Cisco Aironet 1810 Series OfficeExtend Access Point User Guide

First Published: June 1, 2016

Last Updated: July 9, 2020

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Aironet 1810 Series OfficeExtend Access Point User Guide
© 2020 Cisco Systems, Inc. All rights reserved.

Preface v

Audience v

Document Organization v

Conventions vi

Related Documentation and Links vi

CHAPTER 1 **Installing and Configuring the Access Point** 1-1

Before You Begin 1-1

Installing the Access Point in the Network 1-2

Configuring the Wireless LAN Controller IP Address on the Access Point 1-3

Configuring Radio Channels on the Access Point 1-4

Configuring Personal Wireless LANs 1-4

Troubleshooting 1-5

CHAPTER 2 **Understanding the Access Point GUI** 2-1

Accessing the GUI 2-1

Home Page 2-3

AP Info 2-3

SSID 2-3

Client 2-4

Configuration Page 2-5

System Tab 2-6

SSID Tab 2-7

DHCP Tab 2-9

WAN Tab 2-10

Firewall 2-11

Sections and Precedence of Firewall Settings 2-11

Client Filtering 2-11

Port Forwarding 2-12

DMZ 2-12

Backup/Restore 2-13

Event Log Page 2-14

Network Diagnostics 2-15

Preface

The Preface contains the following sections:

- Audience, page v
- Document Organization, page v
- Conventions, page vi
- Related Documentation and Links, page vi

Audience

This document contains information useful to users who connect to a network via a Cisco Aironet 1810 Series OfficeExtend Access Point, which is referred to as the *access point* or as the *AP* in this document. This document is also useful for experienced network administrators who configure and maintain Cisco wireless LAN controllers and Cisco lightweight access points.

This document is meant to be used in conjunction with the following guides:

- *Getting Started Guide - Cisco Aironet 1810 Series OfficeExtend Access Points*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1810/quick/guide/oeap1810getstart.html

- *Cisco Aironet 1810 Series OfficeExtend Access Points Deployment Guide,* at:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_Cisco_OfficeExtend_Access_Point_.html

Document Organization

The following table describes the contents of each chapter in this document:

Table 1 Document Organization

Chapter and Title	Description
Installing and Configuring the Access Point	This chapter provides information on how to install and configure the access point network for your use.
Understanding the Access Point GUI	This chapter describes the access point's GUI.

Conventions

The following table describes conventions used in this document:

Table 2 Command Syntax Guide

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled *Control*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`screen font`	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[ ]	Default responses to system prompts appear in square brackets.

Note Means reader needs to take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader needs to be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation and Links

In addition to the information provided in this publication, you might need to refer to the following documents:

- Getting Started Guide - Cisco Aironet 1810 Series OfficeExtend Access Points:

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1810/quick/guide/oeap1810getstart.html

- Cisco Aironet 1810 Series OfficeExtend Access Points Product Support Page:

  http://www.cisco.com/c/en/us/support/wireless/aironet-1810-series-officeextend-access-points/tsd-products-support-series-home.html

- Cisco Wireless LAN Controller configuration guides:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-installation-and-configuration-guides-list.html

- Cisco Wireless LAN Controller command references:

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

- Cisco Wireless LAN Controller System Message Guide:

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.html

- Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points:

  http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-release-notes-list.html

Installing and Configuring the Access Point

This chapter provides the following information:

- Before You Begin, page 1-1
- Installing the Access Point in the Network, page 1-2
- Configuring the Wireless LAN Controller IP Address on the Access Point, page 1-3
- Configuring Radio Channels on the Access Point, page 1-4
- Configuring Personal Wireless LANs, page 1-4
- Troubleshooting, page 1-5

Before You Begin

The following sections provide information on how to install and configure the Cisco Aironet 1810 Series OfficeExtend Access Point. The specifications of the access point (AP), the parts, mounting options, powering options and other hardware installation procedures are provided in the *Getting Started Guide - Cisco Aironet 1810 Series OfficeExtend Access Points*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1810/quick/guide/oeap1810getstart.html

Ensure that the AP is properly mounted and ready to be powered up before proceeding with the sections that follow. This document is meant to be used in conjunction with the following guides:

- *Getting Started Guide - Cisco Aironet 1810 Series OfficeExtend Access Points*, at:

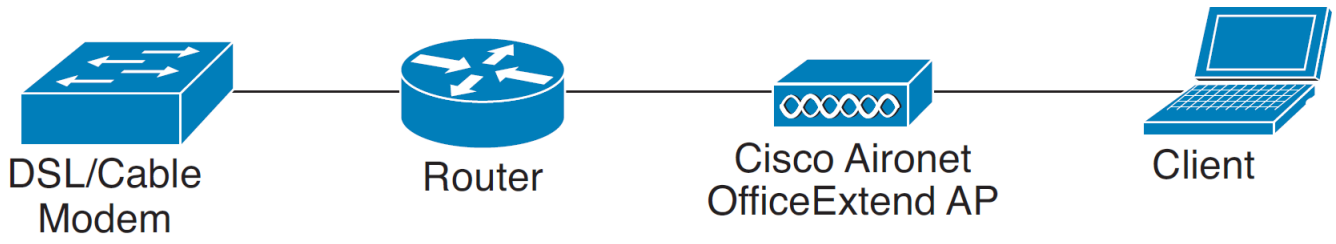
http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1810/quick/guide/oeap1810getstart.html

- *Cisco Aironet 1810 Series OfficeExtend Access Points Deployment Guide,* at:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_Cisco_OfficeExtend_Access_Point_.html

Installing the Access Point in the Network

Figure 1-1 Cisco Aironet 1810 Series OfficeExtend AP Network Deployment Overview



Note In some cases your broadband modem may have an integrated router capability and therefore you do not require a separate router placed between the broadband modem and the Cisco Aironet 1810 Series OfficeExtend Access Point.

To install the Cisco Aironet 1810 Series OfficeExtend AP, follow these steps:

Step 1 Connect the WAN port of the Cisco OfficeExtend Access Point 1810 to your home router/gateway. The Cisco OfficeExtend Access Point gets an IP address from the home router/ gateway.

Note The Cisco OfficeExtend Access Point is not designed to replace the functionality of a home router, and it should not be connected directly to the service provider gateway.

Step 2 After the Cisco OfficeExtend Access Point has started, connect a computer to the port labeled as LAN3. LAN3 is a dedicated local port on OEAP1810. The computer gets an IP address from the default DHCP address pool of 10.0.0.0/24.

Step 3 Open an Internet browser and go to the IP address of the access point. The default IP address is 10.0.0.1

Note Make sure your laptop is not connected to your company's network using a virtual private network (VPN) connection.

