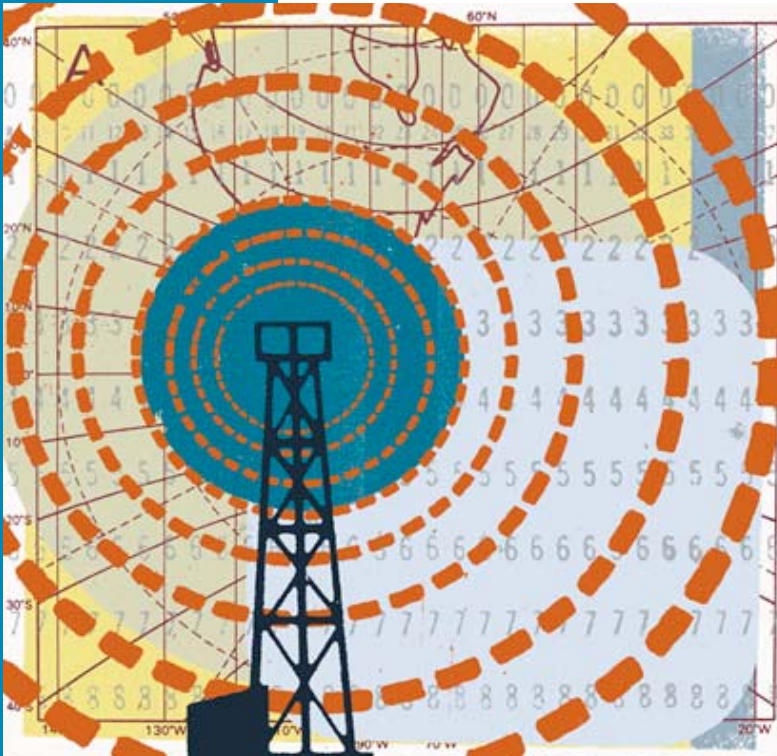


SkyPilot Web Interface Reference



© 2006 SkyPilot Networks, Inc. All rights reserved

This publication, or parts thereof, may not be reproduced in any form, by any method, for any purpose.

Product specifications are subject to change without notice. This material is provided for informational purposes only; SkyPilot assumes no liability related to its use and expressly disclaims any implied warranties of merchantability or fitness for any particular purpose.

SkyPilot Trademarks

SkyConnector, SkyControl, SkyExtender, SkyGateway, SkyPilot, SkyPilot Networks, SkyProvision, and the SkyPilot logo are the trademarks and registered trademarks of SkyPilot Networks, Inc.

Third-Party Trademarks

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

MySQL is a registered trademark of MySQL AB in the United States, the European Union, and other countries.

All other designated trademarks, trade names, logos, and brands are the property of their respective owners.

Third-Party Software Program Credits

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>), licensed under the Apache License.

This product includes the DHCP Server software from Internet Systems Consortium, licensed under the DHCP License. The DHCP Server software is copyright © 2004 Internet Systems Consortium, Inc. ("ISC"). Copyright © 1995–2003 Internet Software Consortium. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of ISC, ISC DHCP, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY INTERNET SYSTEMS CONSORTIUM AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ISC OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes the FTP Server software from vsftpd (<http://vsftpd.beasts.org/>), licensed under the GNU General Public License.

This product includes Java software from Sun Microsystems, licensed under Sun Microsystems' Binary Code License Agreement. Copyright 2003, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

This product includes JBOSS Version 3.2.3 software from JBoss, licensed under the GNU Lesser General Public License. Some bundled products in JBOSS are licensed under the Apache License.

This product contains Java Telnet Application (JTA 2.0).

This product contains the MibBrowser software from Mibble.

This product includes software the copyright of which is owned by and licensed from MySQLAB.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>). Copyright (c) 1998–2005 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)". THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes libraries developed by Eric Young and is licensed under the Original SSLeay License. This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). Copyright (C) 1995–1998 Eric Young (eyay@cryptsoft.com). All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com). The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-). 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)". THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes SNMP software from WestHawk, licensed under the WestHawk License.

This product includes JFreeCharts from <http://www.jfree.org/>, licensed under GNU Lesser General Public License.

This product includes JasperReports from <http://jasperreports.sourceforge.net/index.html>, licensed under GNU Lesser Public License.

GOVERNMENT USE

The following provision applies to United States Government end users. This product is comprised of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212 and are provided to the Government (i) for acquisition by or on behalf of civilian agencies, consistent with the policy set forth in 48 C.F.R. 12.212; or (ii) for acquisition by or on behalf of units of the Department of Defense, consistent with the policies set forth in 48 C.F.R. 227.7202-1 and 227.7202-3.

SkyPilot Firmware 1.4

Document Last Revised: August 22, 2006



Contents

- About This Guide 1**

- About the Web Interface 3**
 - Accessing the Web Interface. 4
 - Logging In to the Web Interface 9

- Using the Web Interface13**
 - Links 14
 - Provisioning 16
 - Password 30
 - Version 31
 - Utilities 33
 - Access Point 34

- About the Access Point Web Interface37**
 - Accessing an Access Point’s Web Interface. 38
 - Logging In to an Access Point’s Web Interface 40
 - Navigating the Access Point Web Interface 42

- Using the Access Point Web Interface43**
 - Summary 44
 - Connected Clients 45
 - Access Point Configuration 46
 - WLANs Settings. 52
 - SNMP Settings. 61
 - SNMP Trap Receivers 66
 - Web Admin Settings. 68
 - Message Log. 70
 - Flash Management. 71
 - Commands. 72



About This Guide

This guide describes the Web interface built in to all SkyPilot™ devices (using SkyPilot firmware version 1.4), and is organized as follows:

- “About the Web Interface” describes the Web interface generally and provides detailed procedures for accessing and logging in to this Web interface.
- “Using the Web Interface” describes how to use the Web interface in administrative mode, including detailed descriptions of the functions you can perform and the device settings you can configure.
- “About the Access Point Web Interface” describes the access point Web interface built in to SkyPilot™ SkyExtender™ DualBand and SkyExtender TriBand access points and provides detailed procedures for accessing and logging in to this Web interface.
- “Using the Access Point Web Interface” describes how to use the access point Web interface, including detailed descriptions of the functions you can perform and the device settings you can configure.



About the Web Interface

A Web-based interface is built into all SkyPilot™ devices. This interface provides much the same functionality as the command-line interface in an easy to use graphical interface.

The following sections briefly describe how to use the Web interface and which provisioning and configuration settings are available through given items in the Web interface's navigation hierarchy. For detailed information about configuration settings and options, particularly how they interrelate, refer to the applicable sections of *SkyPilot Network Administration* and *SkyPilot Command-Line Interface Reference*.

A device's Web interface is enabled or disabled through provisioning. When the interface is enabled, the user functions are enabled, but the administrator functions can still be separately disabled.

When you use the Web interface to make changes to devices' provisioning settings, the changes are made to the configuration stored in flash memory. Therefore, you must reboot the device in order for your changes to take effect.

Section Highlights

- Accessing the Web interface
- Logging in to the Web interface

Accessing the Web Interface

To use the Web interface to monitor and configure a SkyPilot device, you must be able to access the host device via a Web browser.

To access to the Web interface on a SkyPilot device, you need the device's IP address. SkyGateways, SkyConnectors, SkyExtenders, and the SkyExtender portion of DualBands and TriBands ship with a default IP address of 198.168.0.2.

DualBand/TriBand 2.4 GHz antenna access points ship with an IP address of 192.168.0.3, and the TriBand 4.9 GHz antenna access point ships with an IP address of 192.168.0.4. If the device gets its IP address from a DHCP server, you can find the address, which is based on the device's MAC address, in the DHCP server log (the `/var/log/messages` file).

NOTE Even if a SkyPilot device obtains an IP address through DHCP, the device's default IP address is still accessible through the device's Ethernet port or over a Wi-Fi connection.

You can access the Web interface on SkyPilot devices in three ways: through a wired Ethernet connection between the device and a PC, through a remote connection across the SkyPilot mesh network, or (for DualBands and TriBands) through a Wi-Fi connection. See these sections for details:

- "Getting Direct (Wired) Network Access" (the next section)
- "Getting Access via the SkyPilot Mesh Network" on page 7
- "Getting Wi-Fi Access" on page 8

Checking VLAN Status

If your SkyPilot network is configured to use a management VLAN, connected SkyPilot devices automatically use the same VLAN for management traffic.

Therefore, once a SkyPilot device links to the SkyPilot network, you'll need to access the device from a PC that's a member of the management VLAN. Typically this means you'll need to access the Web interface from the SkyPilot EMS server or other management workstation across the SkyPilot mesh network. If you've previously configured the device's data VLAN with the same ID as the

management VLAN, or previously configured a management SSID as a member of the management VLAN, you can use this SSID to connect directly to the device.

Getting Direct (Wired) Network Access

For SkyGateway™ and SkyExtender™ devices (except DualBands), you can access a device's Web interface through a local Ethernet connection. (For DualBands, which don't have an Ethernet connection, you must use a Wi-Fi network connection or connect through the SkyPilot mesh network, as described in the next section.)

To gain direct network access:

- 1 Prepare a PC. To connect to the device's default IP address of 192.168.0.2, you must configure your PC to be a member of the 192.168.0.x subnet.

Open the network settings panel and assign the computer an IP address from 192.168.0.5 to 192.168.0.254, and a subnet mask of 255.255.255.0. (For information about changing a device's IP address from its default, refer to "Managing IP Addresses" in *SkyPilot Network Administration*.)

SkyGateways, SkyConnectors, SkyExtenders, and the SkyExtender portion of DualBands and TriBands ship with a default IP address of 198.168.0.2. DualBand/TriBand 2.4 GHz antenna access points ship with an IP address of 192.168.0.3, and the TriBand 4.9 GHz antenna access point ships with an IP address of 192.168.0.4.

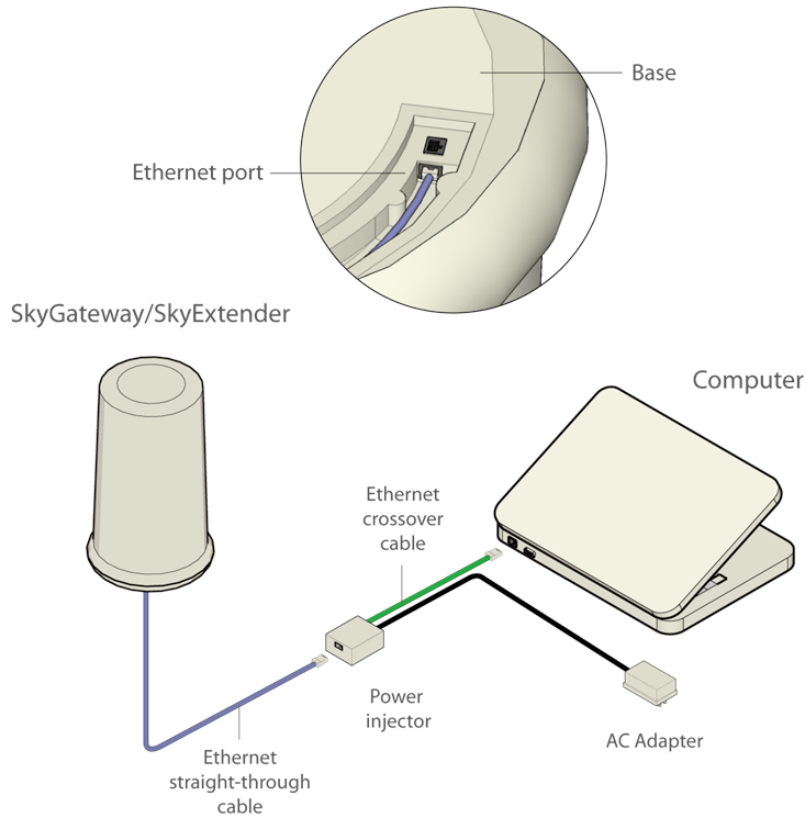
If the device is getting its IP address from a DHCP server, you can find the address, which is based on the device's MAC address, in the DHCP server log (the `/var/log/messages` file).

NOTE Even if a SkyPilot device obtains an IP address through DHCP, the device's default IP address is still accessible through the device's Ethernet port or over a Wi-Fi connection.

- 2 Connect the computer to the SkyPilot device, as shown in Figure 1.
 - a Use an Ethernet crossover cable to connect the computer to the power injector. (For SkyConnectors, a straight through cable can also be used.)

