” traffic or creating accidental “network neighborhoods” at the Ethernet or VLAN level. A private enterprise network may want to disable **Peer to Peer** to permit shared LAN services such as file sharing.

**Management from Wireless Clients.** Check to allow management of the access point from wireless clients.

**SysLog to Remote Server.** Check to allow login to a remote server.

### Radius Server Setting area

Radius servers supply backend authentication services for 802.1x or WPA WLAN security. The Radius Server Setting area of the Access Point Configuration page needs to be configured only if 802.1x or WPA authentication will be used in any of the WLANs. If so, you must provide at least the primary Radius host information. Secondary host parameters are optional; however, use of a secondary host is highly recommended for consumer installations.

Figure 38. Radius Server Setting area of Access Point Configuration page

| Radius Server Setting |  |
|-----------------------|--|
| Primary Host          | 192.168.2.3  |
| Secret                | retold-fever   |
| Authentication Port   | 1812 <input type="button" value="Default AuthPort"/> |
| Accounting Port       | 1813 <input type="button" value="Default AcctPort"/> |
| Secondary Host        |  |
| Secret                |  |
| Authentication Port   | 1812 <input type="button" value="Default AuthPort"/> |
| Accounting Port       | 1813 <input type="button" value="Default AcctPort"/> |

**Primary Host.** An IP address for the primary Radius server that will authenticate users of any 802.1x/WPA WLANs.

**Secret.** The shared secret that is configured in the primary Radius server and is used to authenticate the access point to the Radius server.

**Authentication Port.** A TCP/UDP port for primary Radius server authentication services. The port number you supply must be the one on which the primary Radius server is configured for authentication. Click the **Default AuthPort** button to reset the value to the standard port number.

**Accounting Port.** A TCP/UDP port for the primary Radius server accounting services. The port number you supply must be the one on which the primary Radius server is configured for accounting. Click the **Default AcctPort** button to reset the value to the standard port number.

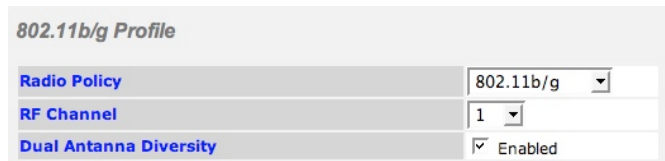
**Secondary Host.** An IP address of the optional secondary Radius server for authenticating users of any 802.1x/WPA WLANs.

**Secret, Authentication Port, and Accounting Port** under **Secondary Host** are the same as above but apply to the secondary Radius server.

### 802.11b/g Profile area

Use the 802.11b/g Profile area of the Access Point Configuration page to select a radio policy and frequency channel for access point operations.

Figure 39. 802.11 b/g Profile area of Access Point Configuration page



| 802.11b/g Profile      |   |
|------------------------|---|
| Radio Policy           | 802.11b/g                                   |
| RF Channel             | 1   |
| Dual Antenna Diversity | <input checked="" type="checkbox"/> Enabled |

**Radio Policy.** Use this menu to specify a mixture of 802.11b/g clients or force all access to 802.11b only. (Typically, you'll want the 802.11b/g mixture.)

**RF Channel.** Use this menu to choose a frequency channel for the access point to operate on. Although 11 channels are available in the US, only three of these channels overlap: 1, 6, and 11. Set the channel to one of the three



nonoverlapping channels unless you plan to implement special channel reuse patterns and possess the requisite technical knowledge.

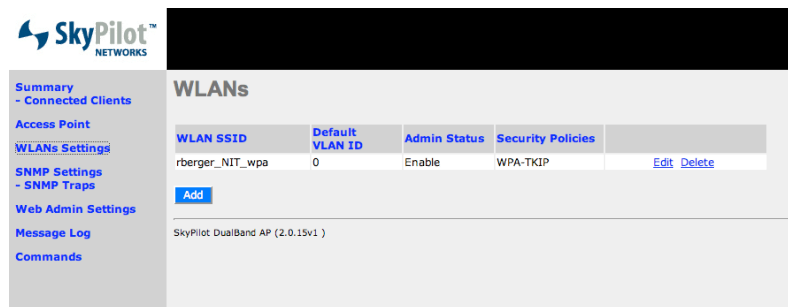
*Dual Antenna Diversity*. Check to enable antenna diversity.

## WLANs page

Clicking *WLAN Settings* in the configuration tool navigation bar takes you to the WLANs page, which lets you view and configure wireless networks (also known as virtual access points or multiple SSIDs). You can configure up to eight WLANs for the access point, each with a unique SSID and independent authentication/security policies.

By default, the access point includes one predefined SSID (*SkyPilotDualBand*) that uses a WPA-PSK configuration (also known as WPA-Personal).

Figure 40. WLANs page



For each SSID you configure, the summary page displays the SSID name, a default VLAN ID (if present), the current administrative status, and the security policies in effect.

This page also provides the ability to edit, delete, or add a WLAN SSID.

### WLAN Details page

The WLAN Details page appears when you click *Add* or (when a WLAN SSID is selected) *Edit* on the WLANs page. Use the WLAN Details page to add a new WLAN or edit an existing WLAN in your access point configuration.