Step 4 At the OfficeExtend Access Point login window, click **Login,** and then enter the username and password to log into the access point. The default username and password are *admin* and *admin*.

Step 5 Choose **Configuration > WAN**.

Step 6 Enter the IP address of the Wireless LAN Controller in the **Controller IP Address** field.

Step 7 Leave the Static IP check box unchecked to allow the WAN IP address to be assigned by DHCP.

Step 8 Click **Apply** to commit your changes.

Step 9 On the verification screen, click **Continue**.

The AP connects to the controller and downloads the current software image. Allow 5 minutes for the device to download and reboot with the new code and configuration.

Note The AP restarts when any change is applied on local the GUI. For example, changing the settings for the personal SSID causes interruption to the corporate SSID. It recovers only after the AP rejoins the controller.

Note You do not need to configure any SSIDs for your AP to connect to your company network. The access point receives the company SSID when it connects to the company network by way of the Internet. If you have problems connecting to your company network, contact your IT administrator. You can configure your local SSID WLAN for other devices. See the"Configuring Radio Channels on the Access Point" section on page 1-4.

Note Cisco Aironet 1810 Series OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a home router or gateway, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. There is not limit to the number of Cisco Aironet 1810 Series OfficeExtend access points that can be deployed behind a single NAT device.

Configuring the Wireless LAN Controller IP Address on the Access Point

Follow these steps to configure the IP address of the Wireless LAN Controller on your Cisco Aironet 1810 Series OfficeExtend access point.

Step 1 Obtain the IP address of your Wireless LAN controller from your company's IT professional.

Step 2 Access the 1810 Series OfficeExtend access point GUI as described in "Accessing the GUI" section on page 2-1.

Step 3 Choose **Configuration > WAN** tab.

Step 4 Enter the IP address of the primary controller in the **Controller IP Address** field.

Step 5 Leave the Static IP check box unchecked to allow the WAN IP address to be assigned by DHCP.

Step 6 Click **Apply** to commit your changes.

A verification screen is displayed.

Step 7 Click **Continue**.

The 1810 Series OfficeExtend Access point will connect to the controller and download the current software image. Allow the device 5 minutes to download and reboot with the new code and configuration.

Configuring Radio Channels on the Access Point

Follow these steps to configure a radio channel for your 1810 Series OfficeExtend access point.

Step 1 Access the 1810 Series OfficeExtend access point GUI as described in "Accessing the GUI" section on page 2-1.

Step 2 Choose **Configuration > System**.

Step 3 Choose the desired radio interface – either 2.4 GHz or 5 GHz.

Step 4 From the **Status** drop-down list, choose **Enabled** to enable the wireless interface.

Step 5 From the **Channel Selection** drop-down list, choose the channel on which this interface will operate.

Note 802.11n mode should be enabled by default. If it is disabled, choose **Enabled** from the **802.11 n-mode** drop-down list.

Step 6 Click **Apply** to commit your changes.

Configuring Personal Wireless LANs

Step 1 Access the 1810 Series OfficeExtend access point GUI as described in "Accessing the GUI" section on page 2-1.

Step 2 Choose **Configuration > SSID**.

Step 3 Choose the radio band, which can be either 2.4 GHz or 5.0 GHz. You can duplicate the configuration on both bands, or have different settings on each band.

Step 4 In the **Personal Network** section:

a. Check the **Enabled** check box to enable this wireless connection. By default it is disabled.

b. Check the **Broadcast** check box to broadcast the SSID over the air. By default it is unchecked.

c. In the **SSID** field, enter the personal SSID that you want to assign to this access point. This SSID will be locally switched.

Note Your personal SSID Wireless LAN and your company SSID Wireless LAN are different. When you configure your personal Wireless LAN, use an SSID name that is different from your company's SSID to help avoid confusion.

Step 5 In the **Security Section**, enable **WPA2-PSK** with AES encryption.

Step 6 Click **Apply** to commit your changes.

Step 7 In the verification screen, click **Continue**.

Troubleshooting

Problem	LED Status	Reasons	Possible Solution
Private WLAN clients can connect to the Internet; but WLANs provided by the controller are unable to connect or not being broadcast.	Cycling through Green, Red and Amber	Access Point is in CAPWAP Discovery mode.	Verify that the correct Wireless LAN Controller IP address is entered in the WAN page of the 1810 Series; verify that CAPWAP ports are allowed through the personal firewalls if any are present on a router between the 1810 series and the modem.
WLANs provided by the controller are not broadcast or clients are unable to connect.	Blinking Amber	Software Upgrade in Process.	Wait for 1810 series to finish code download and perform an automatic reboot.
No connectivity is available through 1810 Series access point.	Blinking Red	No IP address on the 1810 Series access point, waiting for DHCP address.	Restart your home router/gateway or modem followed by your 1810 Series access point.
No connectivity is available through 1810 Series access point, local GUI unavailable, or other issues.	Red	Software Failure	Disconnect and reconnect power to the 1810 Series access point.
The access point signal strength is low.	Not applicable	The access point may not be in the optimal position in relation to your device(s). If the access point is in close proximity and above your device, the signal may become skewed.	Position the access point lower than or with the LED side facing your devices.

Understanding the Access Point GUI

This chapter provides the following information:

- Accessing the GUI, page 2-1
- Home Page, page 2-3
- Configuration Page, page 2-5
- Event Log Page, page 2-14
- Network Diagnostics, page 2-15

Accessing the GUI

Follow these steps to access the Cisco Aironet 1810 Series OfficeExtend access point GUI.

Step 1 Connect your laptop to the local Ethernet port 1, or 2 on the 1810 Series OfficeExtend access point.

Note Ethernet port 4 (Remote LAN port) may not be used to configure the 1810 Series OfficeExtend access point.

Step 2 With the 1810 Series OfficeExtend access point connected to your home router/gateway as described in the procedure "Installing the Access Point in the Network" section on page 1-2, enter the IP address of the 1810 Series OfficeExtend access point in the Address field of your Internet browser (http://<*ap-ipaddress*>) and click **Go**.

Note The default IP address is 10.0.0.1.

Note Make sure your laptop is not connected to your company's network using a virtual private network (VPN) connection.

The 1810 Series Office Extend Access Point Login page is displayed.