- b** Connect the Ethernet straight-through cable between the power injector and the Ethernet interface on the base of the SkyGateway or SkyExtender.
- c** Plug the AC adapter into the power injector.

Figure 1. Ethernet Connection to a SkyGateway/SkyExtender



- 3** Confirm that you can communicate with the SkyPilot device by pinging its address or the default IP address (192.168.0.2).

If the ping is successful, you're ready to log into the Web interface (see "Logging In to the Web Interface" on page 9).

If the ping is unsuccessful, check your connections and confirm the device's IP address before pinging the device again.

Getting Access via the SkyPilot Mesh Network

You can access any device's Web interface via the SkyPilot wireless mesh network.

To gain access via the SkyPilot mesh network:

- 1 Confirm that the SkyPilot device is configured correctly and connected to the SkyPilot wireless mesh network. The device must be connected to the SkyGateway or to a SkyExtender connected to the SkyGateway.

- 2 Determine the IP address of the device you want to access.

The device's default IP address is not accessible via the mesh network.

If you haven't assigned a static IP address, then the device will use DHCP to automatically obtain an IP address. Determine this IP address as follows:

- a Determine the device's MAC address by looking at the label affixed to the bottom of the device. (For DualBands and TriBands, the label shows two addresses: one for the SkyExtender and one for the access point.)
- b For DualBand 2.4 GHz access points and TriBand 4.9 GHz access points, subtract 1 to get the access point's MAC address.

For TriBand 2.4 GHz access points, subtract 33 to get the access point's MAC address.

For example, if the MAC address of a DualBand is 000ADB01319F (hexadecimal), the reserved addresses start at 000ADB013180 (the difference being 1F hexadecimal, or 31 decimal).

- c Look in the DHCP server log (the `/var/log/messages` file) for the MAC address. The corresponding IP address will be listed and is the address you'll use to connect to the device or access point over the SkyPilot wireless mesh network.

For example:

```
[root@ems_server root]# grep 00:0a:db:01:30:fe /var/log/messages
Apr 14 12:05:28 dansems dhcpd: DHCPDISCOVER from 00:0a:db:01:30:fe
via eth0
Apr 14 12:05:28 dansems dhcpd: DHCPOFFER on 10.12.14.12 to
00:0a:db:01:30:fe via eth0
Apr 14 12:05:28 dansems dhcpd: DHCPREQUEST for 10.12.14.12
(10.12.14.1) from 00:0a:db:01:30:fe via eth0
Apr 14 12:05:28 dansems dhcpd: DHCPACK on 10.12.14.12 to
00:0a:db:01:30:fe via eth0
```

NOTE You can also configure the DHCP server to provide a specific IP address based on the MAC address of the access point (from step **2b**).

- 3** Confirm that you can communicate with the SkyPilot device by pinging the address you identified in step **2**.

If the ping is successful, you're ready to log into the Web interface (see the next section).

If the ping is unsuccessful, check your connections and confirm the device's IP address before pinging the device again.

Getting Wi-Fi Access

An alternative method for managing a DualBand/TriBand access point is from a computer with a direct Wi-Fi connection to the access point.

To connect to the access point through a Wi-Fi connection, you need a computer that's capable of Wi-Fi communication and that's within operating range of the access point, as well as a Web browser application.

NOTE The DualBand/TriBand doesn't have to be connected to a SkyPilot mesh network while you're configuring it for access point operations.

To gain direct Wi-Fi network access:

- 1** Set up your host computer's 802.11b/g interface to connect to the access point's default SSID: a string representation of the DualBand/TriBand MAC address (which can be found on the unit's label), without the colon characters.

The default WLAN uses a Wi-Fi Protected Access-Pre-Shared Key (WPA-PSK) protection scheme that uses a public key (password) of `publicpublic` to control access. You are 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:

Enter the IP address 192.168.0.5 and netmask 255.255.255.0 and apply the setting.

- 3** Confirm that your computer can communicate with the access point by pinging its IP address: 192.168.0.3 for DualBand/TriBand 2.4 GHz access point,

192.168.0.4 for TriBand 4.9 GHz. (This is same IP address you use to log into the access point's Web interface.)

If the ping is successful, you're ready to log into the access point's Web interface (see the next section).

Logging In to the Web Interface

You can log into the Web interface in view-only mode, which displays current information about the device, or in administrator mode, which allows you to enter and modify configuration settings for the device.

To log in to the Web interface in administrator mode, you need a user name and password in addition to the device's IP address.

To log in to the Web interface in view-only mode:

- Open a Web browser and enter the URL for the SkyPilot device (its IP address); for example, `http://192.168.0.2/`.

NOTE In order to view the Web interface, the Web interface server must be configured so that its End-User Page is enabled (see "Configuring Web Servers" in *SkyPilot Network Administration* or the `set prov web` command in the *SkyPilot Command-Line Interface Reference*).

The Web interface displays the Node Details screen (Figure 2), which is the only screen available in view-only mode.

Figure 2. Node Details screen

SkyPilot Networks™ CARRIER-CLASS MULTI-SERVICE WIRELESS NETWORKING

Node Details

Device Type : SkyGateway **Current Software** : 1.3
System Mac : 00:0a:db:01:06:b5 **Active Image & State** : SkyGate.1.3beta2.bin/Accepted
IP Address : 192.168.5.225 **Inactive Image & State** : linkerDynModGate_b/Accepted
Subnet Mask : 255.255.255.0 **Uptime** : 4 days 08:09:45
Default Gateway : 192.168.5.1 **Domain** : 16
Provisioning Mode : Auto **Current Frequency** : 5825
Status : Online **Allowed Frequencies** : 5805 5825

Link Info

Show Active links only. Show Inactive links also.

Address	LType	NType	State	LRSSI	RRSSI	LTxMod	RTxMod	Lant	Rant
00:0a:db:00:00:27	data	Extender	standby-o	25	9	24	24	1	2
00:0a:db:00:00:4e	data	Extender	standby-h	22	13	9	12	1	3
00:0a:db:00:00:90	data	Extender	standby-o	26	0	24	24	0	4
00:0a:db:00:00:9f	data	Extender	act mgmt	23	27	36	36	0	4
00:0a:db:01:06:b8	data	CPE-Outdoor	act mgmt	21	18	24	24	0	0
00:0a:db:01:0a:59	data	Extender	act mgmt	23	27	36	24	1	6
00:0a:db:01:0a:60	data	Extender	act mgmt	28	35	36	36	1	5

© SkyPilot Networks Inc.

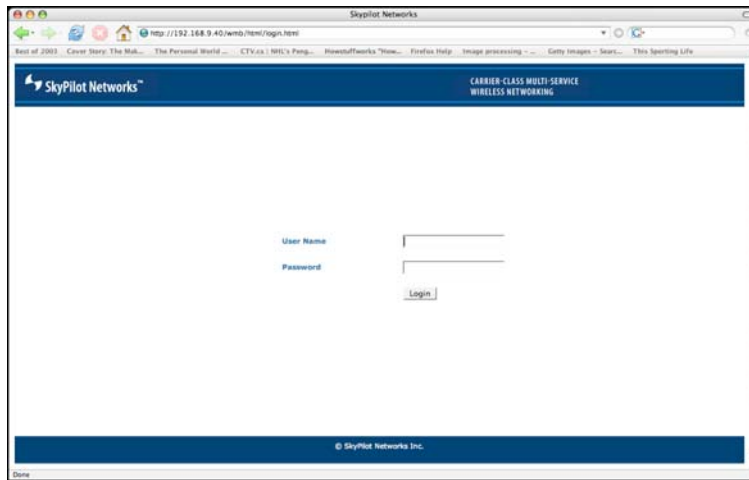
To log in to the Web interface in administrator mode:

- 1 Open a Web browser and enter the URL for the SkyPilot device’s login page: the device’s IP address followed by /admin; for example, `http://192.168.0.2/admin`.

NOTE In order to log in to the Web interface in administrator mode, the Web interface server must be configured so that its WebServer is enabled (see “Configuring Web Servers” in *SkyPilot Network Administration* or the `set prov web` command in the *SkyPilot Command-Line Interface Reference*).

The Web interface displays a login screen (Figure 3).

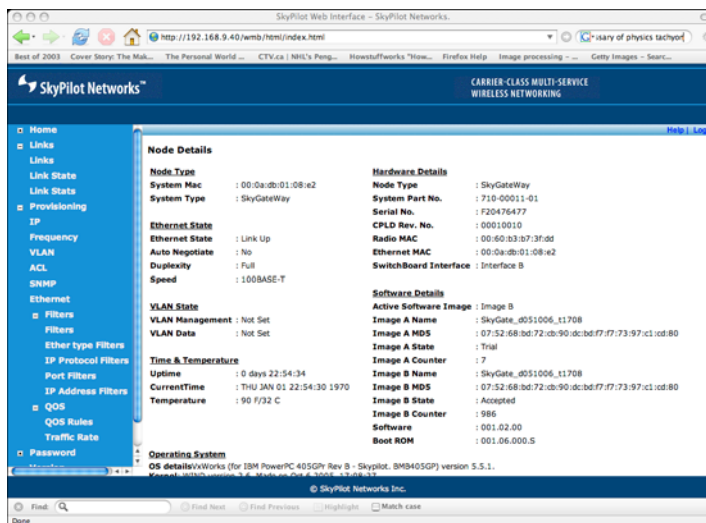
Figure 3. Login screen



- 2 Enter the user name and password. The default user name is `admin`, and the default password is `public`.
- 3 Click **Login**.

The Web interface displays a Node Details screen that shows detailed information about the SkyPilot device you're accessing. There's also a navigation pane on the left, which contains a Windows Explorer-like hierarchy for navigating around in the Web interface, as described in detail in the next section.

Figure 4. Node Details screen





Using the Web Interface

This section describes how to use the Web interface in administrative mode. The top-level items in the navigation hierarchy are as follows:

- Links
- Provisioning
- Password
- Version
- Utilities
- Access Point

A notation like **Provisioning ► IP** in this section refers (in this case) to the **IP** entry below **Provisioning** in the navigation hierarchy.

Links

You can use the items below **Links** in the navigation hierarchy to view information about the network links that the SkyPilot device forms with other devices on the wireless mesh network. This information is useful for confirming wireless mesh operations and for troubleshooting.

NOTE The Links functions are for monitoring only; they do not provide any configuration modification options. For a list of possible link states, refer to “Monitoring Link States” in *SkyPilot Network Administration*.

Links > Links

Use this navigation path to display a summary of link states established by the SkyPilot node.

To view a summary of link states:

- 1 In the navigation pane, expand the **Links** tree.
- 2 Click **Links**.
For each link, the Web interface displays the MAC address, link type, node type, RSSI, and other information related to radio antenna operations.

Links > Link State

Use this navigation path to display details about link states established by the SkyPilot node.

To view details about link states:

- 1 In the navigation pane, expand the **Links** tree.
- 2 Click **Link State**.
For each link, the Web interface displays the link state summary information: modulation, power, gain, and other information related to radio antenna operations.

Links ► Link Stats

Use this navigation path to display detailed statistical information about a device's active links.

To view statistics about active links:

1 In the navigation pane, expand the **Links** tree.

2 Click **Link Stats**.

For each link, the Web interface displays detailed statistical information, including transmit and receive packets, transmit and receive bytes, and retries.

Provisioning

You can use the items below **Provisioning** in the navigation hierarchy to view and modify the configuration stored in a device's flash memory. (Any changes you make will not take effect until the device is restarted.)

Provisioning > Prov Mode

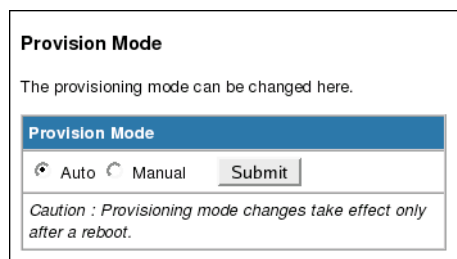
Use this navigation path to configure the device's provisioning mode: automatic or manual. Any change you make doesn't take effect until the device is restarted.

To configure a device's provisioning mode:

- 1 In the navigation pane, expand the **Provisioning** tree.
- 2 Click **Prov Mode**.

The Web interface displays the following screen.

