Understanding the Access Point GUI

This chapter provides the following information:

Accessing the GUI

Follow these steps to access the Cisco Aironet 1815t Series OfficeExtend access point GUI.

Step 1 Connect your laptop to the local Ethernet port 1, or 2 on the 1815t Series OfficeExtend access point.

Note Ethernet port 4 (Remote LAN port) may not be used to configure the 1815t Series OfficeExtend access point.

Step 2 With the 1815t 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 1815t 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 1815t Series Office Extend Access Point Login page is displayed.

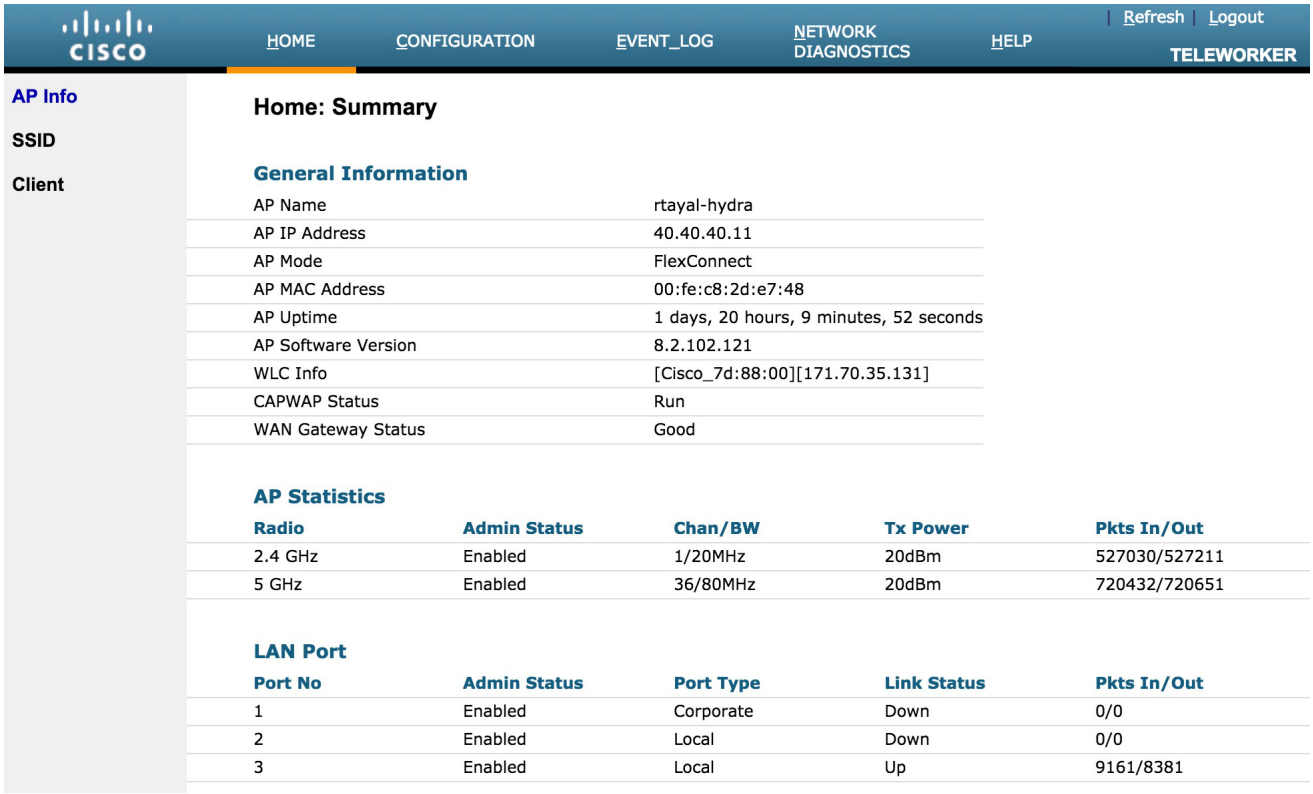
Step 3 When prompted, enter the username and password to log into the access point.

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

The 1815t Series OfficeExtend Access Point welcome page is displayed.

Step 4 On the 1815t Series OfficeExtend Access Point welcome page, click **Enter**. The 1815t 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.