After making edits on the WLAN Details page, click *Save* to save your changes to volatile RAM on the access point, or *Save to flash and activate* to save them to flash memory and instantly update the access point's active configuration.

After a save, the WLANs page reappears, displaying the new WLAN or updated details of the edited WLAN. If you leave the WLANs page without saving the modified configuration to the access point, you can go to the Configuration Management Commands page and perform the necessary steps to save the new information to the access point's flash memory. For more information, see the section "Configuration Management Commands page" on page 72.

Figure 41. WLAN Details page

| WLAN Details  |                                  |
|---|----------------------------------|
| <input type="button" value="Save"/> <input type="button" value="Save to flash and activate"/> |                                  |
| WLAN SSID   | <input type="text"/>             |
| Default VLAN ID   | <input type="text" value="0"/>   |
| Broadcast SSID  | <input type="checkbox"/> Enabled |
| Default Quality of Service  | Bronze ▾                         |
| Admin Status  | <input type="checkbox"/> Enabled |
| DHCP Server Type  | None ▾                           |
| Security Policy   | None ▾                           |
| <input type="button" value="Save"/> <input type="button" value="Save to flash and activate"/> |                                  |

**WLAN SSID.** (Required) Use this field to supply the SSID that's announced for this WLAN. The text string you enter here will appear to 802.11 clients as the name of a WLAN (unless *Broadcast SSID* is not enabled).

**Default VLAN ID.** Use this field to identify the data VLAN ID mapped to this WLAN. If this ID is set to 0, there is no VLAN assignment.

**NOTE** If you're configuring the new WLAN for 802.1x or WPA, a RADIUS server can override the default VLAN setting on a per-user basis.

**Broadcast SSID.** If checked, the access point will broadcast its SSID to 802.11 clients, making it visible to users. If unchecked, the access point will not broadcast the SSID. However, users can still choose to associate with this SSID/WLAN if they

know the SSID and are able to configure their client software to connect to the SSID. (Enable this option for most cases.)

**Default Quality of Service.** Use this menu to choose one of three 802.1p Quality of Service (QoS) levels. The access point does not enforce the selected QoS level; it simply sets the 802.1p tag for the selected level on all traffic that enters the WLAN. The mapping of the QoS pull-down options to 802.1p user priority is: Gold = 6, Silver = 3, and Bronze = 0.

Figure 42. WLAN Details page showing QoS choices

The screenshot shows the 'WLAN Details' configuration page. At the top, there are two buttons: 'Save' and 'Save to flash and activate'. Below this is a table of configuration fields:

|                            |                                  |
|----------------------------|----------------------------------|
| WLAN SSID                  | <input type="text"/>             |
| Default VLAN ID            | 0                                |
| Broadcast SSID             | <input type="checkbox"/> Enabled |
| Default Quality of Service | Bronze                           |
| Admin Status               | <input type="checkbox"/>         |
| DHCP Server Type           | None                             |
| Security Policy            | None                             |

At the bottom of the configuration area, there are two more buttons: 'Save' and 'Save to flash and activate'. Below the buttons, the text 'SkyPilot DualBand AP (2.0.15v1)' is visible.

**Admin Status.** Check to activate this WLAN. If the box is not checked, the WLAN will be configured but not yet activated. If the WLAN is not activated, the access point will not announce or respond to connection requests or other traffic directed to the SSID.

#### DHCP Server Type menu

Use the **DHCP Server Type** menu on the WLAN Details page to specify a DHCP relay or local DHCP server for use by the WLAN. The choices are **None**, **Relay**, and **Server**. Typically, you'll choose **None** to allow IP addresses to be supplied by a central DHCP server elsewhere on the network.

Figure 43. WLAN Details page showing DHCP Server Type menu

The screenshot shows the SkyPilot Networks interface for the 'WLAN Details' page. On the left is a sidebar with navigation links: Summary - Connected Clients, Access Point, WLANs Settings, SNMP Settings - SNMP Traps, Web Admin Settings, Message Log, and Commands. The main content area is titled 'WLAN Details' and contains two 'Save' buttons: 'Save' and 'Save to flash and activate'. Below these are several configuration fields: 'WLAN SSID' (text input), 'Default VLAN ID' (text input with value '0'), 'Broadcast SSID' (checkbox 'Enabled'), 'Default Quality of Service' (dropdown menu with 'Bronze' selected), 'Admin Status' (checkbox 'Enabled'), 'DHCP Server Type' (dropdown menu with 'None' selected and an open menu showing 'None', 'Relay', and 'Server'), and 'Security Policy' (dropdown menu with 'None' selected). At the bottom of the main area, there is another 'Save' and 'Save to flash and activate' button, and a footer note: 'SkyPilot DualBand AP (2.0.15v1)'.

If you choose *Relay*, a new field, *DHCP Server IP*, appears in an area labeled *DHCP Relay Parameters*. Use this field to supply the IP address of the authoritative DHCP server for the network.

Figure 44. DHCP Relay Parameters area of WLAN Details page

This screenshot shows a close-up of the 'DHCP Relay Parameters' section within the 'WLAN Details' page. The 'DHCP Server Type' dropdown is set to 'Relay'. Below it, a new text input field labeled 'DHCP Server IP' is visible. The 'Save' and 'Save to flash and activate' buttons are also present at the bottom of this section.