Figure 5. Provisioning mode configuration page



The screenshot shows a web interface titled "Provision Mode". Below the title, it says "The provisioning mode can be changed here." There is a blue header bar with "Provision Mode" written on it. Below the header bar, there are two radio buttons: "Auto" (which is selected) and "Manual". To the right of the radio buttons is a "Submit" button. Below the form, there is a caution message: "Caution : Provisioning mode changes take effect only after a reboot."

- 3 Select **Auto** or **Manual** and click **Submit**.

A confirmation message is displayed.

- 4 Click **OK**.

Provisioning > IP

Use this navigation path to configure the device's static IP settings: IP address, subnet mask, and gateway.

To configure a device's IP settings:

1 In the navigation pane, expand the **Provisioning** tree.

2 Click **IP**.

The Web interface displays the following screen.

Figure 6. IP configuration page

Network

You can configure your **static IP Address** using this page

Please mention the Subnet mask and also the Default gateway. This setting will be stored and is maintained across reboots.

The existing values are popped up. Please make necessary changes and **SUBMIT** after checking.

Enter a new **IP Address**:

Enter a new **Subnet Mask**:

Enter a new **Gateway**:

Caution : IP changes take effect only after a reboot.

3 Enter settings for the configuration items you want to modify.

4 Click **Submit**.

A confirmation message is displayed.

5 Click **OK**.

Provisioning > Frequency

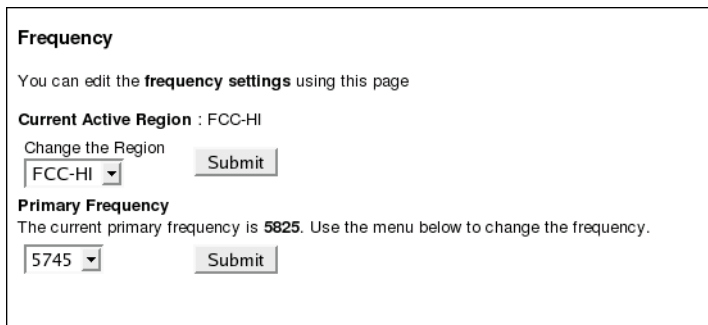
Use this navigation path to configure the device's frequency settings. (Refer to "Frequency" in *SkyPilot Network Administration*.)

To configure frequency settings:

- 1 In the navigation pane, expand the **Provisioning** tree.
- 2 Click **Frequency**.

For SkyGateways, the Web interface displays Figure 7; for all other devices, the Web Interface displays Figure 8.

Figure 7. SkyGateway Frequency configuration page



Frequency

You can edit the **frequency settings** using this page

Current Active Region : FCC-HI

Change the Region

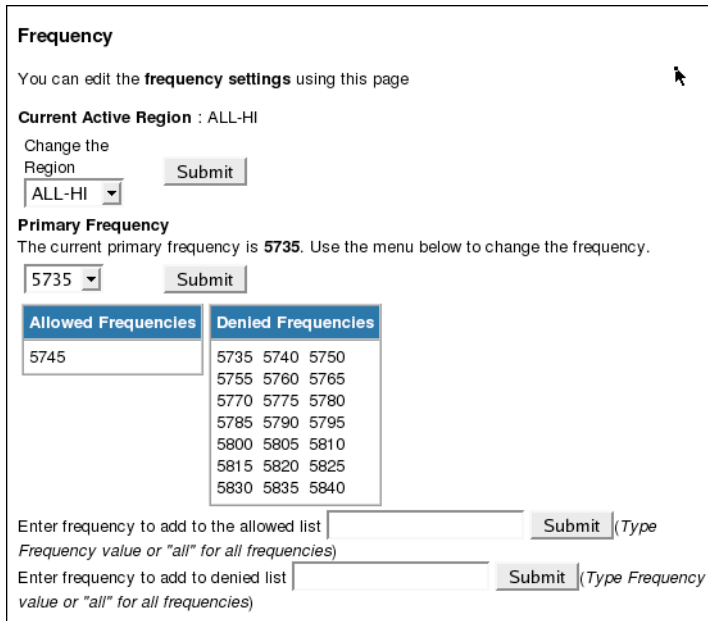
FCC-HI

Primary Frequency

The current primary frequency is **5825**. Use the menu below to change the frequency.

5745

Figure 8. Non-SkyGateway frequency configuration page



Frequency

You can edit the **frequency settings** using this page

Current Active Region : ALL-HI

Change the Region

ALL-HI

Primary Frequency

The current primary frequency is **5735**. Use the menu below to change the frequency.

5735

Allowed Frequencies	Denied Frequencies
5745	5735 5740 5750 5755 5760 5765 5770 5775 5780 5785 5790 5795 5800 5805 5810 5815 5820 5825 5830 5835 5840

Enter frequency to add to the allowed list (Type Frequency value or "all" for all frequencies)

Enter frequency to add to denied list (Type Frequency value or "all" for all frequencies)

- 3 Enter settings for the configuration items you want to modify.

NOTE If you're changing the frequency region, the device must be restarted before you can change its primary frequency.

- 4 Click **Submit**.

A confirmation message is displayed.

- 5 Click **OK**.

Provisioning > VLAN

Use this navigation path to enable or disable VLANs and to specify the VLAN you want to use with the SkyPilot device. (Refer to "Virtual Local Area Networks (VLANs)" in *SkyPilot Network Administration*.)

To configure VLAN settings:

- 1 In the navigation pane, expand the **Provisioning** tree.

- 2 Click **VLAN**.

For SkyGateways, the Web interface displays Figure 9; for all other devices, the Web interface displays Figure 10.

Figure 9. SkyGateway VLAN configuration page

Virtual LAN

All the VLAN settings can be made here.

The existing values are popped up. Please make necessary changes and **SUBMIT** after checking.

Management VLAN :
 Enabled Disabled

Enter VLAN ID (1-4096 or Untagged)
VLAN ID :
 Untagged

P2P

VLAN P2P Enabled IDs are :

Enter VLAN P2P ID (1-4096 or Untagged)
Add
 Untagged

Delete

Caution : If VLAN is enabled you may lose the connection

Figure 10. Non-SkyGateway VLAN configuration page

Virtual LAN

All the VLAN settings can be made here.

The existing values are popped up. Please make necessary changes and **SUBMIT** after checking.

Management VLAN is set at the Gateway and not configurable on non-Gateway devices

Management VLAN ID : Untagged

Data VLAN :
 Enabled Disabled

Enter VLAN ID (1-4096 or Untagged)
VLAN ID :
 Untagged

Caution : If VLAN is enabled you may lose the connection

- 3 Enter settings for the configuration items you want to modify.
- 4 Click **Submit**.
A confirmation message is displayed.
- 5 Click **OK**.

Provisioning > ACL

Use this navigation path to configure access control lists. (For information about ACLs, refer to “Access Control Lists (ACLs)” in *SkyPilot Network Administration*.)

To configure ACL settings:

- 1 In the navigation pane, expand the **Provisioning** tree.
- 2 Click **ACL**.

The Web interface displays the following screen.

Figure 11. ACL configuration page

ACL Settings

Access Control List is displayed here. Addition to the list can be made here.

Existing Access Control List

Index	IP Address	Subnet Mask	Port	Protocol
None.				

Enter the index of ACL to be deleted

Enter the parameters to add a new Access Control

Access Control IP

Access Control SubNet Mask

Access Control Port Number

Access Control Protocol

- 3 Enter settings for the configuration items you want to modify.
- 4 Click **Submit**.
A confirmation message is displayed.
- 5 Click **OK**.

Provisioning > SNMP

Use this navigation path to configure SNMP for your SkyPilot devices. For information about SkyPilot SNMP, refer to “SNMP” in *SkyPilot Network Administration*. For information about using SkyControl, refer to “Monitoring a Network’s Topology with SkyControl” in *SkyPilot Network Administration*.

To configure SNMP settings:

- 1** In the navigation pane, expand the **Provisioning** tree.

- 2** Click **SNMP**.

The Web interface displays the SNMP Configuration screen (Figure 12).

Figure 12. SNMP configuration page

SNMP Settings

All the SNMP settings can be made here.

The existing values are popped up. Please make necessary changes and **SUBMIT** after checking.

SNMP State

Read-Write Read-Only Disabled

Existing snmp Read/Write Community Strings

None.

Add a Read-Write string

Check the box to clear the R-W Community String list.

Existing snmp ReadOnly Community Strings

None.

Add a Read-Only string

Check the box to clear the R-O Community String list

Existing Trap List

Index	IP Address	Port
None.		

Add a trap server IP

Port Number

Enter the index of the Trap server ip to be deleted

- 3 Enter settings for the configuration items you want to modify.
- 4 Click **Submit**.
A confirmation message is displayed.
- 5 Click **OK**.

Provisioning > Ethernet

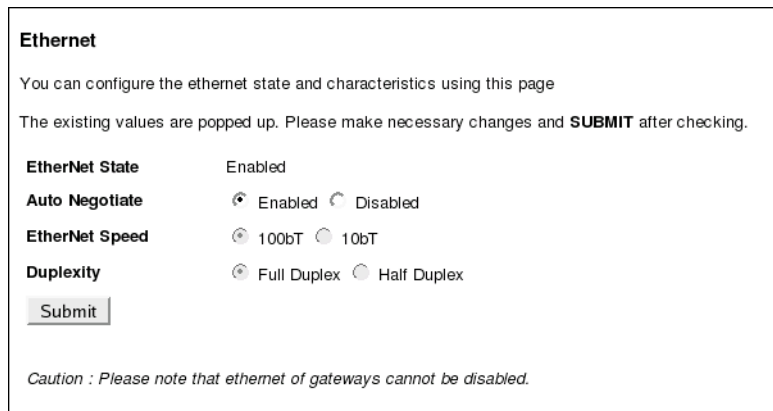
Use this navigation path to configure the Ethernet interface's state and characteristics. (Refer to "Ethernet Interface" in *SkyPilot Network Administration*.)

To configure Ethernet interface settings:

- 1 In the navigation pane, expand the **Provisioning** tree.
- 2 Click **Ethernet**.

For SkyGateways, the Web interface displays Figure 13; for all other devices, the Web interface displays Figure 10.

Figure 13. SkyGateway Ethernet interface configuration page



Ethernet

You can configure the ethernet state and characteristics using this page

The existing values are popped up. Please make necessary changes and **SUBMIT** after checking.

EtherNet State Enabled

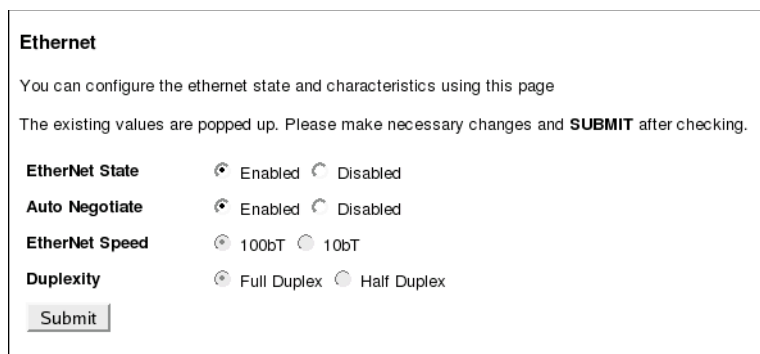
Auto Negotiate Enabled Disabled

EtherNet Speed 100bT 10bT

Duplexity Full Duplex Half Duplex

Caution : Please note that ethernet of gateways cannot be disabled.

Figure 14. Non-SkyGateway Ethernet interface configuration page



Ethernet

You can configure the ethernet state and characteristics using this page

The existing values are popped up. Please make necessary changes and **SUBMIT** after checking.

EtherNet State Enabled Disabled

Auto Negotiate Enabled Disabled

EtherNet Speed 100bT 10bT

Duplexity Full Duplex Half Duplex

- 3 Enter settings for the configuration items you want to modify.

NOTE The SkyGateway Ethernet interface cannot be disabled. Ethernet speed and duplexity can be configured only when autonegotiate is disabled.

- 4 Click **Submit**.

A confirmation message is displayed.

- 5 Click **OK**.

Provisioning > Filters

Use this navigation path to set global and individual permissions for any existing filters. (Refer to “Filtering” in the *SkyPilot Network Administration*.)

To configure filter permissions:

- 1 In the navigation pane, expand the **Provisioning** tree, and then the **Filters** tree.

- 2 Click **Filters**.

The Web interface displays the following screen.