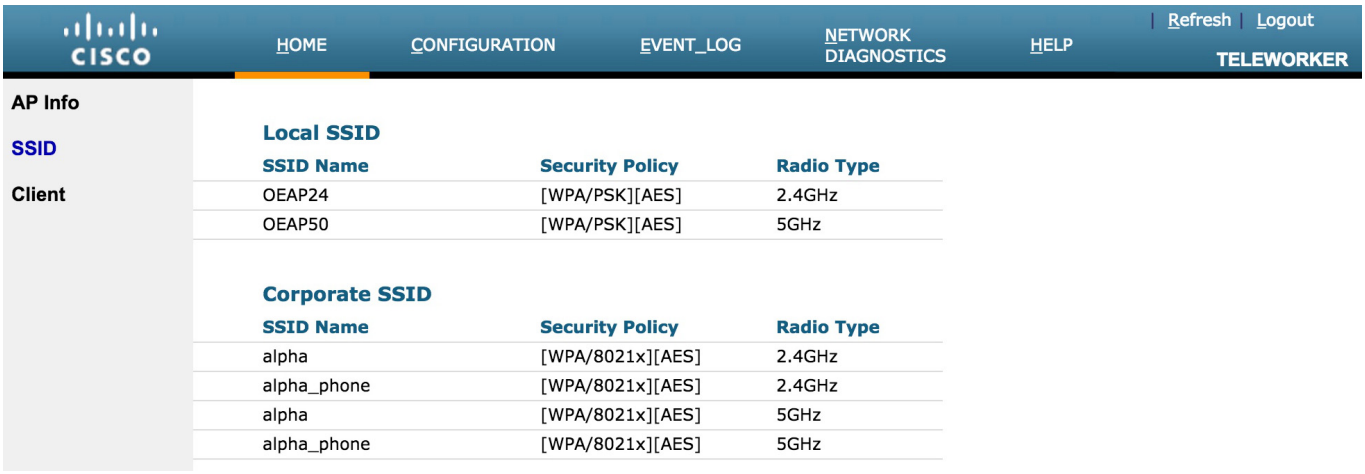
The **CAPWAP** status shows the status of the AP's CAPWAP connection with the controller.

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.

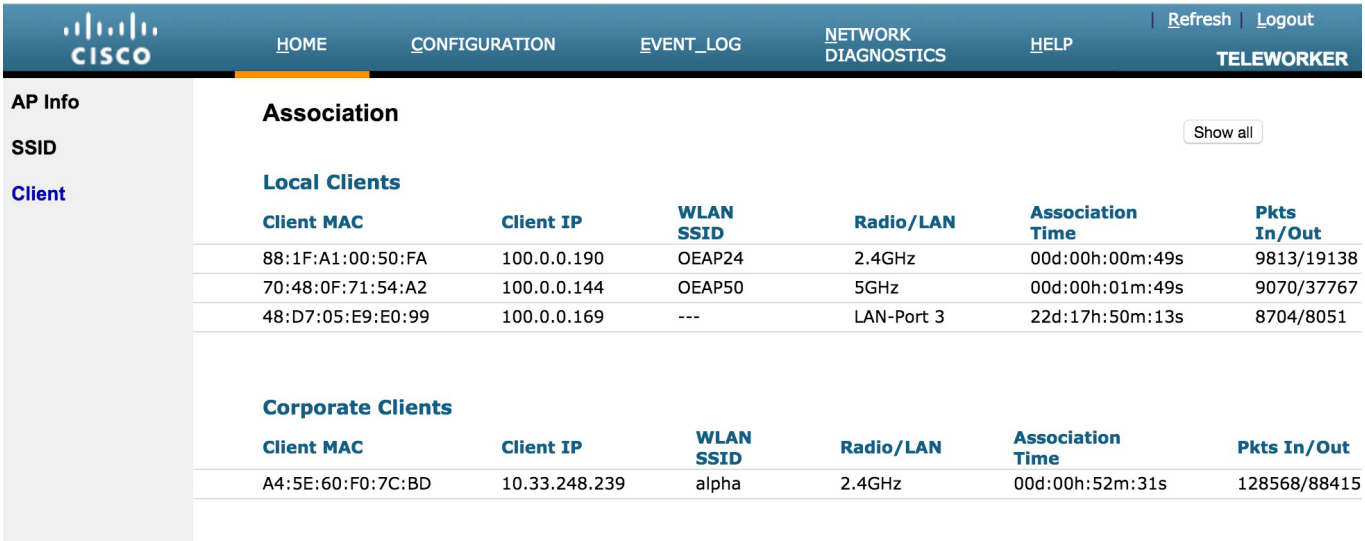
Figure 2-2 Home–SSID Tab



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:

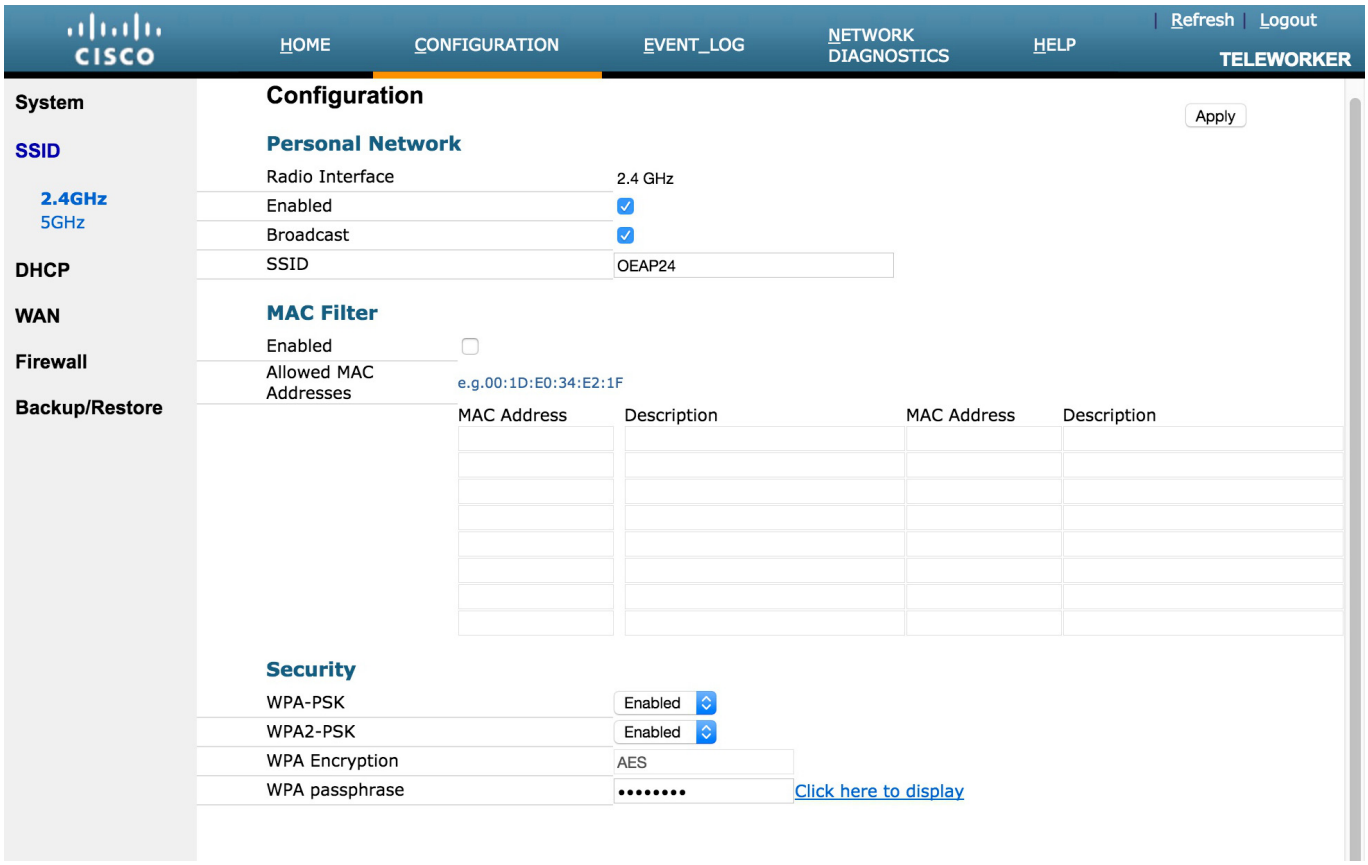
- **Enabled**—Check this check box to set a personal SSID on this radio.
- **Broadcast**—Check this check to broadcast the personal SSID on this radio.
- **SSID**—Specify the personal SSID, which will be the network's name.