If you choose *Server* from the *DHCP Server Type* menu, a *DHCP Server Parameters* area appears that lists additional fields for configuring a local DHCP server for use by the WLAN.

Figure 45. DHCP Server Parameters area of WLAN Details page

**WLAN Details**

Save Save to flash and activate

|                            |   |
|----------------------------|---|
| WLAN SSID                  |   |
| Default VLAN ID            | 0   |
| Broadcast SSID             | <input type="checkbox"/> Enabled            |
| Default Quality of Service | Silver                                      |
| Admin Status               | <input checked="" type="checkbox"/> Enabled |
| DHCP Server Type           | Server                                      |
| Security Policy            | None  |

**DHCP Server Parameters**

|                   |  |
|-------------------|--|
| IP Start Range    |  |
| IP Stop Range     |  |
| Subnet Mask       |  |
| Broadcast Address |  |
| Gateway           |  |
| DNS 1             |  |
| DNS 2             |  |
| DNS 3             |  |
| Domain            |  |
| Lease Time        |  |

seconds

Save Save to flash and activate

SkyPilot DualBand AP (2.0.15v1)

**IP Start Range.** A starting address for the IP address pool supplied by the DHCP server—for example, 192.168.10.100.

**IP Stop Range.** An end address for the IP address pool—for example, 192.168.10.254.

**Subnet Mask.** A subnet mask for this network segment—for example, 255.255.255.0.

**Broadcast Address.** An IP address for IP broadcasts on this network segment.

**Gateway.** The IP address of the default gateway/router for this network segment.

**DNS 1.** The IP address of the primary DNS resolver for this network.

**DNS 2.** The IP address of the secondary DNS resolver for this network.

**DNS 3.** The IP address of the tertiary DNS resolver for this network.

**Domain.** A default domain name for this network.

**Lease Time.** The length of time each DHCP lease remains valid before renewal is necessary.

### Security Policy menu

Use the **Security Policy** menu on the WLAN Details page to specify the types of encryption and authentication you want the WLAN to use.

Figure 46. WLAN Details page showing Security Policy menu

The screenshot shows the 'WLAN Details' configuration page. At the top, there are two buttons: 'Save' and 'Save to flash and activate'. Below this is a form with several fields:

- WLAN SSID**: Text input field.
- Default VLAN ID**: Text input field with '0' entered.
- Broadcast SSID**: Checkable field with 'Enabled' selected.
- Default Quality of Service**: Dropdown menu with 'Bronze' selected.
- Admin Status**: Checkable field with 'Enabled' selected.
- DHCP Server Type**: Dropdown menu with 'Relay' selected.
- Security Policy**: Dropdown menu with 'None' selected. The dropdown is open, showing the following options: None, Static WEP, 802.1X, WPA-TKIP (highlighted), and WPA-AES:CCMP.

Below the Security Policy field is a section for 'DHCP Relay Parameters' and a 'DHCP Server IP' field. At the bottom of the form, there are two buttons: 'Save' and 'Save to flash and activate'. The footer of the page reads 'SkyPilot DualBand AP (2.0.15v1)'.

The choices are:

- **None.** An open network (no authentication or encryption).
- **Static WEP.** No authentication, a shared WEP key, no key rotation, and WEP encryption.

**NOTE** Static WEP is easily cracked and should not be used in production environments.

- **802.1X.** Authentication via 802.1x/EAP. This scheme uses encryption with dynamic WEP (the WEP key is unique per session and is automatically changed at a periodic rate via Radius re-authentication). This is the preferred option for older clients that do not support WPA. WPA is the best choice unless there are specific CPE requirements.

**NOTE** 802.1x requires you to configure at least one Radius server on the Access Point Configuration page.

If **802.1X** is selected, two additional fields become available, as shown in Figure 47.

Figure 47. 802.1X Parameters area of WLAN Details page

The screenshot shows the 'WLAN Details' configuration page. On the left is a navigation menu with options: Summary - Connected Clients, Access Point, WLANs Settings, Domain Settings, SNMP Settings - SNMP Traps, Web Admin Settings, Message Log, and Commands. The main content area is titled 'WLAN Details' and contains a 'Save' button at the top left. Below this is a table of configuration options:

|                            |   |
|----------------------------|---|
| WLAN SSID                  | New SSID                                    |
| Default VLAN ID            | 0   |
| Broadcast SSID             | <input checked="" type="checkbox"/> Enabled |
| Default Quality of Service | Gold  |
| Admin Status               | <input type="checkbox"/> Enabled            |
| DHCP Server Type           | None  |
| Security Policy            | 802.1X                                      |

Below the table is the '802.1X Parameters' section, which includes:

- WEP Key Size:** A dropdown menu with options: 104 bits (selected), 40 bits, and 104 bits.
- Re-keying Period:** A text input field with the value 'seconds (0: Disable)'.

A 'Save' button is located at the bottom left of the 802.1X Parameters section.

**WEP Key Size.** Use this menu to select a key size: 40 bits or 104 bits (also known as 64-bit and 128-bit). 104 bits is preferred unless the WLAN clients are unable to accept that setting.

