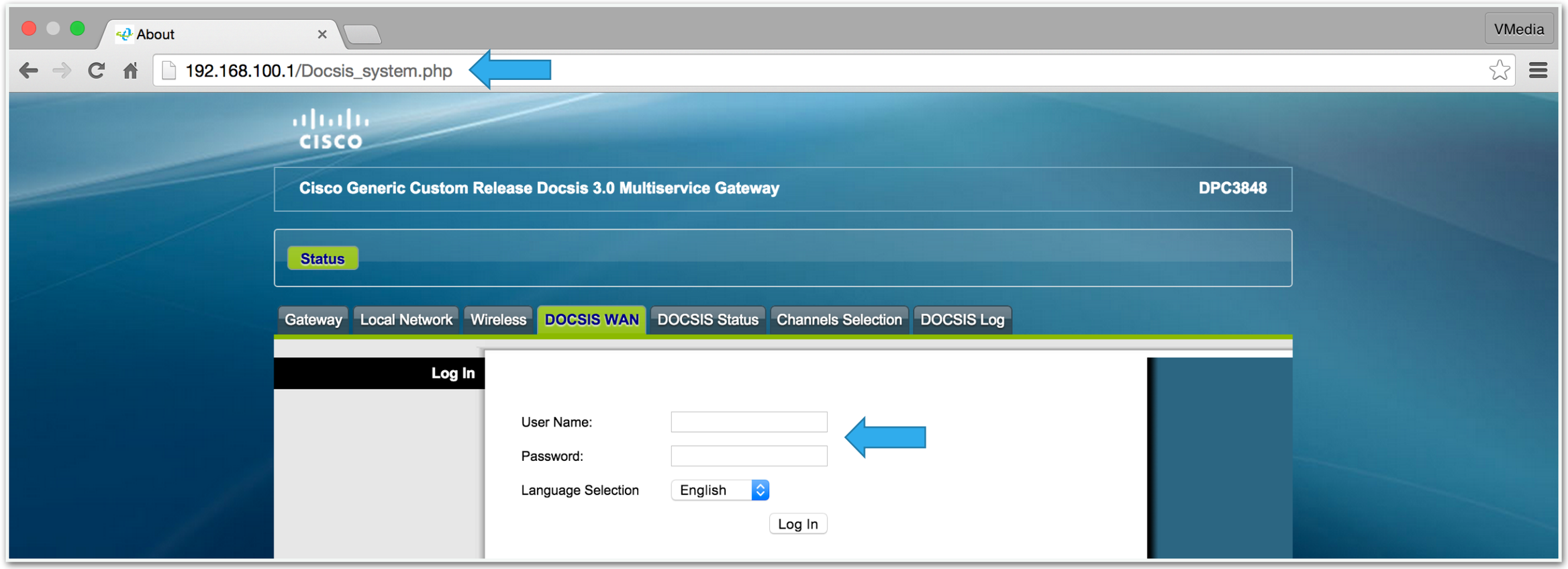
CISCO™ DPC3848

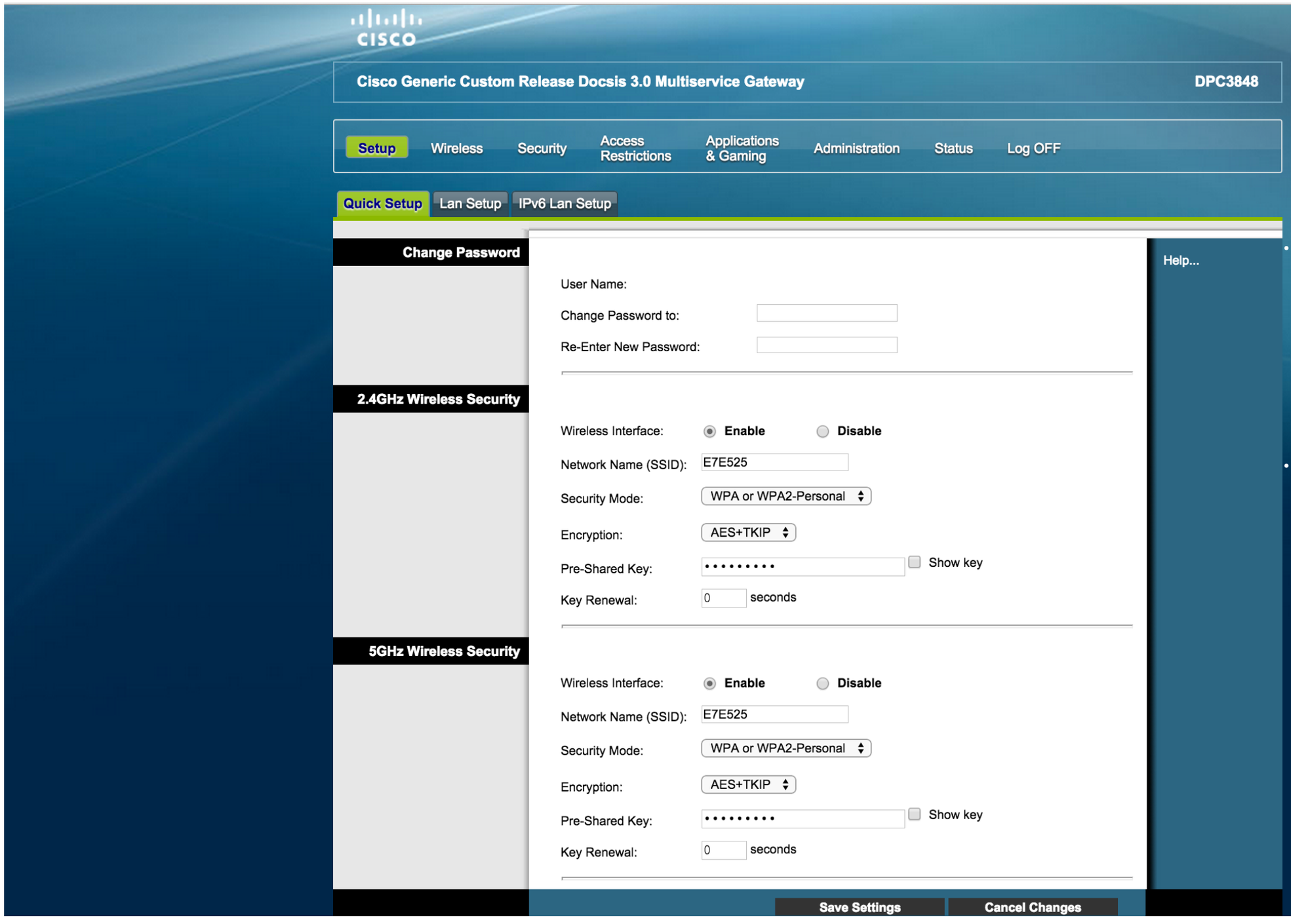
Manual

Login to DCP3848



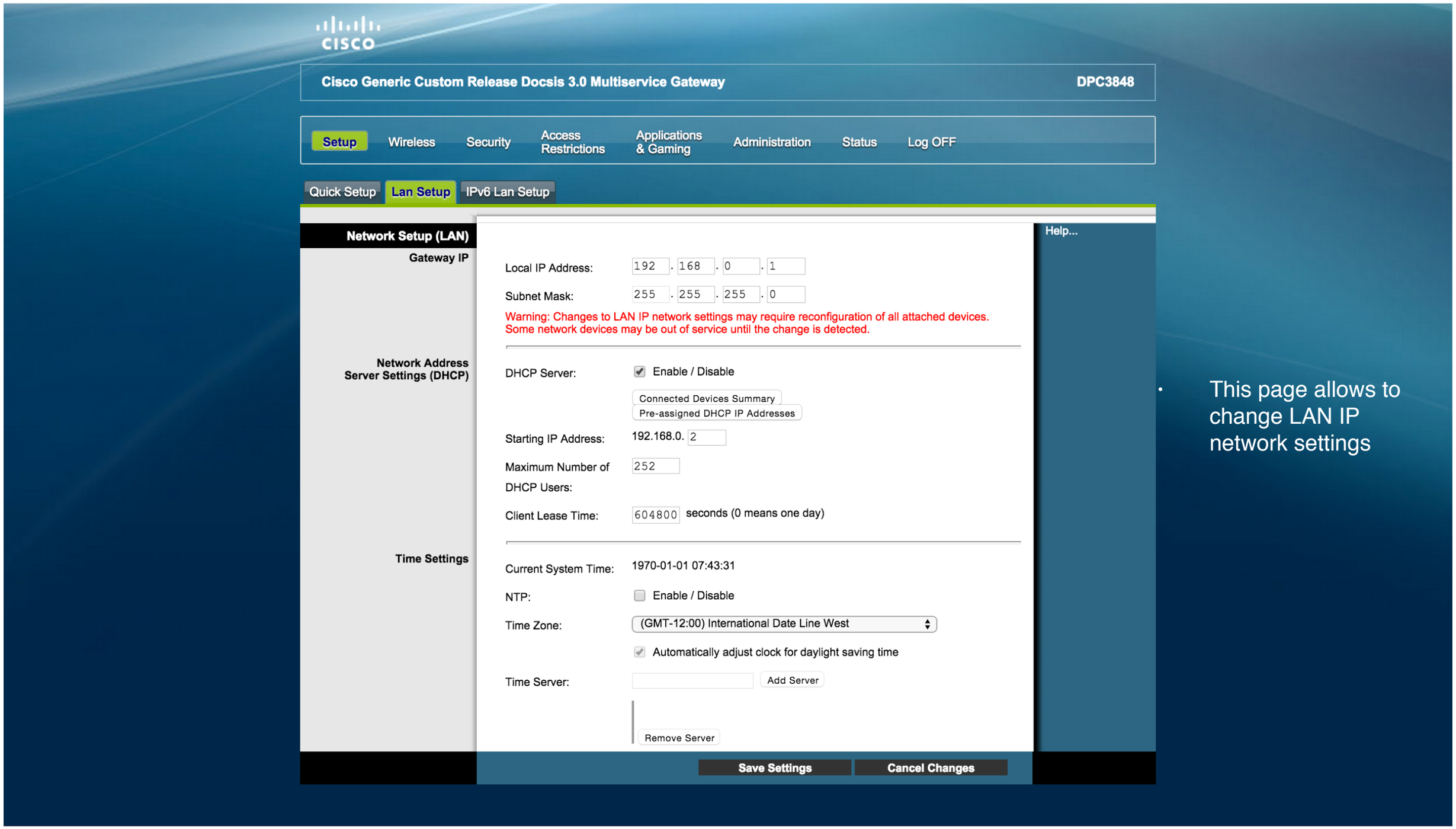