Figure 15. Filters configuration page

Filter

Default Filter Permissions	
Filter Type	Status
Global Filter	OFF
Ether Filter	ON
IP Filter	ON
IP AddrSrc Filter	ON
IP AddrDest Filter	ON
UDPSrc Port Filter	ON
UDPDest Port Filter	ON
TCPsrc Port Filter	ON
TCPDest Port Filter	ON
ARPSrc IP Filter	ON

Set Global Default Permission

Deny

Set Individual Filter Permissions

EtherType

- 3 Enter settings for the configuration items you want to modify.

- 4 Click **Submit**.

A confirmation message is displayed.

- 5 Click **OK**.

To add or delete individual filters:

- 1 In the navigation pane, expand the **Provisioning** tree and then the **Filters** tree.

- 2 Click the desired filter type—for example, **EtherType Filters**.

The Web interface displays the screen for that type of filter, as shown for Ethernet filters in the example below.

Figure 16. Individual filter configuration page

The screenshot shows a web interface for configuring EtherType Filters. At the top, there is a table with columns for Index, Type, Value, and Permission. The table contains one row with the value 'None.' Below the table, there is a section titled 'Enter Index of the EtherFilter to delete' with a text input field and a 'Submit' button. Below that, there is a section titled 'Add EtherFilter' with a 'Protocol' dropdown menu set to 'ARP', a 'Permission' dropdown menu set to 'Allow', and a 'Submit' button.

- 3 To delete a filter, enter its index. To add a filter, select the desired options from the lists.

- 4 Click **Submit**.

A confirmation message is displayed.

- 5 Click **OK**.

Provisioning > QoS

You can use the items below **QoS** in the navigation hierarchy to configure traffic rate controls and traffic rate rules for your SkyPilot network. (Refer to “Quality of Service (QoS)” in the *SkyPilot Network Administration*.)

Provisioning > QoS > QoS Rules

Use this navigation path to configure traffic rate rules for non-SkyGateway devices.

To add or delete individual traffic rate controls:

- 1** In the navigation pane, expand the **Provisioning** tree, and then the **QoS** tree.
- 2** Click **QoS Rules**.

The Web interface displays the Individual Traffic Rate Control screen (Figure 17).

Figure 17. Individual traffic rate control (QoS rules) configuration page

QOS

Direction : IP TOS Low :

IP TOS High : IP TOS Mask :

Protocol : Source IP Address :

Source IP Mask : Destination IP Address :

Destination IP Mask : TCP/UDP Source Port Start :

TCP/UDP Source Port End : TCP/UDP Destination Port Start :

TCP/UDP Destination Port End : Src MAC Address :

Src MAC Mask : Dest MAC Address :

Dest MAC Mask : Ethernet Protocol :

802.1Q VLAN ID : 801.1P User Priority Low :

IEEE 801.1P User Priority High :

QOS List

The Table below lists all the QOS entries

Rule	TOS Low	TOS High	TOS Mask	IP Protocol	IP Src Addr	IP Src Mask	IP Dest Addr	IP
None.								

Enter a Rule No. to delete:

3 To add a traffic rate control (QoS rule), select the desired options from the lists. To delete a traffic rate control (QoS rule), enter its index.

4 Click **Submit**.

A confirmation message is displayed.

5 Click **OK**.

Provisioning ► QoS ► Traffic Rate

Use this navigation path to global traffic rate controls for your SkyPilot network.
(Refer to “Quality of Service (QoS)” in the *SkyPilot Network Administration*.)

To configure traffic rate controls:

- 1 In the navigation pane, expand the **Provisioning** tree, and then the **QoS** tree.
- 2 Click **Traffic Rate**.

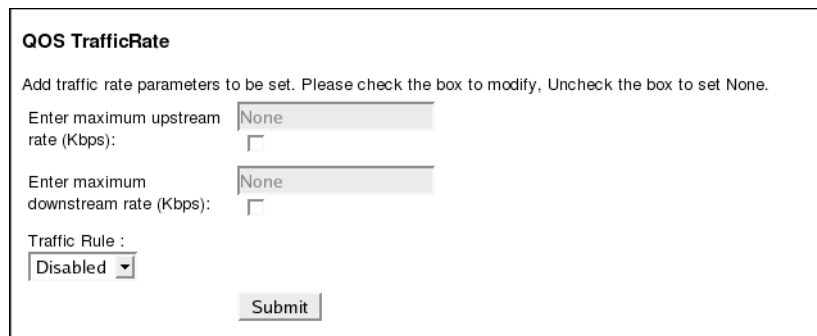
For SkyGateways, the Web interface displays Figure 18; for all other devices, the Web interface displays Figure 10.

Figure 18. SkyGateway traffic rate controls configuration page



The screenshot shows a web interface titled "QOS TrafficRate". Below the title is a line of text: "Add traffic rate parameters to be set. Please check the box to modify, Uncheck the box to set None." There are two input fields: "Enter maximum broadcast rate (Kbps):" with a text box containing "None" and a checkbox to its right, and "Traffic Rule :" with a dropdown menu showing "Disabled". At the bottom center is a "Submit" button.

Figure 19. Non-SkyGateway traffic rate controls configuration page



The screenshot shows a web interface titled "QOS TrafficRate". Below the title is a line of text: "Add traffic rate parameters to be set. Please check the box to modify, Uncheck the box to set None." There are two input fields: "Enter maximum upstream rate (Kbps):" with a text box containing "None" and a checkbox to its right, and "Enter maximum downstream rate (Kbps):" with a text box containing "None" and a checkbox to its right. Below these is "Traffic Rule :" with a dropdown menu showing "Disabled". At the bottom center is a "Submit" button.

- 3 Enter the desired rate controls and choose **Enabled** or **Disabled** from the Traffic Rule list.
- 4 Click **Submit**.
A confirmation message is displayed.
- 5 Click **OK**.

Password

You can use the **Password** entry in the navigation pane to change the password to be used when logging in to the device's Web interface in administrative mode.

To change the device's Web interface administrative-mode password:

- 1 In the navigation pane, click **Password**.

The Web interface displays the Password Settings screen.

Figure 20. Password Settings configuration screen

Password Settings

You can configure your **WebSever Password for admin page** using this page

Enter the **User Name** admin

Enter the **Password**

Re - Enter the **Password**

You can configure your **WebSever Password for enduser page** using this page

Enter the **User Name** guest

Enter the **Password**

Re - Enter the **Password**

- 2 Enter the new password (twice) in the **WebServer Password for admin page** section (near the top of the screen).

- 3 Click **Submit**.

A confirmation message is displayed.

- 4 Click **OK**.

The new password will take effect the next time you access the device's Web Interface.

Version

You can use the items below **Version** in the navigation hierarchy to view the versions of hardware and software on a device, to add software images to a device, and to specify which partition is the active partition. Refer to “Managing Software Images” in *SkyPilot Network Administration*.

Version > **Version HW**

Use this navigation path to display the device’s hardware properties.

To view the device’s hardware properties:

- 1** In the navigation pane, expand the **Version** tree.
- 2** Click **Version HW**.

The Web interface displays the device’s type (SkyGateway, SkyConnector, and so on), part numbers, and addresses.

Version > **Version SW**

Use this navigation path to display the device’s software properties.

To view the device’s software properties:

- 1** In the navigation pane, expand the **Version** tree.
- 2** Click **Version SW**.

The Web interface displays the device’s software properties: information about the software in each partition, which partition is active, and the corresponding software’s state (such as `accepted`).

Version ► Update Image

Use this navigation path to download a software image to the device and to change which partition is the active partition.

To perform image update operations:

- 1 In the navigation pane, expand the **Version** tree.
- 2 Click **Update Image**.

The Web interface displays the following screen.

Figure 21. Image updating page

Image Update

The image currently running in this system can be updated using this page. Please enter the required fields and submit. The image will be taken from the FTP site mentioned and will update the image on the mentioned partition.

Please observe the result below after the image update is done.

Enter the **Ftp Server IP Address**

Enter the **FTP Server UserName**

Enter the **FTP Server Password**

Enter the **Directory Path**

Enter the **FileName**

Enter the **Destination partition**

Set the **Active partition**

Caution : The FTP process may take some time

- 3 To download a software image, enter the server information and make a selection from the destination partition list. To change the active partition, make a selection from the active partition list.
- 4 Click **Submit**.
A confirmation message is displayed.
- 5 Click **OK**.

Utilities

The items below **Utilities** in the navigation hierarchy provide tools to help you with troubleshooting and maintenance tasks:

- **Ping**—Layer 3 ping utility
- **Node test**—Two-way link layer ping test
- **Reboot**—Device reboot
- **Traceroute**—Path trace from the local node to the destination MAC address

To use a SkyPilot utility:

- 1** In the navigation pane, expand the **Utilities** tree.
- 2** Click the link corresponding to the desired task.
The Web interface displays the corresponding utility screen.
- 3** Enter any required information.
- 4** Click **Submit** or **Reboot** (as applicable).

Access Point

The items below **Access Point** in the navigation hierarchy provide tools to make changes to DualBand or TriBand access point parameter values for manually provisioned devices.

- **2.4 GHz Access Point**—Access point interface for a DualBand/TriBand 2.4 GHz antenna
- **4.9 GHz Access Point**—Access point interface for a TriBand 4.9 GHz antenna

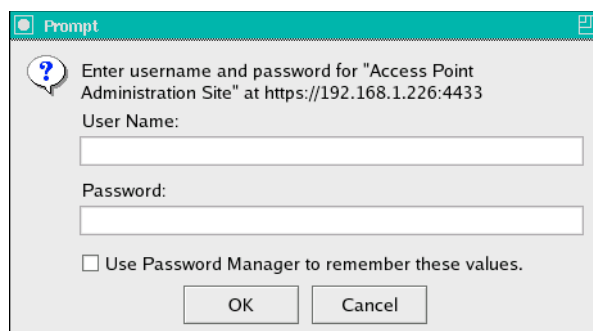
To access a access point's Web interface:

- 1 In the navigation pane, expand the **Access Point** tree and click the link corresponding to the desired antenna.

Depending on your browser settings and whether this is a new browser session, a dialog may appear asking you to confirm certificate authority for the Web address. Click **OK** to proceed.

A new window opens automatically, and for new browser sessions, the Web interface displays the Access Point Login screen. For existing browser sessions, the interface skips the login process (the next step) and immediately displays the Summary screen (Figure 23).

Figure 22. Access Point Login screen



- 2 Enter the user name and password. The default user name is `admin`, and the default password is `public`.
- 3 Click **OK**.

The access point Web interface displays the Summary screen, which shows detailed information about the access point.

Figure 23. Access point summary page

Summary	
AP Name	00:0A:DB:01:2F:BE
Network IP Address	192.168.2.20
Software Version	2.0.21b10e5
Serial Number	182E-BAFE-38A0
Firmware Image Name	SkyAP.2.0.21b10e5.bin
Up Time	1 days, 07:01:36
System Time	Fri Jan 2 07:01:36 1970
Number of WLANs	8
Location	DogFood
Current Clients	8

SkyPilot DualBand AP (2.0.21b10e5)

Once you've successfully accessed the Web interface, you can configure the access point for Wi-Fi operation. For details, see "Using the Access Point Web Interface" on page 43.

- 4 When you're finished using the access point's Web interface, close the window.

NOTE If you expand the **Access Point** tree and click the link corresponding to an antenna before closing an existing access point's Web interface window, an additional window opens. This is not a problem; you can use multiple Web interfaces concurrently.



About the Access Point Web Interface

A Web-based interface is built into SkyPilot™ SkyExtender™ DualBand/TriBand access points.

The following sections briefly describe how to use an access point's Web Interface and which provisioning and configuration settings are available through given items in the Web interface's navigation hierarchy. For detailed information about configuration settings and options, particularly how they interrelate, refer to the applicable sections of the *SkyPilot Network Administration*.

When you use the Web interface to make changes to DualBand or TriBand access point parameter values, you can save the changes to the configuration stored in flash memory and optionally activate those changes immediately.

Section Highlights

- Accessing the access point Web interface
- Logging in to the access point Web interface
- Navigating the access point Web interface

Accessing an Access Point's Web Interface

The easiest way to use an access point's Web interface is to access it via the DualBand/TriBand SkyExtender portion's Web interface (see "Access Point" on page 34). If you use this method, you can skip the remainder of this section and go directly to "Using the Access Point Web Interface" on page 43.