**Re-keying Period.** Use this field to specify (in seconds) how often the dynamic WEP key is updated. For maximum protection, enter a value of 300 or less. Because re-keying requires about a second to complete, lower numbers in this field will increase periodic latency.

- **WPA-TKIP.** Authentication via 802.1x/EAP, and encryption via TKIP (Temporal Key Integrity Protocol), a hardened version of the older WEP standard. The key is updated automatically and transparently with DES (Data Encryption Standard) or AES (Advanced Encryption Standard) encryption.

This option provides the highest level of security, but it requires users to have a WPA client (which is built into recent versions of Windows XP, Mac OS X, and Linux).

**NOTE** The **WPA** option requires you to configure at least one Radius server on the Access Point Configuration page.

When **WPA** is selected, a **Pre-Shared Key** checkbox and **Passphrase** entry field appear.

- **WPA-AES:CCMP.** The complete 802.11i / WPA2 standard, replacing WEP/DES and TKIP with a specific mode of AES called CCMP (Counter-Mode/CBC-MAC Protocol. which uses Cipher Block Chaining-Message Authentication Code). CCMP provides both data confidentiality (encryption) and data integrity. This is the highest security option you can choose, but some legacy 802.11 clients may not support it.

Figure 48. WPA Parameters area of WLAN Details page

The screenshot shows the 'WLAN Details' configuration page. On the left is a navigation menu with options like Summary, Connected Clients, Access Point, WLANs Settings, Domain Settings, SNMP Settings, Web Admin Settings, Message Log, and Commands. The main content area is titled 'WLAN Details' and contains a 'Save' button at the top. Below it is a table of settings:

|                            |   |
|----------------------------|---|
| WLAN SSID                  | New SSID                                    |
| Default VLAN ID            | 0   |
| Broadcast SSID             | <input checked="" type="checkbox"/> Enabled |
| Default Quality of Service | Gold  |
| Admin Status               | <input type="checkbox"/> Enabled            |
| DHCP Server Type           | None  |
| Security Policy            | WPA   |

Below the table is the 'WPA Parameters' section, which includes a 'Pre-Shared Key' checkbox that is currently disabled. A second 'Save' button is located at the bottom of this section.

- **WPA-PSK.** Also known as WPA-Personal; enables a single shared password for access to this WLAN. TKIP is still used to create automatic and transparent key updates, thereby making WPA-PSK secure from an encryption standpoint. It's



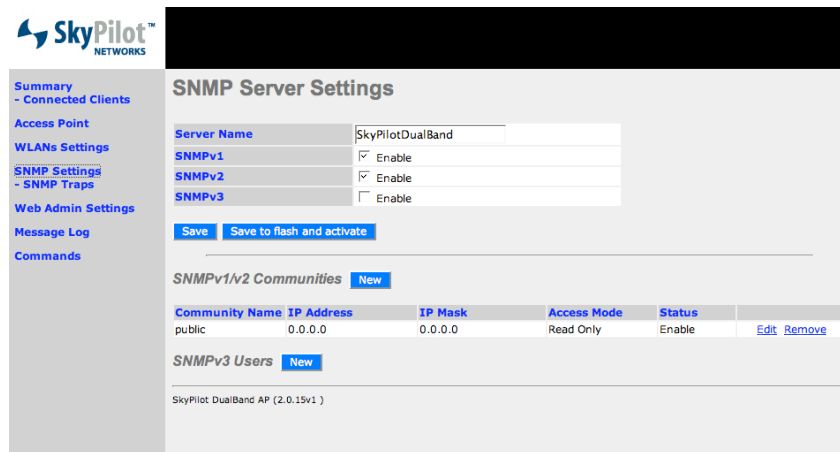
not very useful to service providers, however, since one password is shared by all subscribers (so it's not very secret).

Always enable *Pre-Shared Key* for WPA-PSK.

## SNMP Server Settings page

Clicking *SNMP Settings* in the configuration tool navigation bar takes you to the SNMP Server Settings page. Use this page to configure the access point for SNMP operations.

Figure 49. SNMP Server Settings page



After modifying the SNMP server settings, click *Save* to save your changes to volatile RAM on the access point, or *Save to flash and activate* to save them to flash memory and instantly update the access point's active configuration. (You can also save all configuration changes to flash memory from the Configuration Management Commands page.)

**Server Name.** Use this field to enter a symbolic name that can be returned as a parameter of `SNMPv2-MIB::sysName` and `MANGA-POLEPOINT-MIB::apName`.

**SNMPv1, SNMPv2, or SNMPv3.** Check to enable the SNMPv1, SNMPv2, or SNMPv3 agent. The configuration tool lets you configure a mixture of different SNMP versions.

## SNMP v1/v2 Communities area

The SNMPv1/v2 Communities area of the SNMP Server Settings page displays existing SNMP communities and provides commands for editing, deleting, or creating communities.

Clicking **New** after *SNMPv1/v2 Communities* displays the Community page, where you can configure a new SNMPv1 or SNMPv2 community.