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



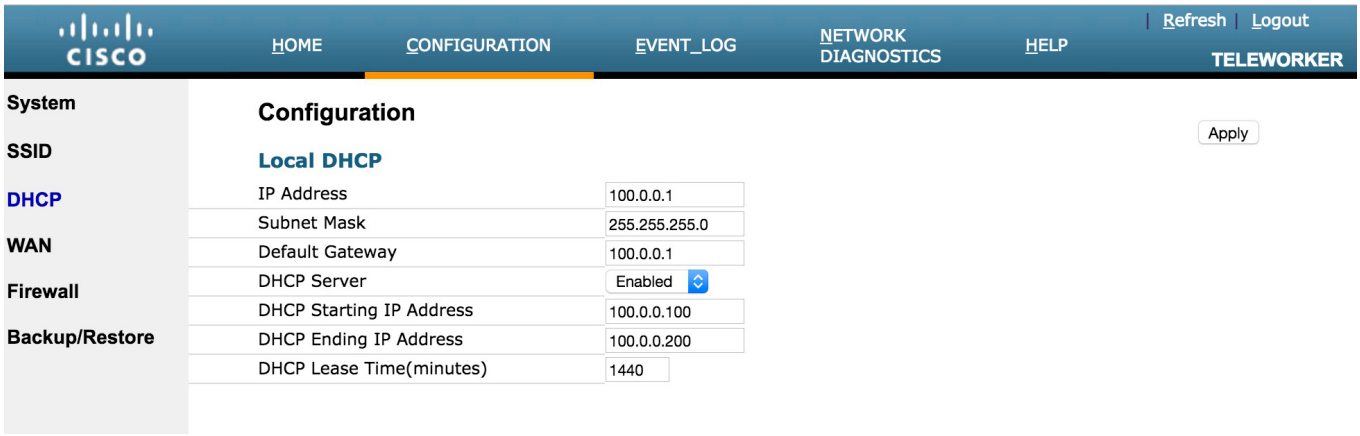
DHCP Tab

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.

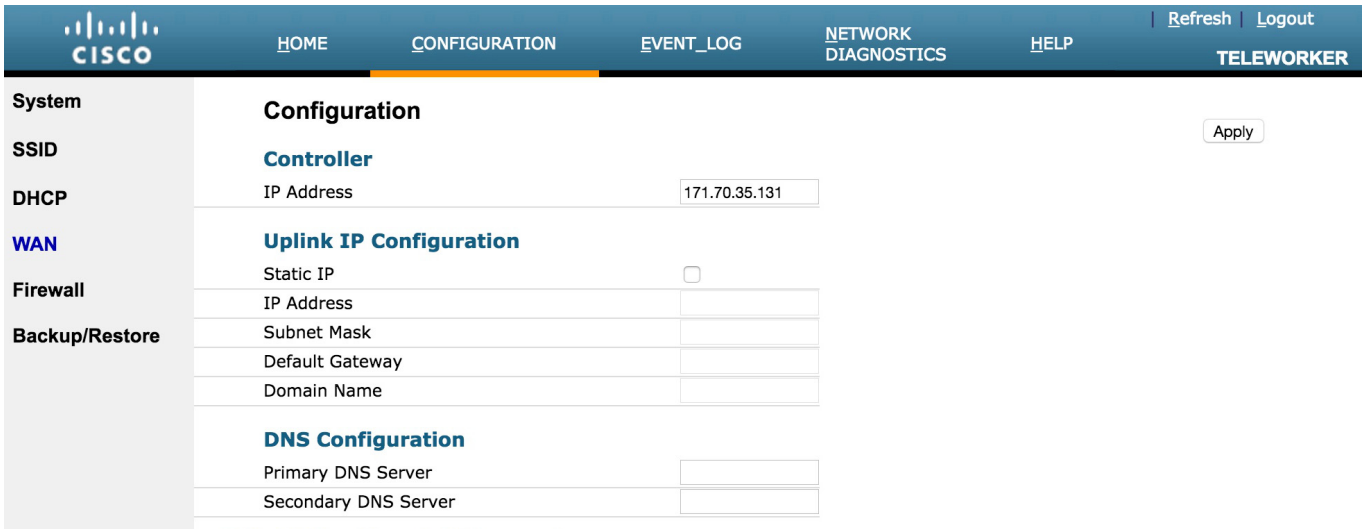
In the **Uplink IP Configuration** section, you can set the following parameters for IP configuration of the WAN port:

- **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.

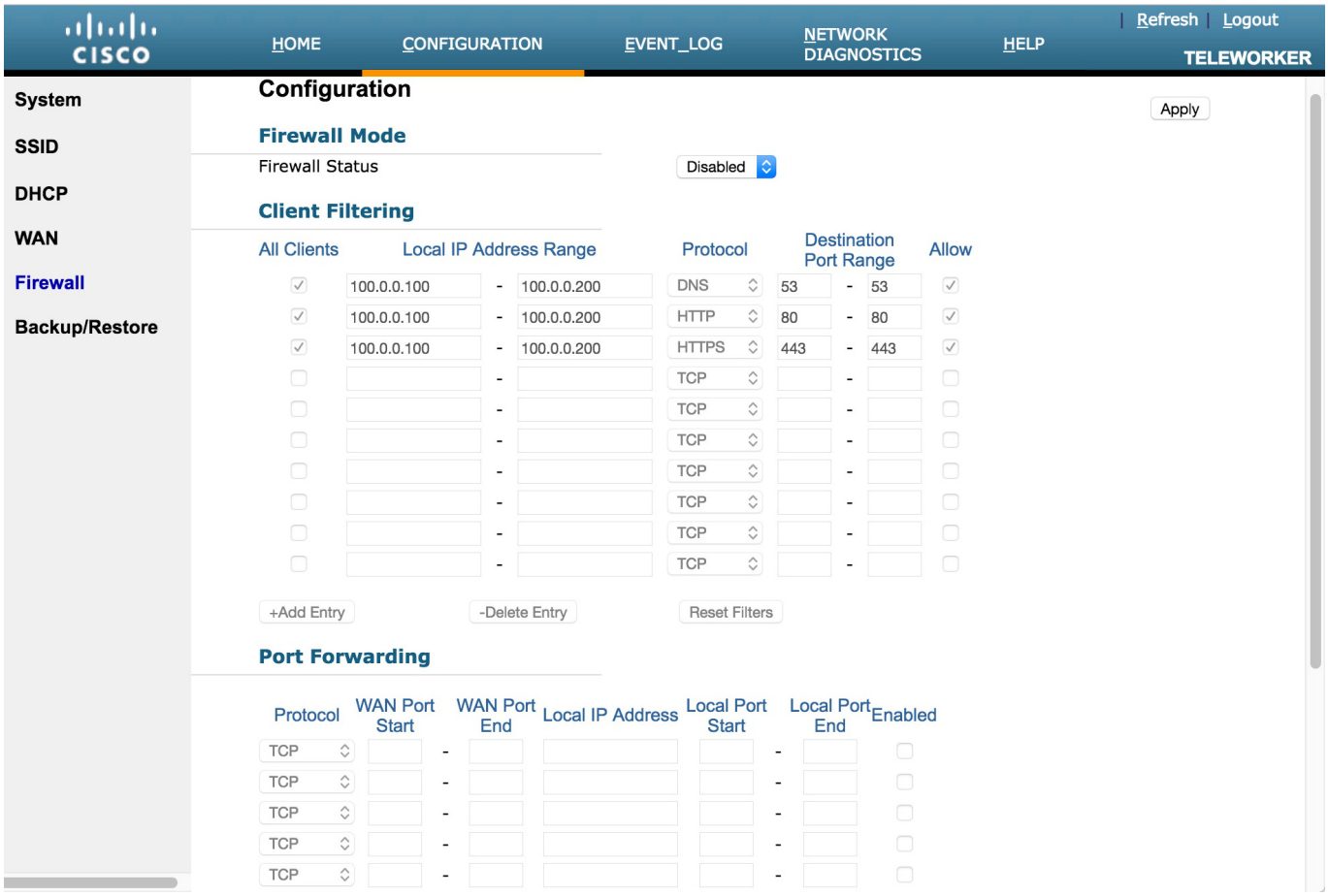
DMZ

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