Alternatively, you can access an access point's Web interface directly via a Web browser, either through the SkyPilot wireless mesh network or (for configured devices) a direct Wi-Fi connection. Details are provided in the following sections:

- "Getting Access via the SkyExtender on the Network" on page 38
- "Getting Direct Wi-Fi Network Access" on page 39

Before you use either procedure to access the access point's Web interface, you must first check the VLAN status, as described in the next section.

Checking VLAN Status

If your SkyPilot network is configured to use a management VLAN, the access point automatically uses the same VLAN for management traffic. Therefore, you'll need to access the access point from a PC that's a member of that management VLAN. Typically this means you'll need to access the Web interface from the SkyPilot EMS server or other management workstation across the SkyPilot mesh network. If you've previously configured a management SSID as a member of the management VLAN, you can use this SSID to connect directly to the access point.

Getting Access via the SkyExtender on the Network

To use the access point's Web interface from the network, verify that the SkyExtender component of the DualBand or TriBand has established a wireless

connection with the SkyGateway or with another SkyExtender connected to the SkyGateway.

To gain access via the SkyExtender DualBand/TriBand:

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

One method you can use is to ping the IP address of the SkyExtender DualBand/TriBand.

- 2 Confirm that you can communicate with the access point by pinging its address (for DualBand/TriBand 2.4 GHz access points, 192.168.0.3; for TriBand 4.9 GHz access points, 192.168.0.4).

If the ping is successful, you're ready to log into the access point Web interface (see "Logging In to an Access Point's Web Interface" on page 40).

If a VLAN is in use on your network, see "Checking VLAN Status" on page 38.

Getting Direct Wi-Fi Network Access

An alternative method for managing a DualBand/TriBand access point is from a computer with a direct Wi-Fi connection to the access point.

To connect to the access point through a Wi-Fi connection, you need a computer that's capable of Wi-Fi communication and that's within operating range of the access point, as well as a Web browser application.

NOTE The DualBand/TriBand doesn't have to be connected to a SkyPilot mesh network while you're configuring it for access point operations.

To gain direct Wi-Fi network access:

- 1 Set up your host computer's 802.11b/g interface to connect to the access point's default SSID: a string representation of the DualBand/TriBand MAC address (which can be found on the unit's label), without the colon characters.

The default WLAN uses a Wi-Fi Protected Access-Pre-Shared Key (WPA-PSK) protection scheme that uses a public key (password) of `publicpublic` to control access. You are 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:

Enter the IP address 192.168.0.5 and netmask 255.255.255.0 and apply the setting.

- 3 Confirm that your computer can communicate with the access point by pinging its IP address: 192.168.0.3 for DualBand/TriBand 2.4 GHz access point, 192.168.0.4 for TriBand 4.9 GHz. (This is same IP address you use to log into the access point's Web interface.)

If the ping is successful, you're ready to log into the access point's Web interface (see the next section).

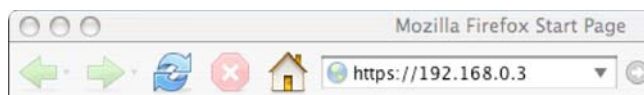
Logging In to an Access Point's Web Interface

To log into a DualBand/TriBand access point's Web interface, you need the access point's IP address. All DualBand/TriBand 2.4 GHz access points ship with an IP address of 198.168.0.3; TriBand 4.9 GHz access points ship with an IP address of 198.168.0.4. (Access point IP addresses cannot be changed.)

To log in to the access point Web interface:

- 1 Open a Web browser and go to the URL for the access point: its default SkyExtender IP address, preceded by `https://`, and appended by the port number in the format `:nnnn/`. For 2.4 GHz access points, the port number is 4433; for 4.9 GHz access points, the port number is 4434. For example, to access a DualBand's 2.4 GHz access point, enter the following value for the URL: `https://192.168.0.2:4433/`.

Figure 24. Entering the access point's URL

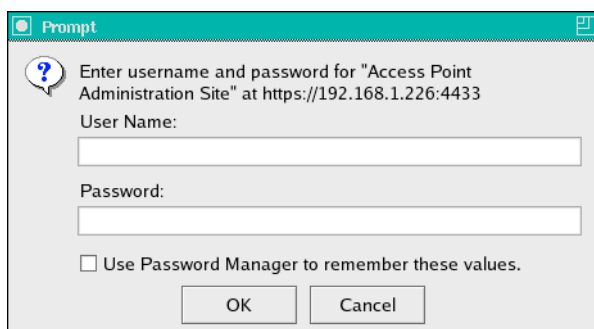


NOTE The access point uses SSL (Secure Sockets Layer) for secure transmission across the Internet. By convention, a URL that requires an SSL connection begins with `https://` (instead of `http://`).

Depending on your browser settings and whether this is a new browser session, a dialog may appear asking you to confirm certificate authority for the Web address. Click **OK** to proceed.

For new browser sessions, the access point Web interface displays the Access Point Login screen. For existing browser sessions, the access point Web interface skips the login process (the next step) and immediately displays the Summary screen (Figure 26).

Figure 25. Access Point Login screen

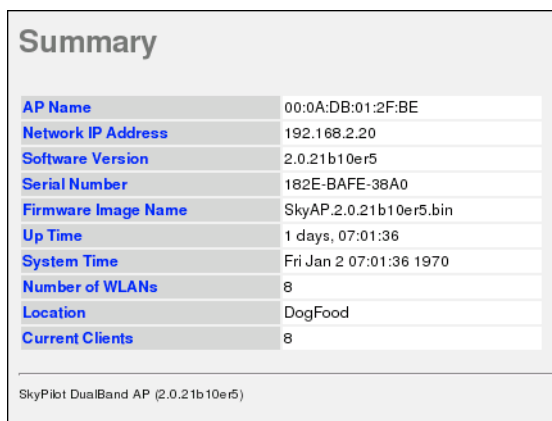


2 Enter the user name and password. The default user name is `admin`, and the default password is `public`.

3 Click **OK**.

The access point Web interface displays the Summary screen, which shows detailed information about the access point.

Figure 26. Access point summary page



Summary	
AP Name	00:0A:DB:01:2F:BE
Network IP Address	192.168.2.20
Software Version	2.0.21b10er5
Serial Number	182E-BAFE-38A0
Firmware Image Name	SkyAP.2.0.21b10er5.bin
Up Time	1 days, 07:01:36
System Time	Fri Jan 2 07:01:36 1970
Number of WLANs	8
Location	DogFood
Current Clients	8

SkyPilot DualBand AP (2.0.21b10er5)

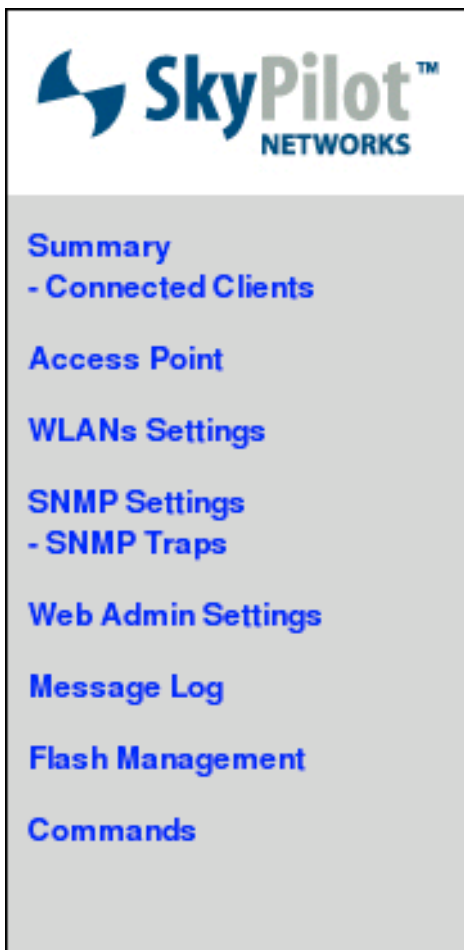
Once you've successfully logged into the Web interface, you can configure the access point for Wi-Fi operation.

Navigating the Access Point Web Interface

The access point Web interface provides a navigation pane on the left (Figure 27) that contains a Windows Explorer–like hierarchical display of monitoring and configuration pages. To view a page, click the corresponding item in the navigation pane.

You can create and modify configurations by clicking items in the navigation pane and then entering data and selecting configuration options.

Figure 27. Security Setting area





Using the Access Point Web Interface

This section describes how to use the access point Web interface by clicking the following items in the navigation pane:

- Summary
- Connected Clients
- Access Point Configuration
- WLANs Settings
- SNMP Settings
- SNMP Trap Receivers
- Web Admin Settings
- Message Log
- Flash Management
- Commands

Summary

The screen you see when you log in to the access point Web interface is the Information Summary screen, and you can return to it at any time by clicking **Summary** in the navigation pane. As shown in Figure 26 on page 41, this screen provides an overview of the access point's current status.

Table 1 describes the fields displayed on the Information Summary screen.

Table 1. Fields on Information Summary screen

Field	Description
AP Name	Name assigned to the access point
Network IP Address	(Default = 192.168.0.3) IP address of the access point assigned by DHCP or provided as a static address
Software Version	Version of software currently running on the access point
Serial Number	Serial number of the access point, assigned by PePLink; used to generate initial MAC address prior to SkyExtender reprogramming
Firmware Image Name	Access point firmware filename
Up Time	Elapsed time since the access point was last booted
System Time	If the time is set by NTP, the current time; otherwise, January 1, 1970 plus the elapsed time since the access point was last booted
Number of WLANs	Number of wireless LANs configured and enabled
Location	Arbitrary string specifying the physical location of the unit
Current Clients	Number of associated 802.11 clients

Connected Clients

You can use **Connected Clients** in the navigation pane to view the list of all clients connected to the DualBand's access point.

To view connected clients:

- In the navigation pane, click **Connected Clients**.

The Web interface displays the Connected Clients screen.

Figure 28. Connected Clients screen

Access Point Information						
Name	00:0A:DB:01:2F:BE					
MAC Address	00:0A:DB:01:2F:BE					
Connected Clients						
MAC Address	WLAN SSID	VLAN ID	Type	Authentication	Status	Details
00:12:f0:ea:ac:2b	SPN11_NIT_psk	100	802.11g	WPA-TKIP	associated	Details
00:20:a6:4e:ee:35	SPN_VISITOR_psk	300	802.11g	WPA-TKIP	associated	Details
00:60:b3:d8:b2:cf	SPN_CORP_wpa	200	802.11g	WPA-TKIP	associated	Details
00:13:ce:32:de:58	SPN_NIT_1x	100	802.11g	802.1x	associated	Details
SkyPilot DualBand AP (2.0.21b10e5)						

Access Point Configuration

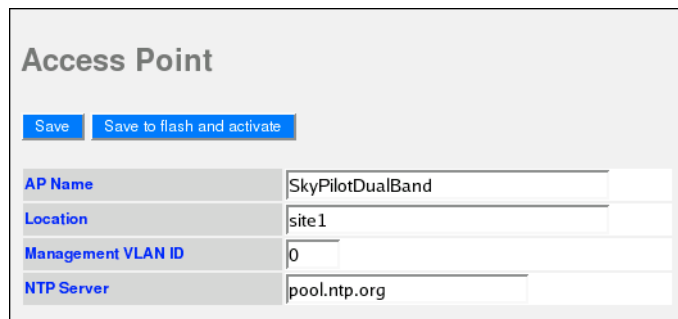
You can use **Access Point** in the navigation pane to view and modify the access point's global configuration parameters. These parameters apply to every SSID on the access point.

To configure an access point:

- 1 In the navigation pane, click **Access Point**.

The Web interface displays the Access Point Configuration screen.

Figure 29. Access Point Configuration screen with address area



The screenshot shows the 'Access Point' configuration page. At the top, there are two buttons: 'Save' and 'Save to flash and activate'. Below these are four configuration fields:

AP Name	SkyPilotDualBand
Location	site1
Management VLAN ID	0
NTP Server	pool.ntp.org

This screen contains an (unlabeled) address area followed by three additional areas, labeled Security Setting, Radius Server Setting, and 802.11b/g Profile.

- 2 Enter settings for the configuration items you want to modify (see the next sections).
- 3 Save your changes:
 - To store your changes to volatile RAM on the access point, click **Save**.
 - To save your changes to nonvolatile flash memory and instantly update the access point's active configuration, click **Save to flash and activate**.

NOTE You can also save all configuration modifications to flash memory from the Configuration Management Commands screen; see "Commands" on page 72.