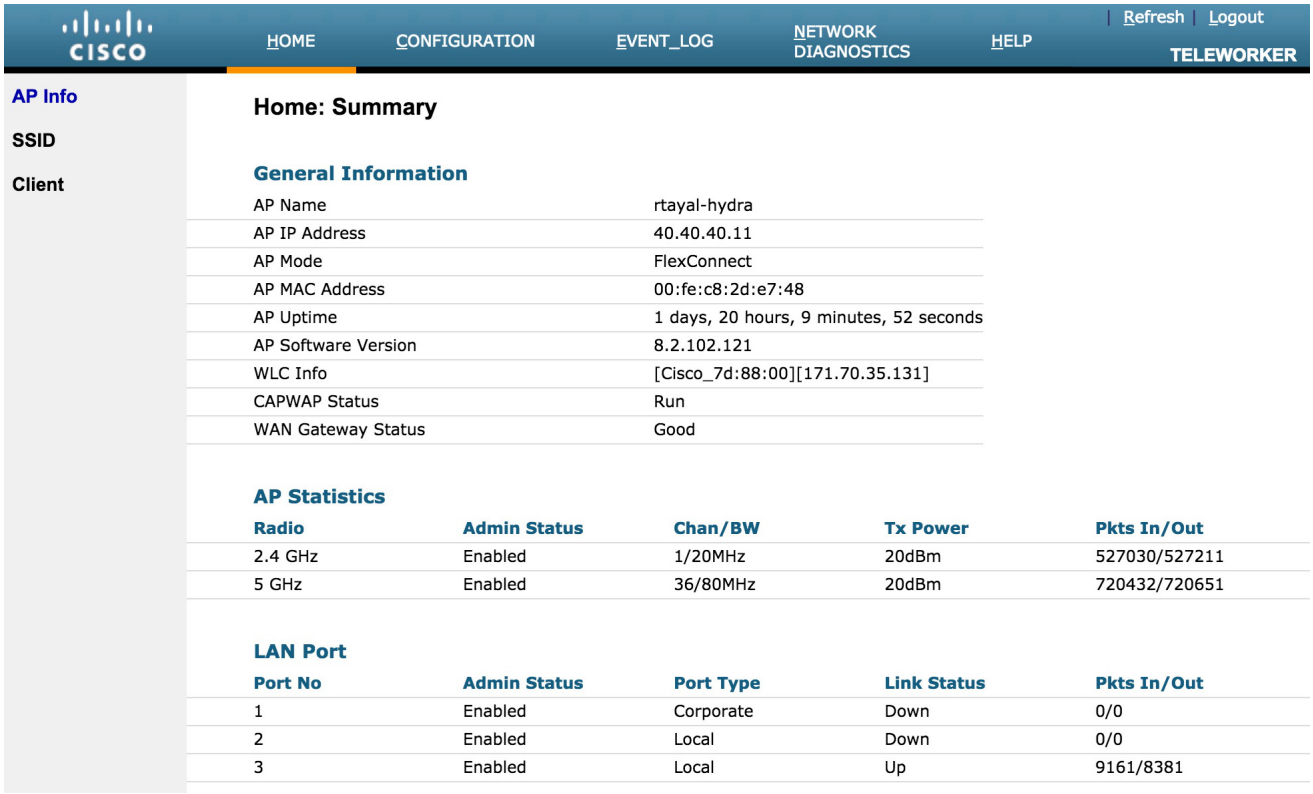
Step 3 When prompted, enter the username and password to log into the access point.

Note The default username and password are *admin* and *admin*.

The 1810 Series OfficeExtend Access Point welcome page is displayed.

Step 4 On the 1810 Series OfficeExtend Access Point welcome page, click **Enter**. The 1810 Series Office Extend Access Point Home page is displayed.

Figure 2-1 Home Page with AP Info Tab View



The GUI consists of these pages:

- Home Page
- Configuration Page
- Event Log Page
- Network Diagnostics
- Help Page

Note When modifying any of the settings described in the following sections, ensure that you click **Apply** for the settings to take effect.

Home Page

This is a multi-tab page showing general information about the AP settings, information about configured Local SSIDs and available Corporate SSIDs, and a summary of the client association statistics. It contains the following tabs:

- AP Info
- SSID
- Client

AP Info

The AP Info tab (see Figure 2-1) shows the access point name, IP address, AP mode, AP MAC address, AP uptime, software version, WLC information, CAPWAP status, and WAN gateway status.

This page also shows radio-specific information, under **AP Statistics**, which shows radio status, channel/bandwidth, transmit power, and number of packets in and out.

This page also displays **LAN Port** statistics such as port number, admin status, port type, link status, and number of packets in and out.

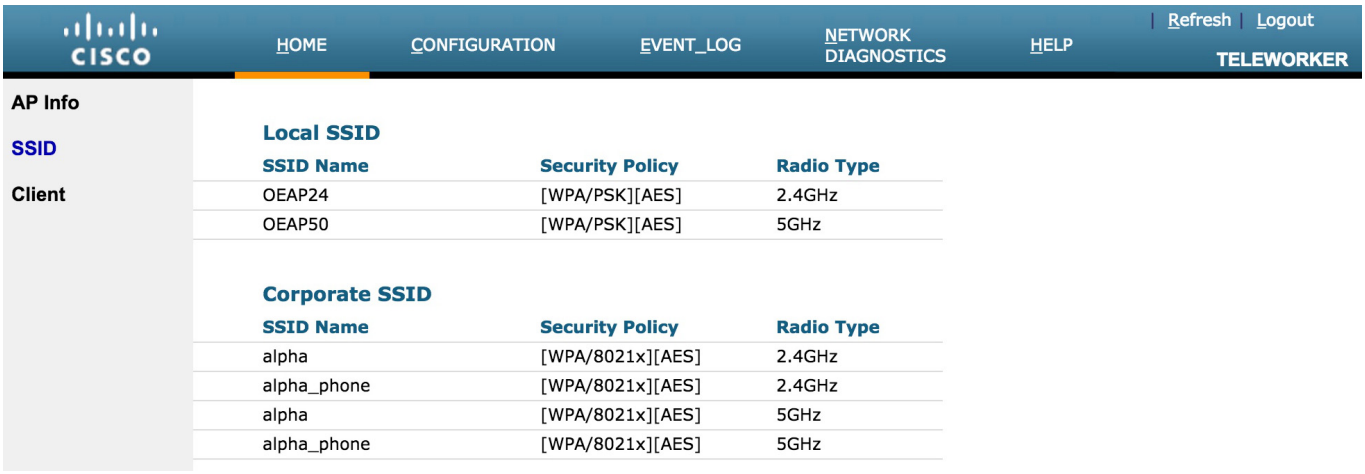
The **CAPWAP** status shows the status of the AP's CAPWAP connection with the controller.

If the WAN connection is established and the AP's Gateway is reachable then the **WAN** status is shown as *Reachable*, else it is shown as *Not Reachable*.