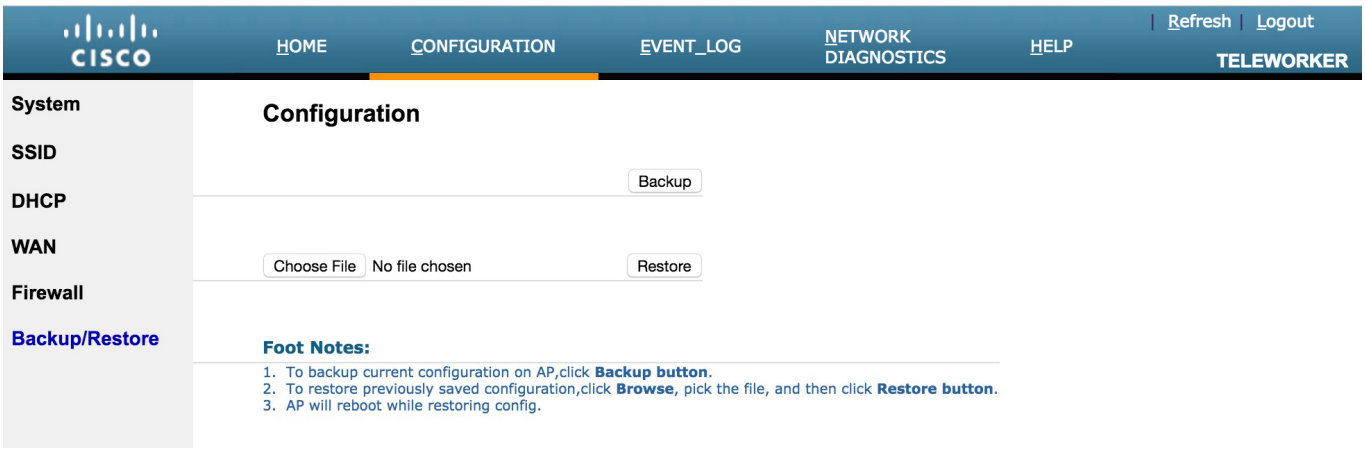


Backup/Restore

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**.