- **To access the modem enter the following IP address *192.168.100.1* in the address bar of your web browser**
- **To log into the modem select: *Status Tab / DOCSIS WAN***
- **Leave both User Name and Password section blank**
- **Select *Log In* to login to the modem**

Setup Tab / Quick Setup



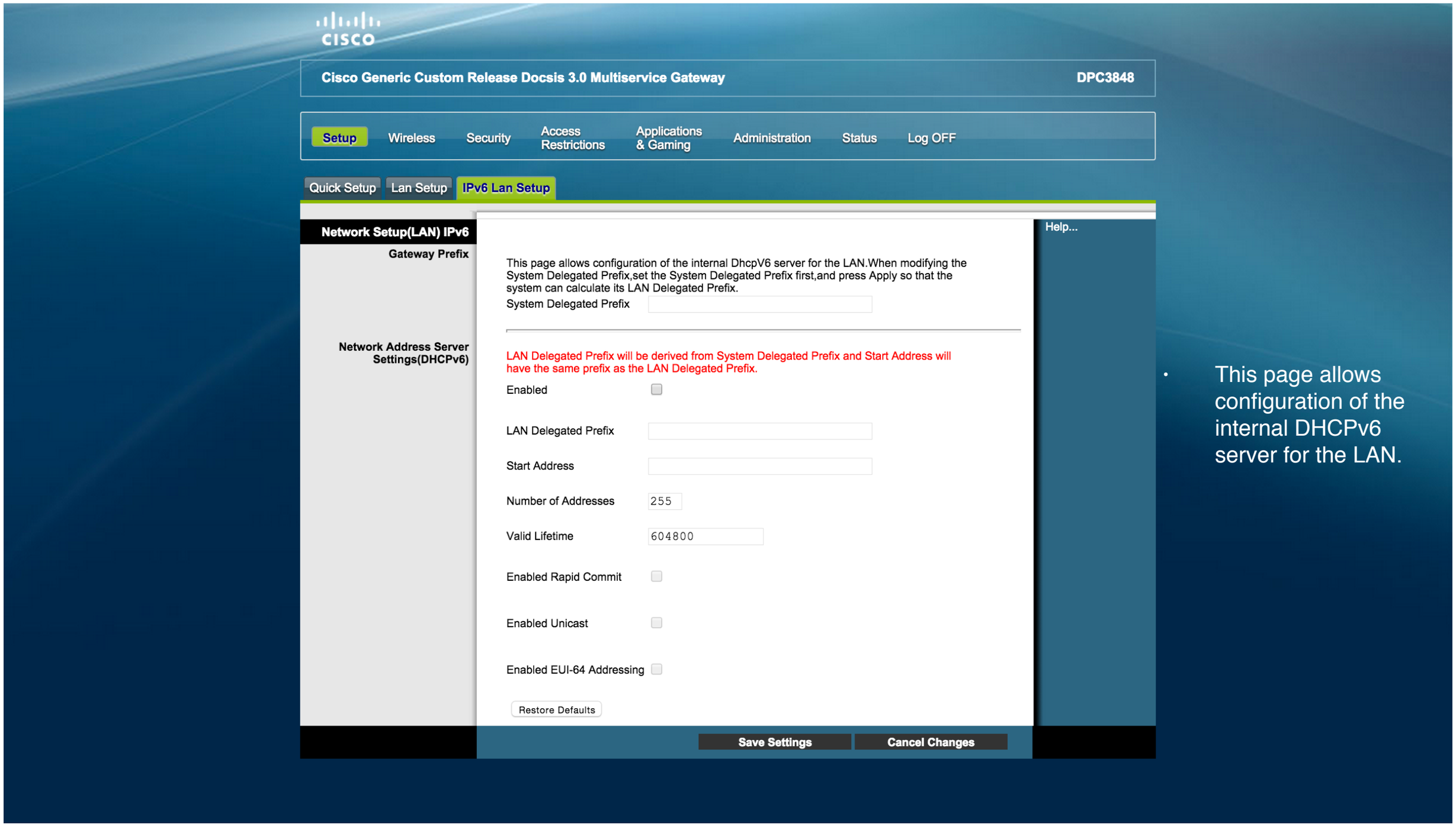
- Wireless Security settings and Password to access modem can be changed in this page
- The following wireless security mode options are supported: Disable, WEP, WPA-Personal, WPA2-Personal, WPA2-Mixed, WPA-Enterprise, and WPA2-Enterprise.