Figure 50. SNMPv1/v2 Community page

| Community      |  |
|----------------|--|
| Community Name | <input type="text"/>                                       |
| IP Address     | <input type="text"/>                                       |
| IP Mask        | <input type="text"/>                                       |
| Access Mode    | Read Only ▾  |
| Status         | <input type="radio"/> Enable <input type="radio"/> Disable |

SkyPilot DualBand AP (2.0.15v1)

**Community Name.** Sets the SNMPv1/v2 community name.

**IP Address.** Along with the **IP Mask** field, specifies which IP addresses can access the SNMPv1/v2 agent with this community name. An IP address of 192.168.2.0 with an IP mask of 255.255.255.0 specifies that any IP address in the range 192.168.2.1 to 192.168.2.254 can access the SNMPv1/v2 agent with this community name.

**IP Mask.** See **IP Address**.

**Access Mode.** Sets the community to read-only or read-write access.

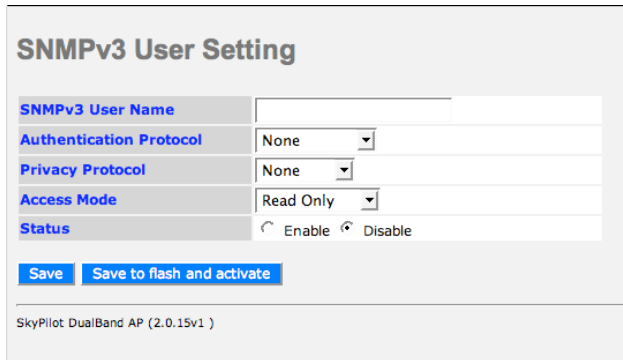
**Status.** Enables or disables the community.

## SNMPv3 Users area

SNMPv3 supports full authentication and encryption of access to the SNMPv3 agent. You can configure multiple SNMPv3 users, each with a unique name, authentication protocol, privacy protocol, and access mode.

Clicking *New* after *SNMPv3 Users* displays the SNMPv3 User Setting page, where you can set the SNMPv3 parameters.

Figure 51. SNMPv3 User Setting page

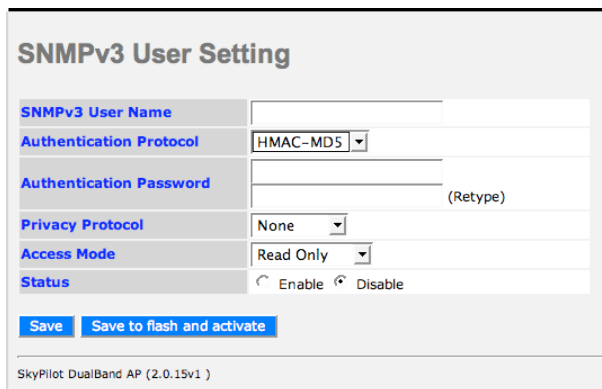


The screenshot shows the 'SNMPv3 User Setting' page. It features a table with the following fields: 'SNMPv3 User Name' (text input), 'Authentication Protocol' (dropdown menu set to 'None'), 'Privacy Protocol' (dropdown menu set to 'None'), 'Access Mode' (dropdown menu set to 'Read Only'), and 'Status' (radio buttons for 'Enable' and 'Disable'). Below the table are two buttons: 'Save' and 'Save to flash and activate'. At the bottom, it says 'SkyPilot DualBand AP (2.0.15v1)'.

*SNMPv3 User Name.* A user name for logging in to the SNMPv3 agent.

*Authentication Protocol.* A choice of *None*, *HMAC-MD5*, or *HMAC-SHA*. If *HMAC-MD5* or *HMAC-SHA* is chosen, two new fields appear that require you to fill in the password used to authenticate the user name.

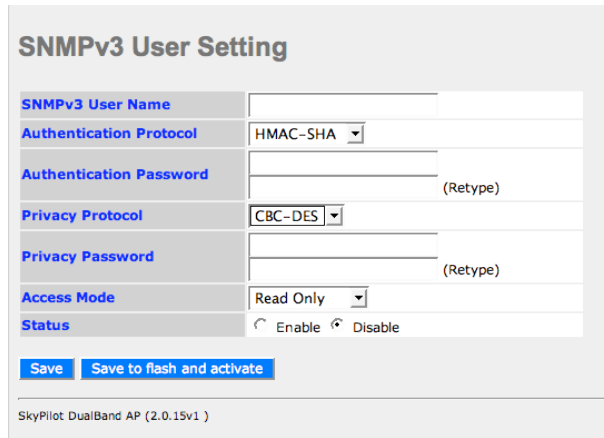
Figure 52. SNMPv3 User Setting page showing authentication password fields



The screenshot shows the 'SNMPv3 User Setting' page with the 'Authentication Protocol' dropdown menu set to 'HMAC-MD5'. This has caused the 'Authentication Password' field to appear, which consists of two text input boxes with '(Retype)' written next to the second one. The other fields ('SNMPv3 User Name', 'Privacy Protocol', 'Access Mode', 'Status') and buttons ('Save', 'Save to flash and activate') are the same as in Figure 51. At the bottom, it says 'SkyPilot DualBand AP (2.0.15v1)'.

*Privacy Protocol.* A choice of *None* or *CBC-DES*. If *CBC-DES* is chosen, two new fields appear that require you to fill in the secret key to be used as input for the DES encryption algorithm.