SSID

The SSID tab (see Figure 2-2) lists configured Local SSIDs and available Corporate SSIDs and the configured security policy.

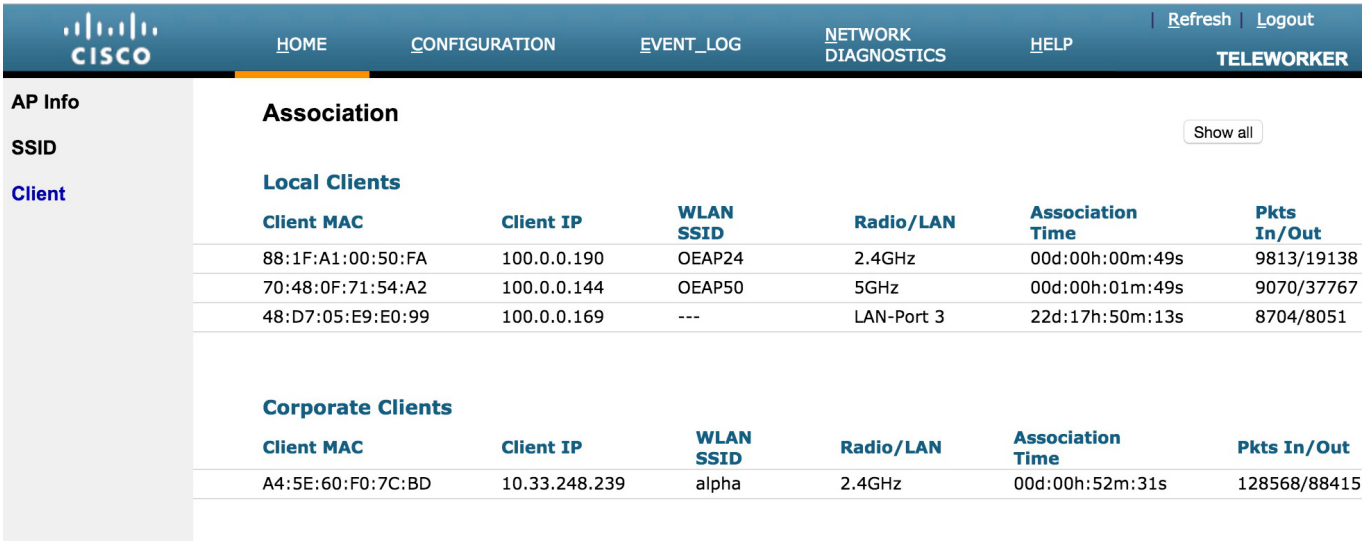
Figure 2-2 Home–SSID Tab



Client

The Client tab (see Figure 2-3) gives the details of associated clients with Local as well as Corporate SSIDs. For each connected client, this page reports the client MAC address, client IP address, WLAN SSID, Radio/LAN, elapsed association time, number of packets in and out.

Figure 2-3 Home–Client Tab



Configuration Page

The Configuration page is a multi-tab page with the following options:

- System Tab
- SSID Tab
- DHCP Tab
- WAN Tab
- Firewall
- Backup/Restore

Wherever applicable, default values are shown.

System Tab

The Configuration System (see Figure 2-4) tab displays and allows the user to configure general system information.

The **Login** section allows the user to change the username and password for the access point.

Note You can leave the username and password fields, along with the router's user name and password fields blank, to disable access control.

The **Radio** section allows the user to configure radio interface parameters. You can configure the parameters for both the 2.4 GHz and the 5 GHz radios. To set these parameters, first click the radio you want to configure from under the **System** tab.

You can set the following parameters for each radio:

- **Status**—Enable/disable the selected radio interface (i.e. 2.4 GHz or 5 GHz).
- **802.11ac mode**—Enable/disable the 802.11ac mode. This parameter is present only for the 5 GHz radio.
- **802.11n mode**—Enable/disable the 802.11n mode.
- **Bandwidth**—Select the channel bandwidth. You can choose 20MHz, 40MHz, or 80MHz.
- **Channel Selection**—Select a particular channel to operate in. For automatic selection, choose **Auto**.

Figure 2-4 Configuration–System Tab

SSID Tab

The Configuration SSID tab (see Figure 2-5) contains fields necessary for you to configure your personal SSIDs, for the 2.4 GHz and the 5 GHz radio interface.

The **Personal Network** section allows the user to configure the following:

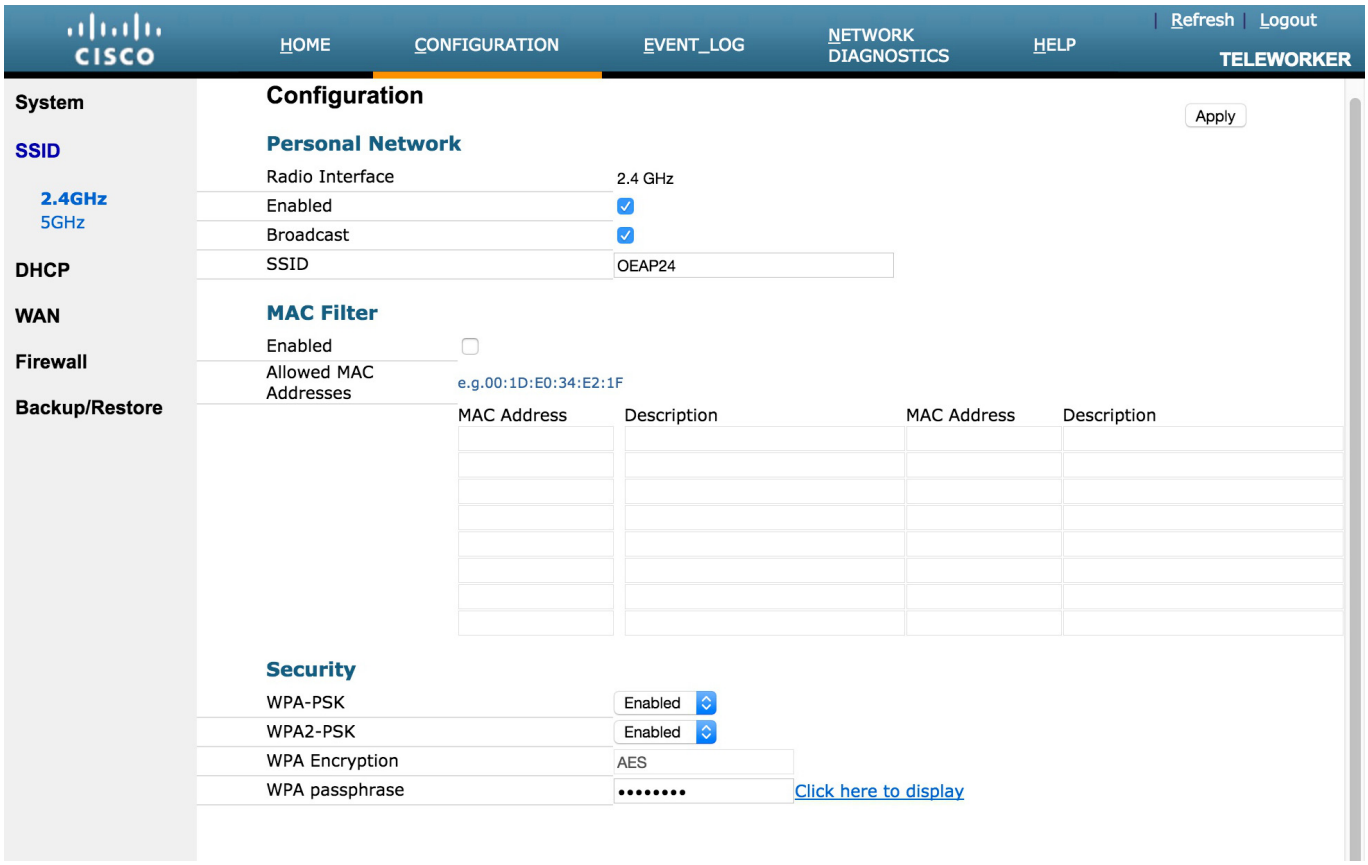
- **Enabled**—Check this check box to set a personal SSID on this radio.
- **Broadcast**—Check this check to broadcast the personal SSID on this radio.
- **SSID**—Specify the personal SSID, which will be the network's name.