Address Area

Use the address area of the Access Point Configuration screen (the top group of configuration items, as shown in Figure 29 on page 46) to view and edit names and general address settings for the access point.

Table 2 describes the fields displayed in the address area.

Table 2. Fields in address area

Field	Description
AP Name	Name assigned to the access point. This is not used by SkyPilot EMS, nor does it relate to the device address; it is for administrator reference only.
Location	Location name assigned to the access point. This is not used by SkyPilot EMS, nor does it relate to the device address; it is for administrator reference only.
Management VLAN ID	(Read-only) Displays 0 if there is no management VLAN; otherwise displays the SkyExtender's management VLAN ID.
NTP Server	Host name of server providing the time to the access point.

Security Setting Area

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

Figure 30. Security Setting area

Security Setting	
Telnet Server	<input checked="" type="checkbox"/> Enabled
Telnet Server Password	***** User Name: admin
Maximum Remote Session	10
Remote Session Idle Timeout	0 minutes
Peer to Peer	<input type="checkbox"/> Enabled
802.1X Version	<input type="radio"/> V1 <input checked="" type="radio"/> V2
Management from Wireless Clients	<input checked="" type="checkbox"/> Enabled
SysLog to Remote Server	<input checked="" type="checkbox"/> Enabled
SysLog Server Address	192.168.2.3 Port 514

Table 3 describes the fields displayed in the Security Setting area.

Table 3. Fields in Security Setting area

Field	Description
Telnet Server	If the Enabled check box is selected, enables the Telnet server for remote access to the access point's command line.
Telnet Server Password	(Available only if Telnet Server is enabled) Password and user name for logging in to the Telnet server.
Maximum Remote Session	Maximum number of simultaneous remote Telnet sessions allowed, or 0 to allow unlimited sessions.
Remote Session Idle Timeout	Number of minutes a Telnet or <code>ssh</code> session stays connected without activity, or 0 to never time out.
Peer to Peer	<p>If the Enabled check box is selected, enables peer-to-peer (blocks Layer 2 broadcast and ARP traffic between wireless clients).</p> <p>Typically you'll 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 allow shared LAN services such as file sharing.</p>
802.1X Version	802.1X protocol version.
Management from Wireless Clients	If the Enabled check box is selected, enables wireless client access to the access point's web interface; if the check box is not selected, access is disabled (and the Web interface will be accessible only through the SkyPilot wireless mesh network).
SysLog to Remote Server	If the Enabled check box is selected, enables system logging to a remote syslog server.
SysLog Server Address	(Available only if SysLog to Remote Server is enabled) IP address of the SysLog server.
Port	(Available only if SysLog to Remote Server is enabled) Port number for the SysLog server.

Radius Server Setting Area

Radius servers supply backend authentication services for 802.1x or WPA WLAN security.

Use the Radius Server Setting area of the Access Point Configuration screen only if 802.1x or WPA authentication will be used in any of the WLANs, in which case you must configure the primary Radius host information. Secondary host parameters are optional.

Figure 31. Radius Server Setting area

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"/>

Table 4 describes the fields displayed in the Radius Server Settings area.

Table 4. Fields in Radius Server Setting area (Page 1 of 2)

Field	Description
Primary Host	IP address of the primary Radius server that will authenticate users of any 802.1x/WPA WLANs.
Secret	Shared secret used by the primary Radius server that authenticates the access point.
Authentication Port	TCP/UDP port for primary Radius server authentication services; must match the port number configured for authentication on the primary Radius server. Click Default AuthPort to reset the value to the default port number (1812).

Table 4. Fields in Radius Server Setting area (Page 2 of 2)

Field	Description
Accounting Port	TCP/UDP port for primary Radius server accounting services; this must match the port number configured for accounting services on the primary Radius server. Click Default AcctPort to reset the value to the default port number (1813).
Secondary Host	Same as Primary Host above, but for the secondary Radius server.
Secret	Same as Secret above, but for the secondary Radius server.
Authentication Port	Same as Authentication Port above, but for the secondary Radius server.
Accounting Port	Same as Accounting Port above, but for the secondary Radius server.

802.11b/g Profile Area

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

Figure 32. 802.11b/g Profile area

802.11b/g Profile

Radio Policy	802.11b/g ▾
Country	Default (US) ▾
RF Channel	11 (2.462 GHz) ▾

Table 5 describes the fields displayed in the 802.11b/g Profile area.

Table 5. Fields in 802.11b/g area

Field	Description
Radio Policy	Specifies whether clients are a mix of 802.11b/g or 802.11b only. Typically, you'll want the 802.11b/g mix.
Country	Country in which the access point is operating; limits the available RF Channel selections.
RF Channel	Radio frequency channel for access point operation. In the US, 11 channels are available, but only three of them do not overlap: 1, 6, and 11. Set the channel to one of the three nonoverlapping channels unless you plan to implement special channel reuse patterns.

WLANs Settings

You can use **WLANs Settings** in the navigation pane to view, delete, add, and modify 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.

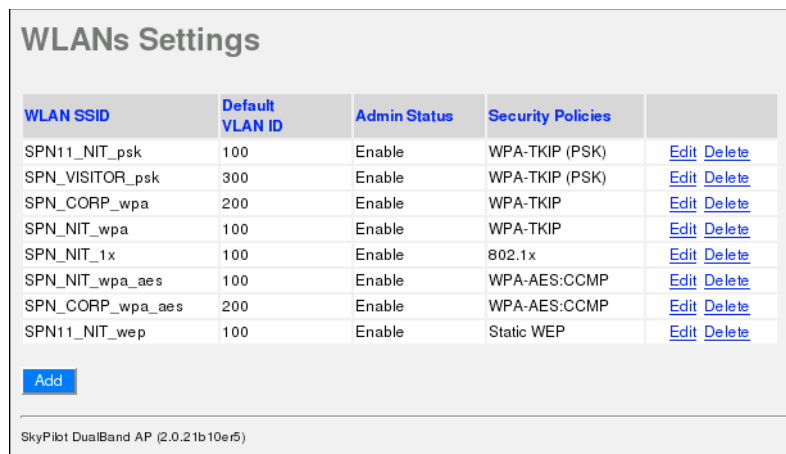
By default, the access point includes one predefined SSID (the DualBand/TriBand MAC address), which uses a WPA-PSK (Pre-Shared Key) configuration (also known as WPA-Personal).

To add, configure, or delete a WLAN:

- 1 In the navigation pane, click **WLANs Settings**.

The Web interface displays the WLANs Settings page, which provides information about every WLAN currently configured, including its SSID name, VLAN ID (if present), current administrative status, and security policies in effect.

Figure 33. WLANs Settings page



WLAN SSID	Default VLAN ID	Admin Status	Security Policies	
SPN11_NIT_psk	100	Enable	WPA-TKIP (PSK)	Edit Delete
SPN_VISITOR_psk	300	Enable	WPA-TKIP (PSK)	Edit Delete
SPN_CORP_wpa	200	Enable	WPA-TKIP	Edit Delete
SPN_NIT_wpa	100	Enable	WPA-TKIP	Edit Delete
SPN_NIT_1x	100	Enable	802.1x	Edit Delete
SPN_NIT_wpa_aes	100	Enable	WPA-AES:CCMP	Edit Delete
SPN_CORP_wpa_aes	200	Enable	WPA-AES:CCMP	Edit Delete
SPN11_NIT_wep	100	Enable	Static WEP	Edit Delete

[Add](#)

SkyPilot DualBand AP (2.0.21b10e5)

- 2 Do any of the following:
 - To view the details about a WLAN or to modify its configuration, click **Edit** in its summary line and enter information for the configuration items you want to modify (see the next section).
 - To delete a WLAN, click **Delete** in its summary line, and then **OK** in response to the confirmation prompt.

- To add a WLAN, click **Add** and enter the necessary configuration items (see the next section).

3 Save your changes:

- To store your changes to volatile RAM on the access point, click **Save**.
- To save your changes to nonvolatile flash memory and instantly update the SkyExtender DualBand access point's active configuration, click **Save to flash and activate**.

NOTE You can also save all configuration modifications to flash memory from the Configuration Management Commands screen; see "Commands" on page 72.

The Web interface redisplay the WLANs summary page, showing the new WLAN or updated details of a modified WLAN.

WLAN Details

The WLAN Details screen appears when you click **Edit** or **Add** on the WLANs Settings page.

Figure 34. WLAN Details screen

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 checked="" type="checkbox"/> Enabled
Default Quality of Service	Low ▾
Admin Status	<input checked="" type="checkbox"/> Enabled
DHCP Server Type	None ▾
Security Policy	None ▾
<input type="button" value="Save"/> <input type="button" value="Save to flash and activate"/>	
SkyPilot DualBand AP (2.0.21b10e15)	

Depending on the configuration options you select, the Web interface displays some or all of four areas, labeled DHCP Relay Parameters, DHCP Server Parameters, 802.1x Parameters, and WPA Parameters.

Table 6 describes the fields displayed in the WLAN Details screen.

Table 6. Fields in WLAN Details screen (Page 1 of 3)

Field	Description
WLAN SSID	(Required) Text string specifying the SSID that's announced for this WLAN (unless Broadcast SSID is not enabled).
Default VLAN ID	Data VLAN ID mapped to this WLAN, or use 0 to indicate no VLAN assignment. NOTE If you're configuring this WLAN for 802.1x or WPA, a RADIUS server can override the default VLAN setting on a per user basis.
Broadcast SSID	If the Enabled check box is selected, enables access point broadcasting of the SSID to 802.11 clients (making the WLAN visible to users). If the Enabled check box is not selected (disabling broadcasting), users can still associate with this SSID/WLAN if they know the SSID and can configure their client software to connect to the SSID. Typically, you'll want to enable SSID broadcasting.
Default Quality of Service	Quality of Service (QoS) level. The access point doesn't enforce the selected QoS level; it simply sets the 802.1p tag for the selected level on all traffic that enters the WLAN. QoS choices correspond to 802.1p user priorities as follows: <ul style="list-style-type: none"> ● High = 6 ● Low = 0

Table 6. Fields in WLAN Details screen (Page 2 of 3)

Field	Description
Admin Status	<p>If the Enabled check box is selected, activates this WLAN.</p> <p>If the Enabled check box is not selected (making the WLAN inactive), the WLAN can still be fully configured, but the access point will not announce or respond to connection requests or other traffic directed to the SSID.</p>
DHCP Server Type	<p>Type of DHCP used by this WLAN:</p> <ul style="list-style-type: none"> ● None—Allows IP addresses to be supplied by a central DHCP server elsewhere on the network (typical setting). ● Relay—DHCP requests on this WLAN will be forwarded to the specified DHCP server. If you select this option, the Web interface displays the DHCP Relay Parameters area, where the IP address of the server is specified (see “DHCP Relay Parameters Area” on page 57). ● Server—The access point acts as a DHCP server on the WLAN. If you select this option, the Web interface displays the DHCP Server Parameters area, where the DHCP server configuration is specified (see “DHCP Server Parameters Area” on page 57).