Figure 53. SNMPv3 User Setting page showing privacy password fields



The image shows a web form titled "SNMPv3 User Setting". The form contains several fields: "SNMPv3 User Name" (text input), "Authentication Protocol" (dropdown menu with "HMAC-SHA" selected), "Authentication Password" (text input with "(Retype)" label), "Privacy Protocol" (dropdown menu with "CBC-DES" selected), "Privacy Password" (text input with "(Retype)" label), "Access Mode" (dropdown menu with "Read Only" selected), and "Status" (radio buttons for "Enable" and "Disable", with "Disable" selected). At the bottom of the form are two buttons: "Save" and "Save to flash and activate". Below the form, the text "SkyPilot DualBand AP (2.0.15v1)" is visible.

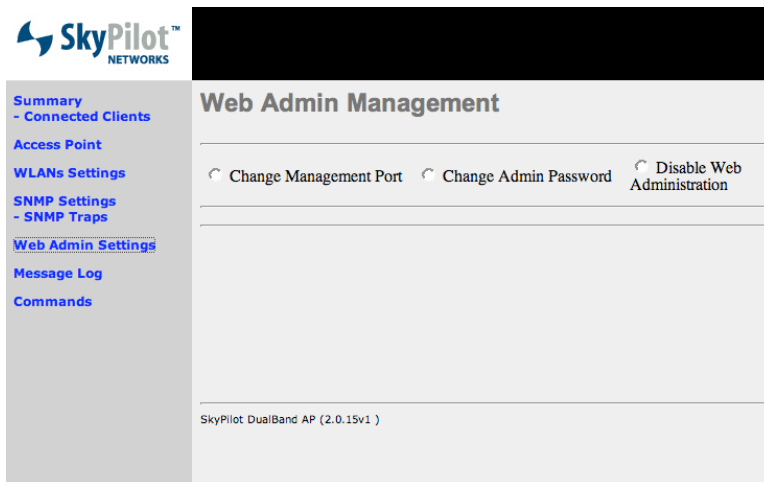
*Access Mode.* Allows this SNMPv3 user to have read-only or read-write access.

*Status.* Enabled or disables this SNMPv3 user.

## Web Admin Management page

Clicking *Web Admin Settings* in the configuration tool navigation bar takes you to the Web Admin Management page. Use this page to view and modify the parameters that control Web access to the configuration tool: management port, user name, and password.

Figure 54. Web Admin Management page



To modify a Web access parameter, click the radio button that corresponds to the parameter you want to change.

After modifying the Web Admin configuration settings, click *Save* to save your changes to volatile RAM on the access point, or *Save to flash and activate* to save them to flash memory and instantly update the access point's active configuration. (You can also save all configuration changes to flash memory from the Configuration Management Commands page.)

***Change Management Port.*** Click this button to assign a new port address for accessing the configuration tool. When this option is selected, a *Port* entry field appears.

Figure 55. Change Management Port

The screenshot shows the 'Web Admin Management' section of a configuration tool. At the top, there are three radio buttons: 'Change Management Port' (which is selected), 'Change Admin Password', and 'Disable Web Administration'. Below this, the 'Change Management Port' section is active, showing a 'Port' input field with the value '443'. There are two buttons: 'Save' and 'Save to flash and activate'. At the bottom left, the text 'SkyPilot DualBand AP (2.0.15v1)' is visible.

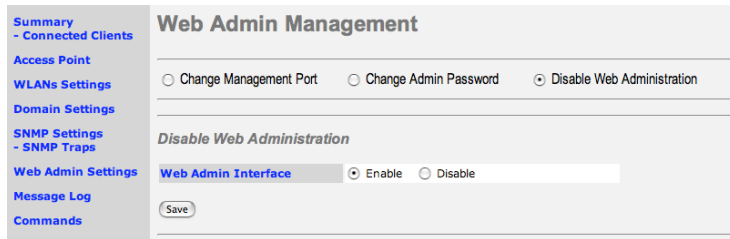
**Change Admin Password.** Click this button to assign a new password for Web access to the configuration tool. When this option is selected, password entry and confirmation fields appear.

Figure 56. Change Admin Password

The screenshot shows the 'Web Admin Management' section of a configuration tool. At the top, there are three radio buttons: 'Change Management Port', 'Change Admin Password' (which is selected), and 'Disable Web Administration'. Below this, the 'Change Admin Password' section is active, showing two input fields: 'New Password' and 'New Password (Retype)'. There are two buttons: 'Save' and 'Save to flash and activate'. At the bottom left, the text 'SkyPilot DualBand AP (2.0.15v1)' is visible.

**Disable/Enable Web Administration.** When this option is selected, radio buttons for disabling or enabling Web access of the configuration tool appear. Click the appropriate button.