The **MAC Filter** section allows for MAC filtering. Check the **Enabled** check box to enable MAC filtering. Specify the MAC addresses that are to be allowed wireless access, in the table provided.

The **Security Section** allows the user to configure security parameters for the selected SSID and radio interface. The following authenticated key management parameters can be configured:

- **WPA-PSK**—Enable/disable WPA-PSK security.
- **WPA2/PSK**—Enable/disable WPA2-PSK security. If you enable this, ensure that the client is configured for WPA2/PSK and AES encryption.
- **WPA Encryption**—The WPA data encryption algorithm is set to AES.
- **WPA Passphrase**—Enter a passphrase having 8 to 32 ASCII characters. The passphrase is case-sensitive.

Figure 2-5 Configuration–SSID Tab



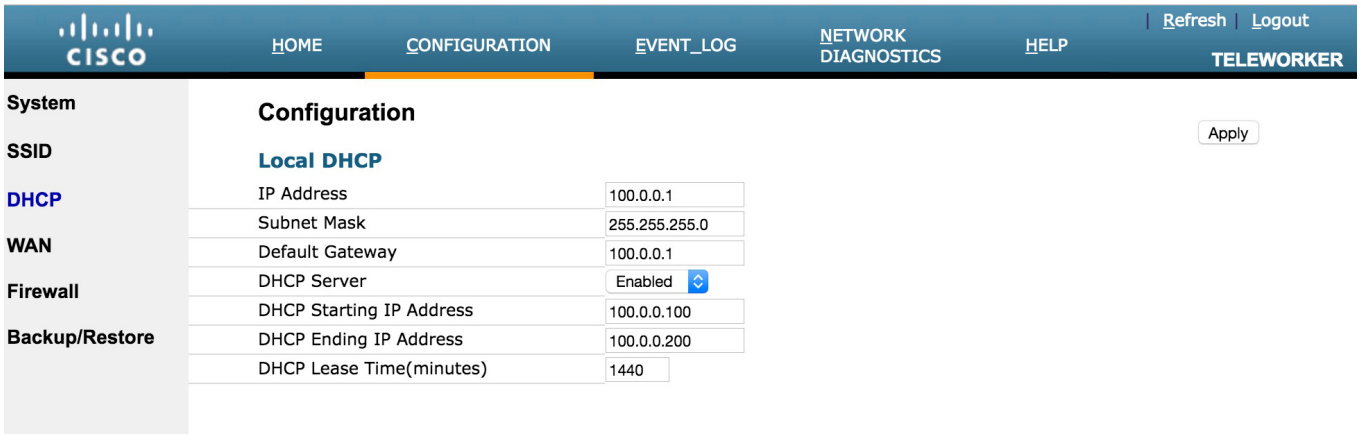
DHCP Tab

The Configuration DHCP tab (see Figure 2-6) contains the fields necessary for configuring the local DHCP server.

The following parameters can be set for the LAN interface:

- **IP Address**—Set the IP address.
- **Subnet Mask**—Set the IP net mask.
- **Default Gateway**—Set the default gateway.
- **DHCP Server**—Enable/disable the DHCP server functionality on the LAN.
- **DHCP Starting IP Address**—Set the start of the IP address range that the DHCP server will use.
- **DHCP Ending IP Address**—Set the end of the IP address range that the DHCP server will use.
- **DHCP Lease Time (minutes)**—Set the time for which the DHCP leases will be valid.

Figure 2-6 Configuration–DHCP Tab



WAN Tab

The Configuration Wireless Access Network (WAN) tab (see Figure 2-7) contains the fields necessary for you to configure the IP address of the Wireless LAN controller on your access point.

In the **Controller** section's **IP Address** field, set the IP address of the primary wireless controller to which the AP will join.

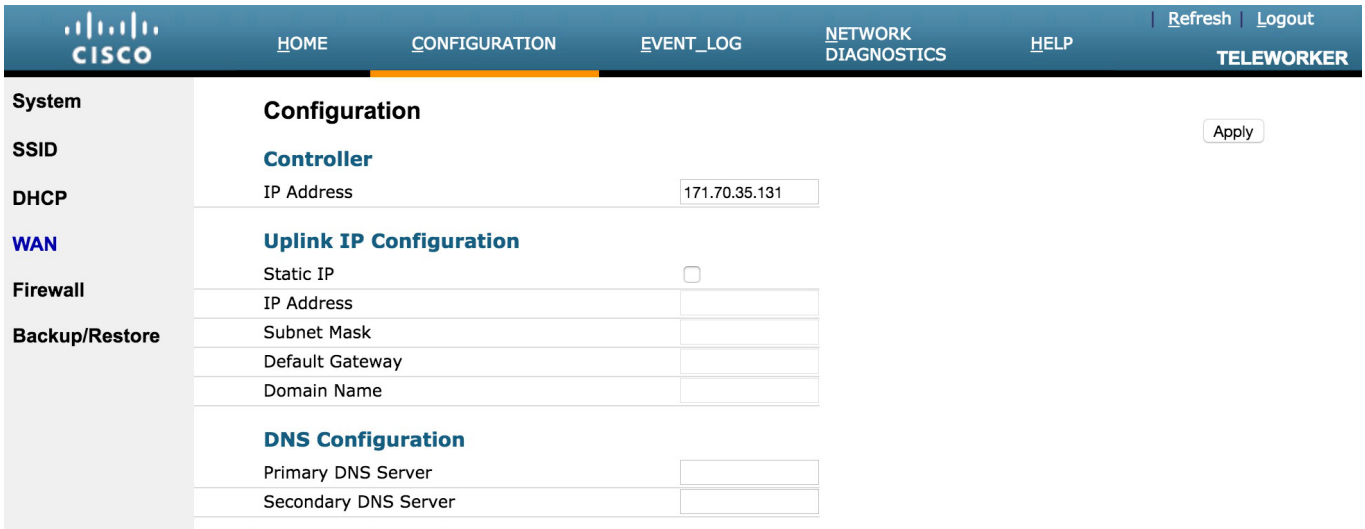
In the **Uplink IP Configuration** section, you can set the following parameters for IP configuration of the WAN port:

- **Static IP**—Check this check box to specifying a static IP for the WAN port.
- **IP Address**—Set the IP address of the connection.
- **Subnet Mask**—Set the IP netmask of the connection.
- **Default Gateway**—Set the IP address of the default gateway for the connection.
- **Domain Name**—Enter the domain name as provided by your ISP. This is an optional field.

The DNS configuration section is optional. You can set the following parameters here:

- **Primary DNS Server**—Enter the IP address of a primary DNS server for resolving host names.
- **Secondary DNS Server**—Enter the IP address of a secondary DNS server for resolving host names.

Figure 2-7 Configuration-WAN Tab



Firewall

The Configuration Firewall tab (see Figure 2-8) contains fields to enable/disable the access point's firewall and set various firewall parameters.

Set the **Firewall Status** as **Enabled** to apply client filtering and port forwarding rules. To disable the firewall, from the drop-down list choose **Disabled**, and then click **Apply**. The firewall is disabled by default.

The following firewall settings are available:

- Selective unblocking of traffic based on application types such as HTTP, HTTPS, SSH, and FTP.
- Unblocking of traffic based on LAN destination addresses, protocols and ports.
- Port forwarding, with 10 or less total entries for separate port numbers.

Note All firewall settings are applicable on the WAN port for local traffic (traffic sent directly to the Internet, and not to the corporate network). Firewall protection for CAPWAP traffic and traffic sent through the controller to the corporate office is configured and monitored on the WLC.

Sections and Precedence of Firewall Settings

The following are the sections in the Firewall tab, listed in the order of precedence of the firewall settings:

1. Port Forwarding
2. DMZ
3. Client Filtering

Client Filtering

The Client Filtering sections allows you to add filtering rules to filter traffic from clients, by specifying the following for each rule:

- Set the rule for all LAN clients or only for clients in a specified IP address range.
  - To set the rule for all local clients, check the **All Clients** check box.
  - To set the rule for a range of IP address, specify the **Local IP Address Range**.
- Set the rule to filter access to applications using the any of the following protocols:
  - FTP
  - Telnet
  - SMTP
  - DNS
  - TFTP
  - HTTP
  - POP3
  - NNTP

  - SNMP
  - HTTPS

  Select the required protocol for the rule by choosing it from the **Protocol** drop-down list.

- Set the rule to filter the traffic to specified destination port range, or to TCP or UDP ports as a whole. Depending on your requirement, you can use the **Destination Port Range** fields, or select **TCP** or **UDP** from the **Protocol** drop-down list.
- Set the rule as an allow or disallow rule for the combination of the aforementioned parameters. Check the **Allow** check box to make this an allow rule. Else, uncheck it.

Port Forwarding

The Port Forwarding settings allow you to configure port forwarding rules for packets from WAN port to Local LAN clients and back. A maximum of 10 Port Forwards can be set, but their ranges should be of the same size and should not overlap. For each rule you can set the following parameters:

- Protocol—You select either of the following options as per your requirements:
  - Select **TCP** or **UDP** and then set the **WAN Port Start** and **WAN Port End** values.
  - Select one of these protocols— FTP, Telnet, SMTP, DNS, TFTP, HTTP, POP3, NNTP, SNMP, or HTTPS

  Note If HTTP or HTTPS protocol is selected, the OfficeExtend GUI will not be accessible from the WAN side because the port is overridden to the client destination.

- WAN port range—You can manually set this, using the **WAN Port Star**t and **WAN Port End** fields, only if the protocol is specified as TCP or UDP. For all other protocols this range displays the pre-configured port number.
- Local IP address—Specify the Local LAN client IP Address where the traffic is to be forwarded to.
- LAN port range—Set this range using the **Local Port Start** and **Local Port End** fields.