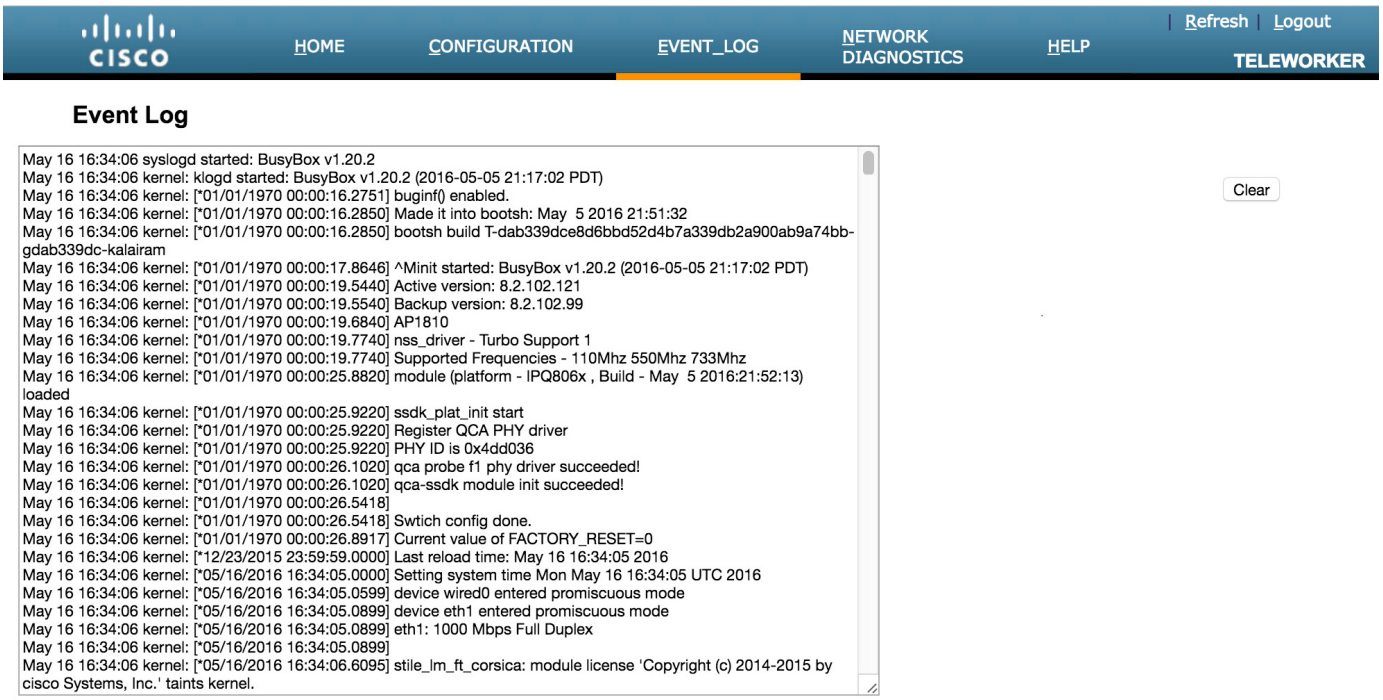
Figure 2-9 Backup/Restore Tab



Event Log Page

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

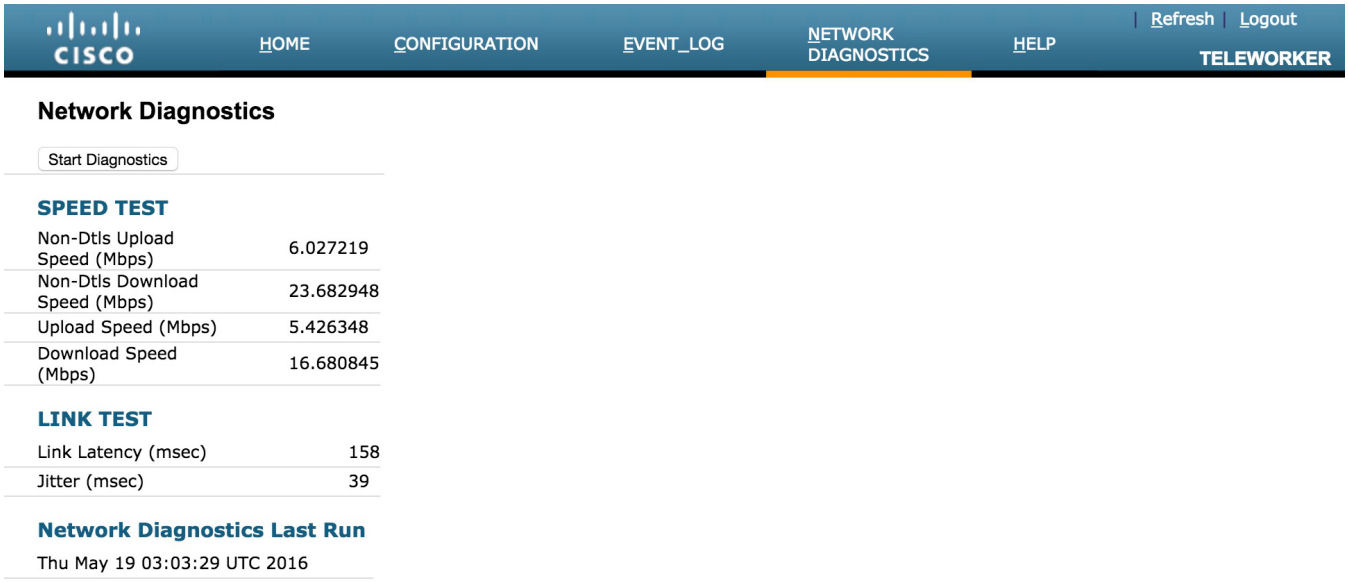
Figure 2-10 Event Log Page



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**.