Figure 57. Disable Web Administration

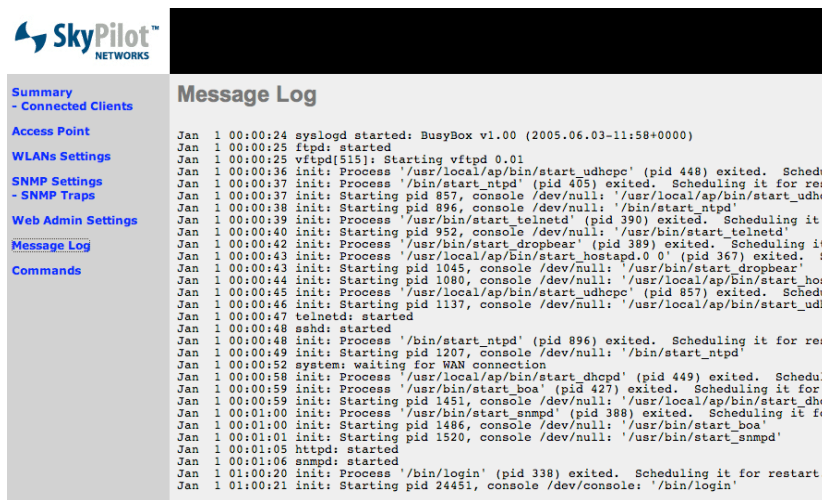


## Message Log page

Clicking *Message Log* in the configuration tool navigation bar takes you to the Message Log page. Use this page to display a log of recent events—a snapshot of the most recent *syslog* output.

The page is updated each time you click *Message Log* in the navigation bar or click the *Reload* button on the page. Figure 58 shows an example.

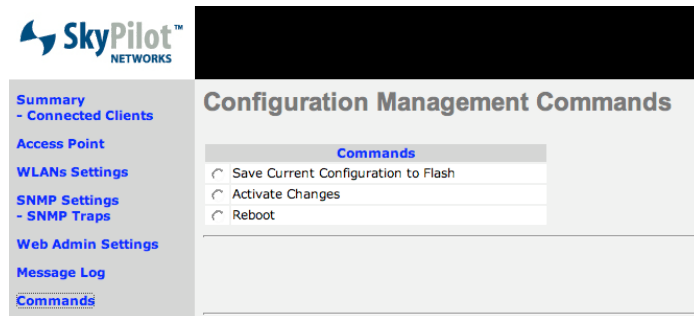
Figure 58. Sample message log (partial)



## Configuration Management Commands page

Clicking *Commands* in the configuration tool navigation bar takes you to the Configuration Management Commands page. Use the commands on this page to save configuration changes to volatile RAM or to activate configuration changes by saving them to flash (nonvolatile) memory. You can also reboot the access point from this page.

Figure 59. Configuration Management Commands page



Choose a command by clicking the corresponding radio button. When a command is chosen, a *Proceed* button appears. When you click *Proceed*, the configuration tool prompts you for confirmation before completing the operation.

**Save Current Configuration to Flash.** Saves changes in the configuration to the access point's flash memory. (The access point won't use the modified configuration until the device reboots or you choose *Activate Changes*.)

**Activate Changes.** Saves configuration changes to flash memory, activating any changes you've made to the configuration.

**NOTE** In some cases, this operation can break 802.1x network connections—for example, if you added or deleted a WLAN.

**Reboot.** Reboots the access point. Upon reboot, the access point loads the configuration file stored in flash memory; any changes that were not saved to flash memory are lost.



## Connecting to the Access Point Command-Line Interface

This appendix describes tells you how to access the command-line interface of the access point in order to troubleshoot the device. Typically, you will use this technique to confirm the IP address of the access point component of the SkyPilot DualBand.

You can connect to the access point command-line interface via Telnet over a wireless network connection. Access to the command-line interface over Ethernet is unavailable because the external Ethernet port on the SkyExtender is available for power transmission only and is unable to handle data traffic.

After logging in to the access point component (by supplying a password), you can enter commands at the command prompt.

### Getting access via a local Wi-Fi connection

You can connect to command-line interface from a computer with a direct Wi-Fi connection to the SkyExtender DualBand access point.

#### 1 Prepare a PC or laptop.

You will need a Wi-Fi/WPA-PSK capable computer that's within operating range of the access point and a Telnet application you can use to open a connections between the devices.

The access point component of SkyExtender DualBand ships with the default IP address *192.168.0.3*.

#### 2 Open the connection to the access point.

From your Telnet application, open a connection to the access point.

- 3** Log in by entering the default user name (*admin*) and password (*public*) at the command prompt.

Once you're logged in, you can use the command-line interface to set configuration parameters or retrieve the IP address of the access point

- 4** Get the IP address of the access point.

Because there are two radios inside the SkyExtender DualBand, you request the IP address of the "B" radio by entering the following command:

```
ifconfig br0
```

Figure 61. Checking "B" radio IP address

```
login: admin
Password:

BusyBox v1.00 (2005.06.03-11:58+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ifconfig br0
br0      Link encap:Ethernet  HWaddr 00:0A:DB:01:30:FE
         inet addr:192.168.2.18  Bcast:192.168.2.255  Mask:255.255.255.0
         BROADCAST MULTICAST  MTU:1504  Metric:1
         RX packets:3 errors:0 dropped:0 overruns:0 frame:0
         TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:225 (225.0 B)  TX bytes:427 (427.0 B)

#
```

This example shows the IP address of the access point (`inet addr`) as 192.168.2.18.