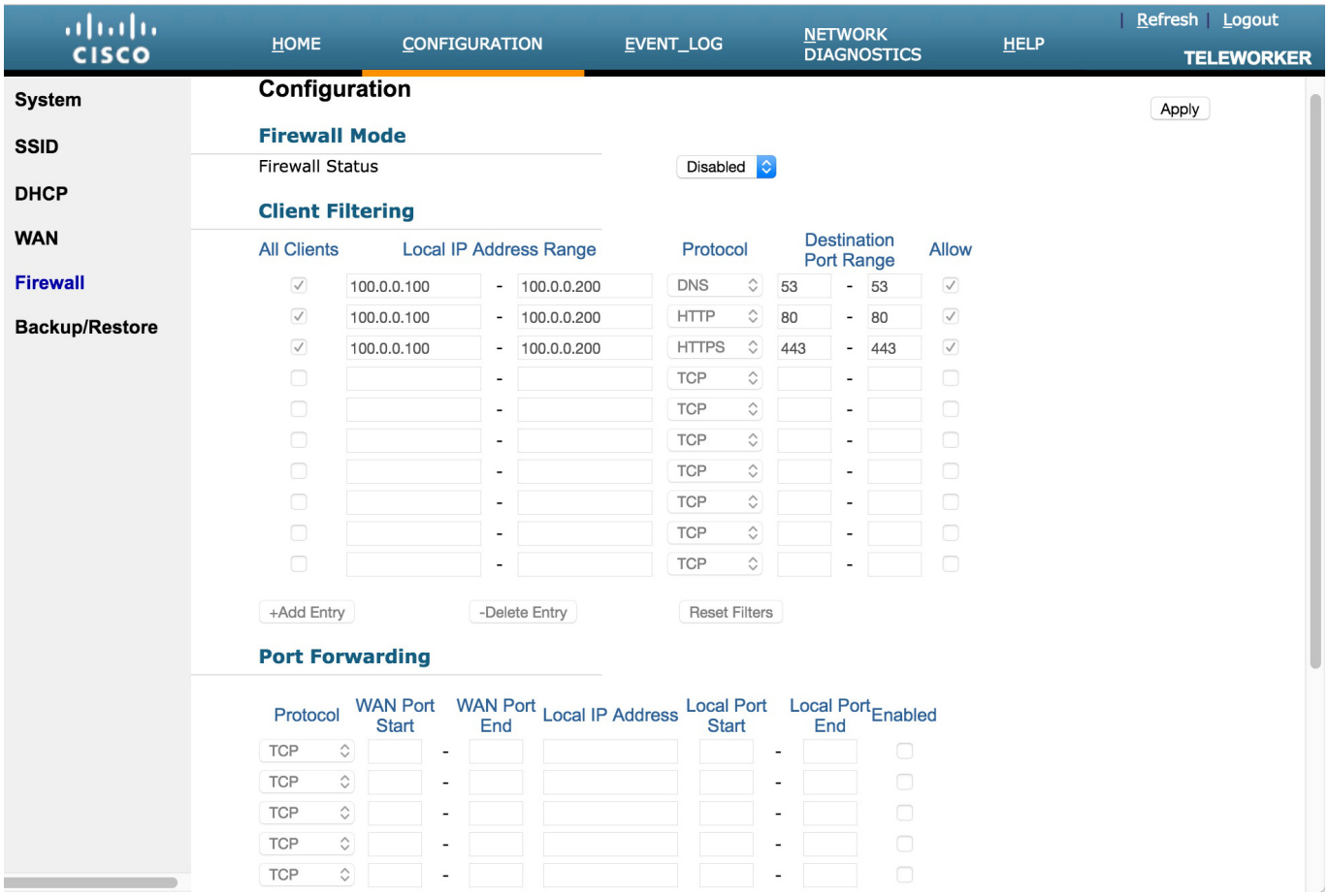
DMZ

The DMZ feature allows one network computer connected to a local LAN or WLAN to be exposed to the Internet for using special-purpose services such as Internet gaming. The DMZ feature forwards all the ports terminating on a WAN IP to one internal computer, whose address is set as the **DMZ IP Address**.

The DMZ feature, if enabled, will forward all incoming WAN packets to the LAN machine, except the CAPWAP control/data and packets which are destined to any ports and which have a port forwarding rule. The DMZ feature is not applicable to corporate networks such as Remote-LAN and Corp WLAN.

However, the Port Forwarding feature is more secure, compared to DMZ feature because the former only opens the ports you want to have opened, while DMZ opens all the ports of one computer, exposing the computer to the Internet/WAN.

Figure 2-8 Firewall Settings Page

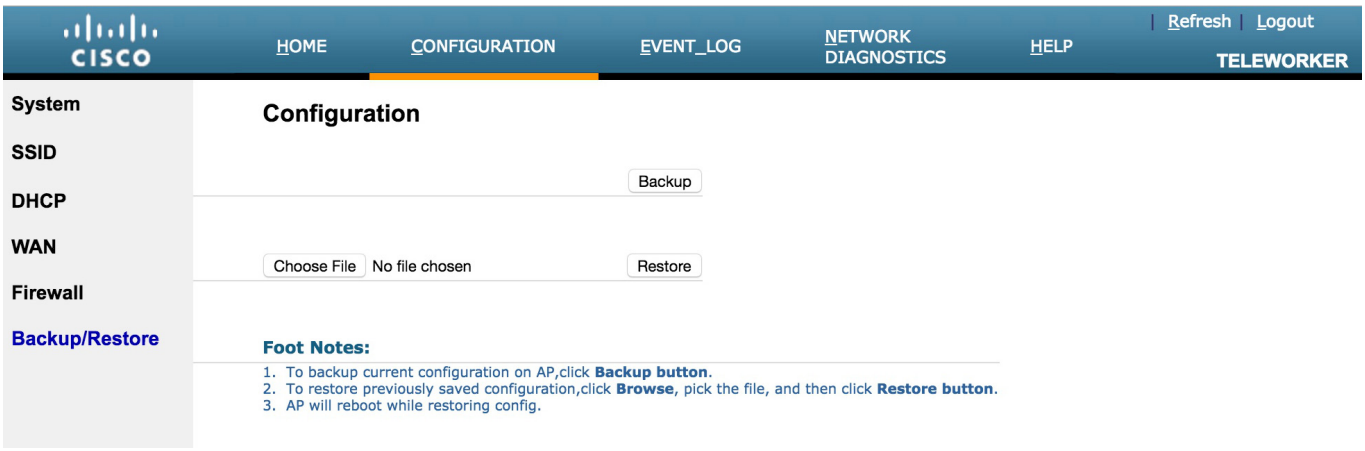


Backup/Restore

The Backup/Restore tab (see Figure 2-9) allows the following functions;

- To backup the contents of the AP's NVRAM (that is, the configuration file) for archiving or management purposes. For this, click **Backup**.
- To upload a configuration file to the access point. For this, click **Browse**, browse to and choose the configuration file, and then click **Restore**.