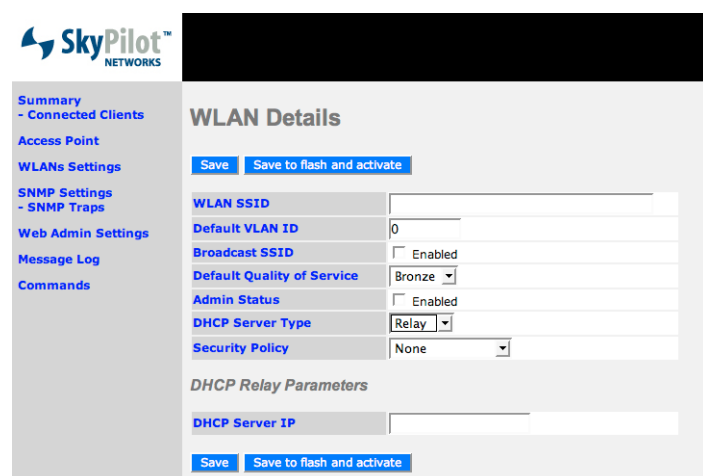
Table 6. Fields in WLAN Details screen (Page 3 of 3)

Field	Description
Security Policy	<p data-bbox="570 321 1146 380">Encryption and/or authentication scheme used by this WLAN:</p> <ul style="list-style-type: none"> <li data-bbox="570 405 1214 432">● None—Open network (no authentication or encryption). <li data-bbox="570 447 1214 604">● Static WEP—No authentication, shared WEP key, no key rotation, and WEP encryption. If you select this option, the Web interface displays the Static WEP Parameters area, where the keys are configured (see “Static WEP Parameters Area” on page 58). Static WEP is easily cracked, and should not be used in production environments. <li data-bbox="570 695 1214 877">● 802.1x—802.1x/EAP authentication via dynamic WEP. The WEP key is unique per session and is automatically changed at a periodic rate via Radius reauthentication. If you select this option, the Web interface displays the 802.1x Parameters area, where the keys are configured (see “802.1x Parameters Area” on page 59). This is the preferred choice for older clients that do not support WPA. <li data-bbox="570 968 1214 1192">● WPA-TKIP—802.1x/EAP authentication via TKIP (Temporal Key Integrity Protocol), a hardened version of the older WEP standard. The key is updated automatically and transparently with DES or AES encryption. If you select this option, the Web interface displays the WPA Parameters area, where the preshared key parameters are configured (see “WPA Parameters Area” on page 60). This option provides a higher level of security than WEP or 802.1x, but it requires users to have a WPA client (which is built into recent versions of Windows XP, Mac OS X, and Linux). WPA-TKIP can be configured to use Radius authentication or a pre-shared key. <li data-bbox="570 1377 1214 1661">● WPA-AES:CCMP—Complete 802.11i (WPA2) standard, replacing WEP/DES and TKIP with a specific mode of the Advanced Encryption Standard (AES): the Counter Mode with Cipher Block Chaining–Message Authentication Code (CBC-MAC) protocol (CCMP). CCMP provides both data confidentiality (encryption) and data integrity. If you select this option, the Web interface displays the WPA Parameters area, where the preshared key parameters are configured (see “WPA Parameters Area” on page 60). This is the highest security option you can choose, but some legacy 802.11 clients may not support it.

DHCP Relay Parameters Area

The DHCP Relay Parameters Area appears when you select **Relay** as the **DHCP Server Type** on the WLAN Details screen. Use this area to configure the IP address of the authoritative DHCP server for a network.

Figure 35. DHCP Relay Parameters area

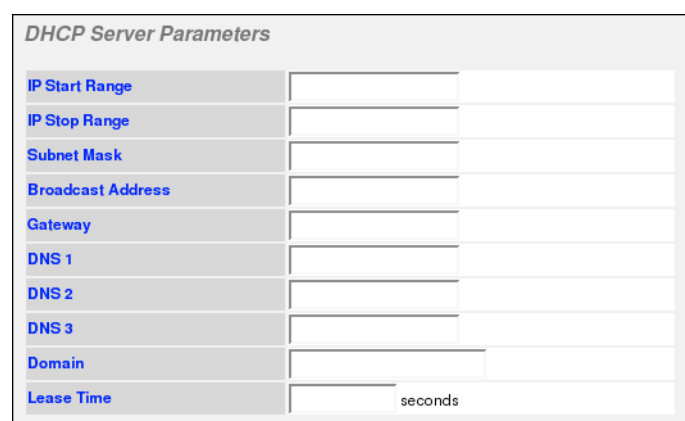


The screenshot shows the SkyPilot Networks web interface. On the left is a navigation menu with options: Summary - Connected Clients, Access Point, WLANs Settings, SNMP Settings - SNMP Traps, Web Admin Settings, Message Log, and Commands. The main content area is titled "WLAN Details" and contains two sections. The first section, "WLAN Settings", includes fields for WLAN SSID, Default VLAN ID (0), Broadcast SSID (Enabled checkbox), Default Quality of Service (Bronze dropdown), Admin Status (Enabled checkbox), DHCP Server Type (Relay dropdown), and Security Policy (None dropdown). Below this is the "DHCP Relay Parameters" section, which includes a DHCP Server IP field. Both sections have "Save" and "Save to flash and activate" buttons.

DHCP Server Parameters Area

The DHCP Server Parameters area (Figure 36) appears when you select **Server** as the **DHCP Server Type** on the WLAN Details screen. Use this area to configure a local DHCP server for use by the WLAN.

Figure 36. DHCP Server Parameters area



The screenshot shows the "DHCP Server Parameters" configuration page. It contains a table with the following fields:

DHCP Server Parameters	
IP Start Range	
IP Stop Range	
Subnet Mask	
Broadcast Address	
Gateway	
DNS 1	
DNS 2	
DNS 3	
Domain	
Lease Time	seconds

Table 7 describes the fields displayed in the DHCP Server Parameters area.

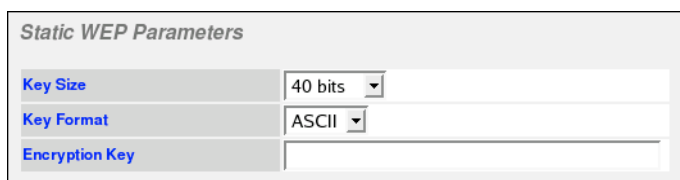
Table 7. Fields in DHCP Server Parameters area

Field	Description
IP Start Range	Starting address for the IP address pool supplied by the DHCP server; for example, 192.168.10.100
IP Stop Range	Ending address for the IP address pool supplied by the DHCP server; for example, 192.168.10.254
Subnet Mask	Subnet mask for this network segment; for example, 255.255.255.0
Broadcast Address	IP address for IP broadcasts on this network segment
Gateway	IP address of the default gateway/router for this network segment
DNS 1	IP address of the primary DNS resolver for this network
DNS 2	IP address of the secondary DNS resolver for this network
DNS 3	IP address of the tertiary DNS resolver for this network
Domain	Default domain name for this network
Lease Time	Number of seconds each DHCP lease remains valid before renewal is necessary

Static WEP Parameters Area

The Static WEP Parameters area (Figure 37) appears when you select **Static WEP** as the **Security Policy** on the WLAN Details screen. Use this area to configure the keys used for WEP encryption.

Figure 37. Static WEP Parameters area



The screenshot shows a form titled "Static WEP Parameters". It contains three rows of configuration options:

- Key Size:** A dropdown menu currently set to "40 bits".
- Key Format:** A dropdown menu currently set to "ASCII".
- Encryption Key:** An empty text input field.

Table 9 describes the fields displayed in the Static WEP Parameters area.

Table 8. Fields in Static WEP Parameters area

Field	Description
Key Size	Key size to use for this network's encryption: 40 bits or 104 bits (also known as 64-bit or 128-bit, respectively). 104 bits is preferred unless the WLAN clients are unable to accept that setting.
Key Format	Format of the Encryption Key , below: ASCII or HEX.
Encryption Key	Text string that functions as the key; up to 255 printable characters.

802.1x Parameters Area

The 802.1x Parameters area (Figure 38) appears when you select **802.1x** as the **Security Policy** on the WLAN Details screen. Use this area to configure the keys used for 802.1x/EAP encryption.

Figure 38. 802.1x Parameters area

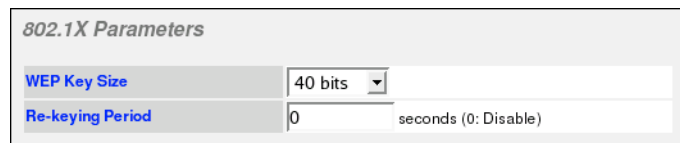


Table 9 describes the fields displayed on the 802.1x Parameters area.

Table 9. Fields Displayed in 802.1x Parameters area

Field	Description
WEP Key Size	Key size to use for this network's encryption: 40 bits or 104 bits (also known as 64-bit or 128-bit, respectively). 104 bits is preferred unless the WLAN clients are unable to accept that setting.
Re-keying Period	Number of seconds between dynamic key updates. For maximum protection, enter 300 seconds (5 minutes) or less. However, don't use too small a value; rekeying requires about a second to complete, so too frequent rekeying can increase downtime.

WPA Parameters Area

The WPA Parameters area (Figure 39) appears when you select **WPA-TKIP** or **WPA-AES:CCMP** as the **Security Policy** on the WLAN Details screen. Use this area to configure the keys used for WPA encryption.

Figure 39. WPA Parameters area

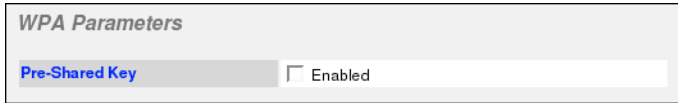


Table 10 describes the fields displayed on the WPA Parameters area.

Table 10. Fields Displayed in 802.1x Parameters area

Field	Description
Pre-Shared Key	If the Enabled check box is selected, enables use of a pre-shared key
Passphrase	(Available only if Pre-Shared Key is selected) Text string that functions as a password; up to 255 printable characters

SNMP Settings

You can use **SNMP Settings** in the navigation pane to configure the access point for SNMP operations.

To configure SNMP:

- 1 In the navigation pane, click **SNMP Settings**.

The Web interface displays the SNMP Server Settings screen, which provides information about SNMP settings in general, and information about every SNMP community currently configured, including its name, IP addresses, access mode, and status.

Figure 40. SNMP Server Settings screen

SNMP Settings

Server Name: 00:0A:DB:01:2F:BE

SNMPv1: Enable

SNMPv2: Enable

SNMPv3: Enable

Save Save to flash and activate

SNMPv1/v2 Communities New

Community Name	IP Address	IP Mask	Access Mode	Status	
public	0.0.0.0	0.0.0.0	Read Only	Enable	Edit Remove

SNMPv3 Users New

SkyPilot DualBand AP (2.0.21b10e5)

This screen contains an (unlabeled) general settings area followed by two additional areas, labeled SNMPv1/v2 Communities and SNMPv3 Users.

- 2 Do any of the following:
 - To modify general SNMP settings for the access point, enter the desired information at the top of the screen (see the next section).
 - To view the details about an SNMP community, or to modify its configuration, click **Edit** in its summary line and enter information for any of the configuration items you want to modify (see “SNMPv1/v2 Community Area” on page 63 or “SNMPv3 User Setting Area” on page 64).
 - To remove an SNMP community, click **Remove** in its summary line, and then **OK** in response to the confirmation prompt.

- To add an SNMP community, click **New**, and enter the necessary configuration items (see “SNMPv1/v2 Community Area” on page 63 or “SNMPv3 User Setting Area” on page 64).

3 Save your changes:

- To store your changes to volatile RAM on the access point, click **Save**.
- To save your changes to nonvolatile flash memory and instantly update the SkyExtender DualBand access point’s active configuration, click **Save to flash and activate**.

NOTE You can also save all configuration modifications to flash memory from the Configuration Management Commands screen; see “Commands” on page 72.

The Web interface redisplay the SNMP Server Settings screen, showing the new SNMP community or updated details of a modified SNMP community.

General Settings Area

Use the general settings area of the SNMP Server Settings screen (the top group of configuration items, as shown in Figure 40 on page 61) to modify general SNMP settings for the access point. You can configure agents for any combination of SNMP versions.

Table 11 describes the fields displayed in the settings area.

Table 11. Fields in general settings area

Field	Description
Server Name	Symbolic name that can be returned as a parameter of <code>SNMPv2-MIB::sysName</code> and <code>MANGA-POLEPOINT-MIB::apname</code> .
SNMPv1	If the Enable check box is selected, enables the SNMPv1 agent.
SNMPv2	If the Enable check box is selected, enables the SNMPv2 agent.
SNMPv3	If the Enable check box is selected, enables the SNMPv3 agent.

SNMPv1/v2 Community Area

The SNMPv1/v2 Community area appears when you click **New** or **Edit** for SNMPv1/v2 on the SNMP Server Settings page. Use this area to add and view SNMPv1/v2 community settings.

Figure 41. SNMPv1/v2 Community area

The screenshot shows a web interface for configuring an SNMP community. It includes the following elements:

- Community Name:** A text input field.
- IP Address:** A text input field.
- IP Mask:** A text input field.
- Access Mode:** A dropdown menu currently showing 'Read Only'.
- Status:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Buttons:** 'Save' and 'Save to flash and activate'.
- Footer:** 'SkyPilot DualBand AP (2.0.2.1b-10e5)'

Table 12 describes the fields displayed in the SNMPv1/v2 Community area.

Table 12. Fields in SNMPv1/v2 Community area

Field	Description
Community Name	Name of the SNMPv1/v2 community.
IP Address	IP address (along with the IP mask, below) for which the SNMPv1/v2 agent with this community name will allow access. For example, an IP address of 192.168.2.0 with an IP mask of 255.255.255.0 specifies that the SNMPv1/v2 agent with this community name will allow access to its data from IP addresses from 192.168.2.1 to 192.168.2.254.
IP Mask	See IP Address .
Access Mode	Access mode of this community: Read Only or Read & Write .
Status	Enables or disables the community.