## Manually Updating the Access Point Firmware

This appendix describes how to manually update the firmware in your SkyExtender DualBand access point.

- 1** Use FTP client software to download the firmware image from the SkyPilot FTP site to a host computer.

The image file is available on the FTP site as a binary file that you can identify by the prefix and version number in its name—for example, *SkyAP.2.0.16.bin*.

The image file for the access point is distinct from the binary version of the image file used by the SkyExtender component, which uses a different prefix—for example, *SkyExt.2.0.16.bin*.

- 2** After downloading the binary file, rename it *firmware.img*.

**Note** The access point can load an image file only if it is named *firmware.img*.

- 3** Obtain the IP address of the SkyExtender DualBand access point.

Open an IP connection between the host computer running an FTP client and the SkyExtender DualBand connected to the SkyPilot wireless mesh network.

See Chapter 5, “Using the Access Point Configuration Tool,” for instructions on using an IP connection or Wi-Fi connection to get the IP address of the access point.

#### 4 Upload the image file you renamed *firmware.img*.

FTP to the IP address of the access point and upload the firmware image. Run the FTP client in the same directory as where the firmware image file is currently residing.

**NOTE** Do not turn off power to the access point or otherwise interrupt the updating of the firmware.

The following is an example of a command-line exchange in a firmware update.

```
# ftp 192.168.0.3
Connected to 192.168.0.3
220 Simple FTPd welcomes you.
Name (192.168.0.3:root): root
331 User name okay, need password.
Password: public
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put firmware.img
local: firmware.img remote: firmware.img
500 Syntax error.
227 Entering Passive Mode (192,168,2,18,4,1)
150 Opening data connection.
100% |*****| 3862 KB 544.05
KB/s 00:07
226 Transfer complete.
3955338 bytes sent in 00:07 (529.99 KB/s)
ftp> bye
performing firmware upgrade....
```

Uploading *firmware.img* to the access point via FTP initiates automatic copying of the uploaded file to the access point's flash (nonvolatile) memory.

After several minutes, the flash update completes and the access point automatically reboots.

## Monitoring the firmware update

You can monitor the progress of a firmware update by pinging the access point. Reboot starts when the ping stops. When pinging resumes, the access point is back online.

The configuration file in flash memory is unaffected by the firmware update. After the firmware update is complete, the access point uses the same configuration that was present in its flash memory before the update.

## WLAN Configuration Types

The appendix describes the two WLAN configuration types: open (unprotected) configuration and Wi-Fi protected access (WPA).

### Open configuration

An open configuration allows anyone with Wi-Fi capability to connect to the wireless network via the SkyExtender DualBand access point.

An open configuration doesn't include any mechanism for authenticating users at the network layer. However, you can provide authentication at the application layer through a **captive portal** mechanism operating outside the wireless mesh network. A captive portal forces all HTTP traffic from an unauthenticated user to a login Web page and blocks the traffic until the user successfully logs in to the Web page. (See [http://en.wikipedia.org/wiki/Captive\\_portal](http://en.wikipedia.org/wiki/Captive_portal) for more information on captive portals.)

**NOTE** The configuration of a captive portal for an open WLAN depends on third-party solutions and is outside the scope of this document.

The advantage of an open network configuration is that it makes it very easy for users to connect to the WLAN.

Among the disadvantages of open access are security concerns, since a lack of encryption other than SSL/TLS (available only during login) makes the network vulnerable to unauthorized access and denial-of-service attacks. Additionally, users must start each session from a Web browser before they can use other

Internet applications such as email, SSH, FTP, or chat clients. Open access also makes the network more vulnerable to unauthorized access and malicious actions (including denial-of-service attacks) than WPA-secured networks.

## Wi-Fi protected access (WPA)

Wi-Fi protected access (WPA) is an industry-standard mechanism and protocol that requires users to be authenticated before they can have access to the wireless network. (See [http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) for more information.)

WPA is implemented with:

- A client (called a **supplicant**) in the end-user computer or CPE
- A policing mechanism (called the **authenticator**) in the access point
- A backend database of user names, passwords, and associated policies (called the **authentication server**) which is usually based on Radius

WPA uses the IEEE 802.1x and IETF EAP protocols to allow a client to bootstrap a secure connection with the access point and the Radius server to exchange credentials (*userName@domain/password*) and keys for encryption of all traffic between the client and the access point—even after authentication. WPA still uses WEP for encryption, but it creates keys for each session (not shared with multiple clients) and has mechanisms (TKIP) whereby the keys change all the time, thus eliminating the security issues in the original WEP. For even better encryption, the SkyExtender DualBand can support AES in addition to WEP.

Before you can configure your access point for WPA, you must first configure a Radius server to support:

- The IP address and shared secret of the SkyExtender DualBand access point.
- EAP-PEAP/MSCHAPv2 and EAP-TTLS/PAP or MSCHAPv2 (not EAP-TLS) suitable for WP. Your Radius supplier can provide instructions.
- A Users database with user names, passwords. You may also need to identify a proxy Radius if you're delegating different domains to other service providers.

**NOTE** The configuration of a Radius server for authenticating Wi-Fi users depends on third-party solutions and is outside the scope of this document.