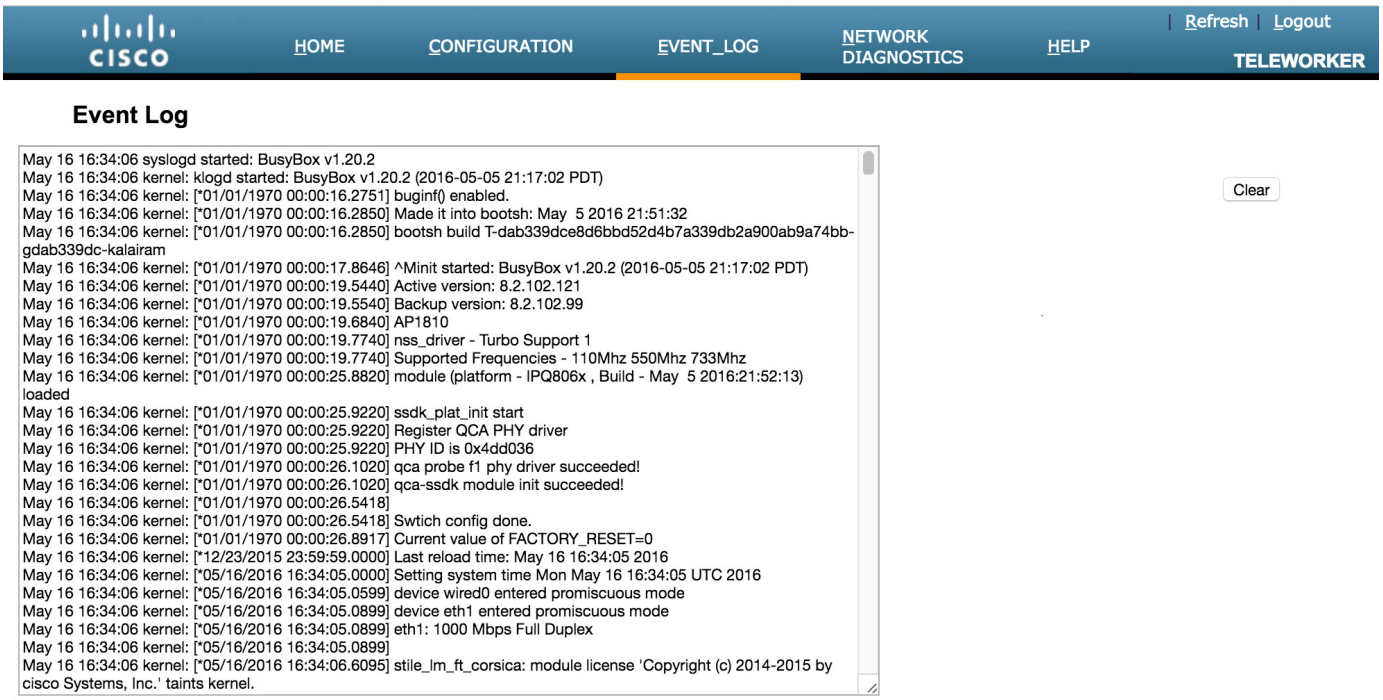
Figure 2-9 Backup/Restore Tab



Event Log Page

This page shows you the logged errors and allows you to clear the log. Click **Clear** to clear the log.

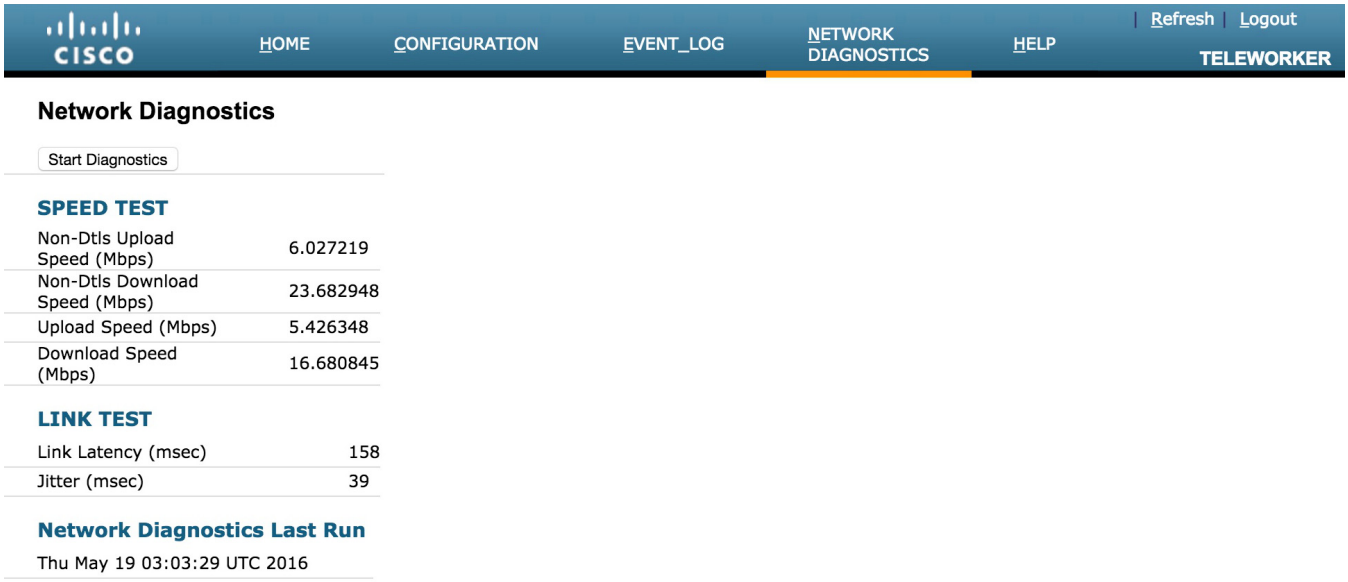
Figure 2-10 Event Log Page



Network Diagnostics

The Network Diagnostics page (see Figure 2-11) allows you to run the Speed Test and Link Test for the Network between AP and Controller. To run diagnostics, click **Start Diagnostics**.

Figure 2-11 Network Diagnostics



The functionalities of the Network Diagnostics tab are as follows:

- **Speed Test**—The Speed test feature calculates both the download and upload speeds (DTLS and non-DTLS) between the controller and the AP. It provides the network speed with DTLS and Non-DTLS connections.
  Using the Speed Test feature you can determine the non-DTLS throughput of the system, by running a speed test on demand. This allows for root cause failure analysis and debugging of network bottlenecks.
- **Link Test**—The Link test provides the link latency and the jitter values. Link latency monitors the round-trip time of the CAPWAP packets (echo request and response) from the access point to the controller. The round-trip time is calculated in milliseconds. The jitter value is then calculated using the link latency values. Jitter is the amount of variation in latency/response time, in milliseconds.
- **Network Diagnostics Last Run**—Shows the details of the last run diagnostics along with its timestamp.

Note You can run the Speed and Link tests from the AP's GUI, the controller's GUI, and the controller's CLI.

Running Network Diagnostics via Controller CLI

From the wireless LAN controller CLI, you can use the following command to run network diagnostics: **show ap network-diagnostics** *ap-name*

Example:

```
(Cisco Controller)> show ap network-diagnostics ap1
AP network diagnostics has been initiated
Waiting for network diagnostics to complete
====================== AP Network Diagnostics ====================
Speed Test Results:
DTLS Upload Speed       ................ 10.83 Mbps
DTLS Download Speed     ................ 9.87 Mbps
Non-DTLS Upload Speed   ................ 22.29 Mbps
Non-DTLS Download Speed ................ 24.44 Mbps
Link Test Results:
Latency   ................ 1 mSec
Jitter    ................ 0 mSec
(Cisco Controller)>
```

Running Network Diagnostics via Controller GUI

You can initiate the network diagnostics tests from the **Network Diagnostics** tab in the controller GUI. This tab is available at **Wireless > All APs > Details**.