SNMPv3 User Setting Area

The SNMPv3 User Setting area appears when you click **New** or **Edit** for SNMPv3 on the SNMP Server Settings page. Use this area to add and view SNMPv3 community settings.

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.

Figure 42. SNMPv3 User Setting area

The screenshot shows a web form titled "SNMPv3 User Setting". It contains the following fields and controls:

- SNMPv3 User Name:** A text input field.
- Authentication Protocol:** A dropdown menu with "None" selected.
- Privacy Protocol:** A dropdown menu with "None" selected.
- Access Mode:** A dropdown menu with "Read Only" selected.
- Status:** Two radio buttons, "Enable" (selected) and "Disable".

At the bottom of the form are two buttons: "Save" and "Save to flash and activate". The footer of the interface displays "SkyPilot DualBand AP (2.0.2.1b10e5)".

Table 13 describes the fields displayed in the SNMPv3 User Setting area.

Table 13. Fields in SNMPv3 User Setting area (Page 1 of 2)

Field	Description
SNMPv3 User Name	User name for logging in to this SNMPv3 agent.
Authentication Protocol	Authentication protocol used by this SNMPv3 agent: <ul style="list-style-type: none">• None—Open network (no authentication).• HMAC–MD5—MD5 encrypted authentication.• HMAC–SHA—SHA encrypted authentication. If you select HMAC–MD5 or HMAC–SHA , the Web interface displays an additional field, Authentication Password , for configuring the password; see Figure 43.

Table 13. Fields in SNMPv3 User Setting area (Page 2 of 2)

Field	Description
Privacy Protocol	Encryption protocol used by this SNMPv3 agent: <ul style="list-style-type: none"> • None—Open network (no encryption). • CBC-DES—DES encrypted authentication. If you select this option, the Web interface displays an additional field, Privacy Password, for configuring the password.
Access Mode	Access mode of this community: Read Only or Read & Write .
Status	Enables or disables the community.

Figure 43. Additional password fields in SNMPv3 User Setting area

The screenshot shows the 'SNMPv3 User Setting' configuration page. It contains the following fields and controls:

- SNMPv3 User Name:** A text input field.
- Authentication Protocol:** A dropdown menu currently set to 'HMAC-MD5'.
- Authentication Password:** Two text input fields, the second labeled '(Retype)'.
- Privacy Protocol:** A dropdown menu currently set to 'None'.
- Access Mode:** A dropdown menu currently set to 'Read Only'.
- 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 (2.0.21b 10e5)' is visible.

SNMP Trap Receivers

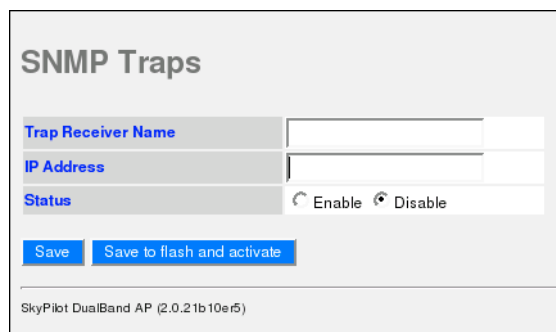
You can use **SNMP Traps** in the navigation pane to configure SNMP trap receivers for access point SNMP operations.

To configure SNMP traps receivers:

- 1 In the navigation pane, click **SNMP Traps**.

The Web interface displays the SNMP Traps screen, where you can configure the SNMP trap receivers.

Figure 44. SNMP Traps screen



The screenshot shows the 'SNMP Traps' configuration page. It features three input fields: 'Trap Receiver Name', 'IP Address', and 'Status'. The 'Status' field has radio buttons for 'Enable' and 'Disable'. Below the fields are two buttons: 'Save' and 'Save to flash and activate'. At the bottom of the page, the text 'SkyPilot DualBand AP (2.0.2.1b10e5)' is visible.

- 2 Enter the desired information.
- 3 Save your changes:
 - To store your changes to volatile RAM on the access point, click **Save**.
 - To save your changes to nonvolatile flash memory and instantly update the SkyExtender DualBand access point's active configuration, click **Save to flash and activate**.

NOTE You can also save all configuration modifications to flash memory from the Configuration Management Commands screen; see "Commands" on page 72.

The Web interface redisplay the SNMP Traps screen, showing the information you've just entered along with a status message.

Table 14 describes the fields displayed on the SNMP Traps screen.

Table 14. Fields in SNMP Traps screen

Field	Description
Trap receiver Name	Name of the SNMP trap receiver
IP Address	IP address to which any node using this trap receiver will send SNMP traps
Status	Enables or disables the SNMP trap

Web Admin Settings

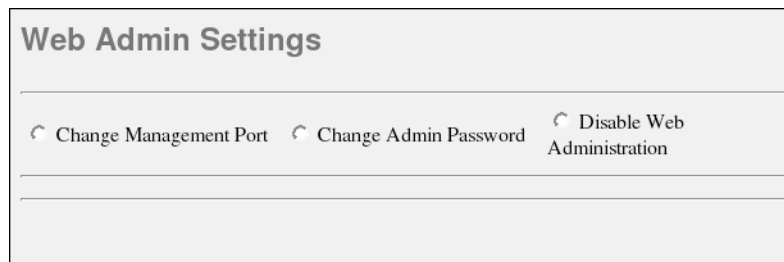
You can use **Web Admin Settings** in the navigation pane to view and configure the parameters that control web access to the access point's Web interface, including management port, user name, and password.

To configure access point Web interface access:

- 1 In the navigation pane, click **Web Admin Settings**.

The Web interface displays the Web Admin Settings screen.

Figure 45. Web Admin Settings page



- 2 Select the option that corresponds to the parameter you want to change.

Depending on the option you select, the Web interface displays one or more fields in which you can configure the appropriate settings:

- To assign a new port address on which to access the Web interface, select **Change Management Port**. See Figure 46.
- To assign a new password for Web access to the Web interface, select **Change Admin Password**. See Figure 47.
- To disable Web access to the Web interface, select **Disable Web Administration**.

(You can restore web access for DualBands/TriBands configured for automatic provisioning by using SkyProvision, and for DualBands/TriBands configured for manual provisioning by using the command-line interface `set factoryap` command.)

- 3** Save your changes:
- To store your changes to volatile RAM on the access point, click **Save**.
 - To save your changes to nonvolatile flash memory and instantly update the access point's active configuration, click **Save to flash and activate**.

NOTE You can also save all configuration modifications to flash memory from the Configuration Management Commands screen; see "Commands" on page 72.

Figure 46. Change Management Port option

The screenshot shows the 'Web Admin Settings' page. At the top, there are three radio button options: 'Change Management Port' (which is selected), 'Change Admin Password', and 'Disable Web Administration'. Below these options, the 'Change Management Port' section is active. It features a 'Port' label and a text input field containing the number '443'. At the bottom of this section are two buttons: 'Save' and 'Save to flash and activate'. The footer of the page reads 'SkyPilot DualBand AP (2.0.21b10e5)'.

Figure 47. Change Admin Password option

The screenshot shows the 'Web Admin Settings' page. At the top, there are three radio button options: 'Change Management Port', 'Change Admin Password' (which is selected), and 'Disable Web Administration'. Below these options, the 'Change Admin Password' section is active. It features two text input fields: 'New Password' and 'New Password (Retype)'. At the bottom of this section are two buttons: 'Save' and 'Save to flash and activate'. The footer of the page reads 'SkyPilot DualBand AP (2.0.21b10e5)'.

Message Log

You can use **Message Log** in the navigation pane to see a snapshot of the most recent syslog output.

NOTE This display is not dynamically updated. To update it, click **Message Log** again in the navigation pane or click your browser's **Reload** button.

Figure 48. Message Log screen

```
Message Log
Jan 2 03:09:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:10:05 dot1x: vath2: STA 00:16:6f:0d:40:8a IEEE 802.11: deassociated
Jan 2 03:10:07 system: ath_newassoc -- ni->ni_bssid = 00:16:6f:0d:40:8a, ni->ni_macaddr = 00:16:6f:0d:40:8a
Jan 2 03:10:07 system: return it not CIPHER_WEP!
Jan 2 03:10:07 dot1x: vath2: STA 00:16:6f:0d:40:8a IEEE 802.11: associated
Jan 2 03:10:07 dot1x: vath2: STA 00:16:6f:0d:40:8a IEEE 802.11: authenticating
Jan 2 03:10:08 dot1x: vath2: STA 00:16:6f:0d:40:8a IEEE 802.11: client downens authenticated
Jan 2 03:10:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:10:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:11:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:11:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:12:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:12:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:13:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:13:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:14:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:14:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:15:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:15:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:16:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:16:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:17:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:17:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:17:53 dot1x: vath0: STA 00:16:cb:b7:a5:11 IEEE 802.11: deassociated
Jan 2 03:18:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:18:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:19:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:19:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:20:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:20:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:21:17 system: ath_newassoc -- ni->ni_bssid = 00:16:cb:b7:a5:11, ni->ni_macaddr = 00:16:cb:b7:a5:11
Jan 2 03:21:17 system: return it not CIPHER_WEP!
Jan 2 03:21:17 dot1x: vath0: STA 00:16:cb:b7:a5:11 IEEE 802.11: associated
Jan 2 03:21:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
Jan 2 03:21:43 dot1x: vath2: STA 00:12:f0:ea:c5:e6 IEEE 802.11: authenticating
Jan 2 03:22:20 dot1x: vath6: STA 00:13:ce:32:de:58 IEEE 802.11: authenticating
```

Flash Management

You can use **Flash Management** in the navigation pane to view the version of firmware on the access point as well as information about the software images in the access point's flash memory.

Figure 49. Flash Management screen

Flash Management		
	Flash 1	Flash 2
Firmware Version	v2.0.21.0	v2.0.21.0
Flash Status	Bootable	Bootable
Boot from		⚙
Next Firmware Upgrade Target	⚙	

SkyPilot DualBand AP (2.0.21b10e15)

Commands

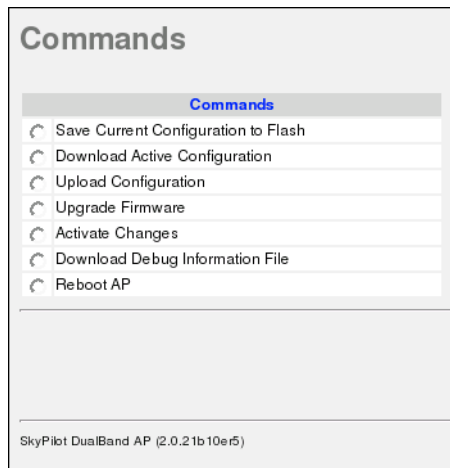
You can use **Commands** in the navigation pane to save configuration changes to volatile RAM memory, to activate configuration changes by saving them to flash memory, and to reboot the access point.

To manage configuration changes:

- 1 In the navigation pane, click **Commands**.

The Web interface displays the Configuration Management Commands screen.

Figure 50. Configuration Management Commands screen



- 2 Select the option that corresponds to the command you want, as described in Table 15. Depending on the option you select, the Web interface displays one or more fields in which you can configure the appropriate settings.

Table 15. Configuration Management options (Page 1 of 2)

To do this	Select
Save changes in the configuration to the access point's flash (nonvolatile) memory.	Save Current Configuration to Flash
The access point won't use the modified configuration until the device reboots or you explicitly activate the changes as described below.	

Table 15. Configuration Management options (Page 2 of 2)

To do this	Select
Download an image into the access point's active partition	Download Active Configuration
Upload the image in the access point's active partition to the designated server	Upload Configuration
Download and install a new firmware image to the access point.	Upgrade Firmware
<p>Save the configuration to flash memory and activate any changes you've made.</p> <p>In some cases—for example, if you've added or deleted a WLAN—this operation can break 802.11x network connections.</p>	Activate Changes
Download a debug log file	Download Debug Information File
<p>Reboot the access point and load the configuration file stored in its flash memory.</p> <p>Any configuration changes that weren't saved to flash memory are lost when you reboot.</p>	Reboot AP

3 Click **Proceed**.

A confirmation message is displayed.

4 Click **OK**.