Setup Tab / IPv6 Setup



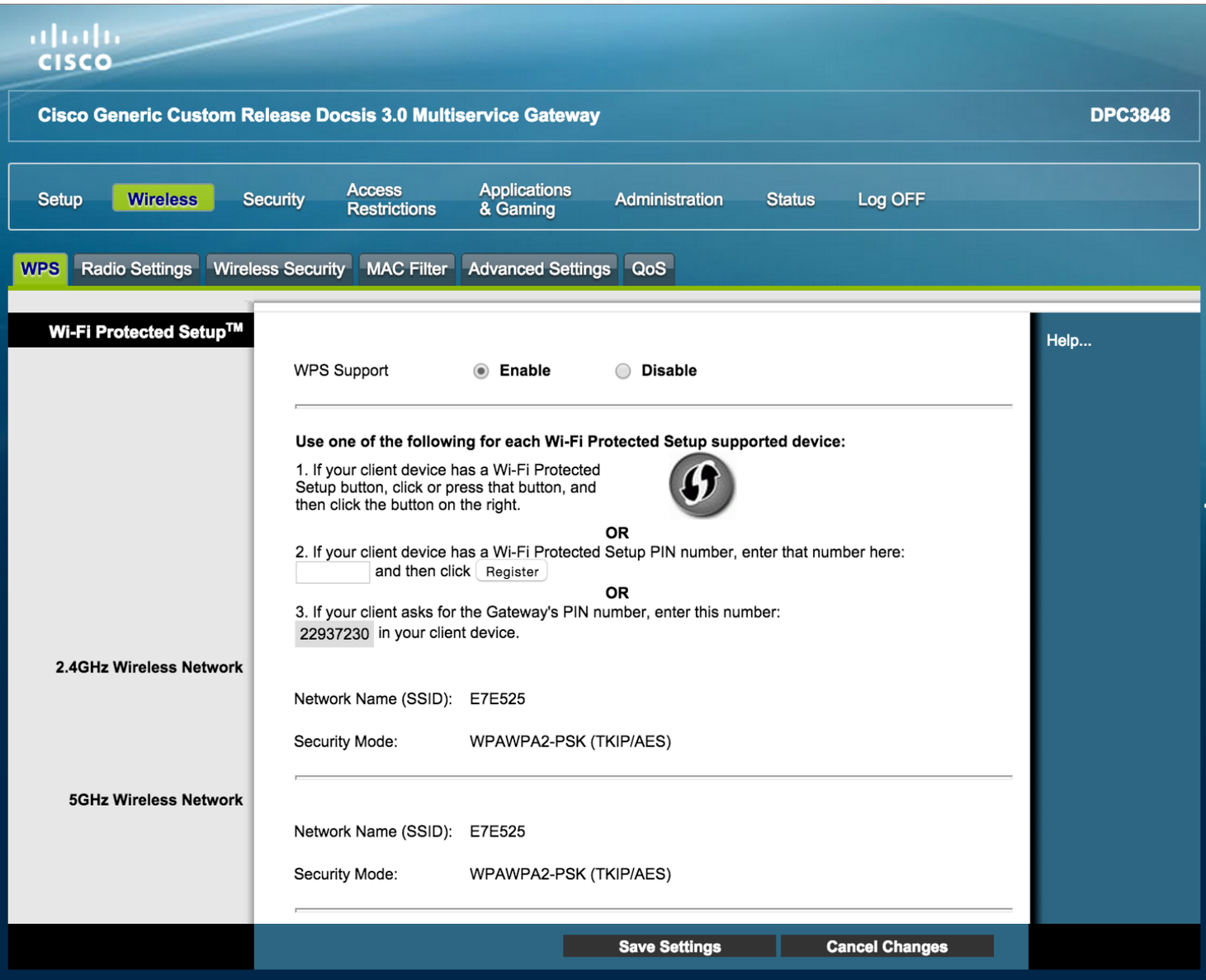
- This page allows to change LAN IP network settings

Setup Tab / IPv6 Setup



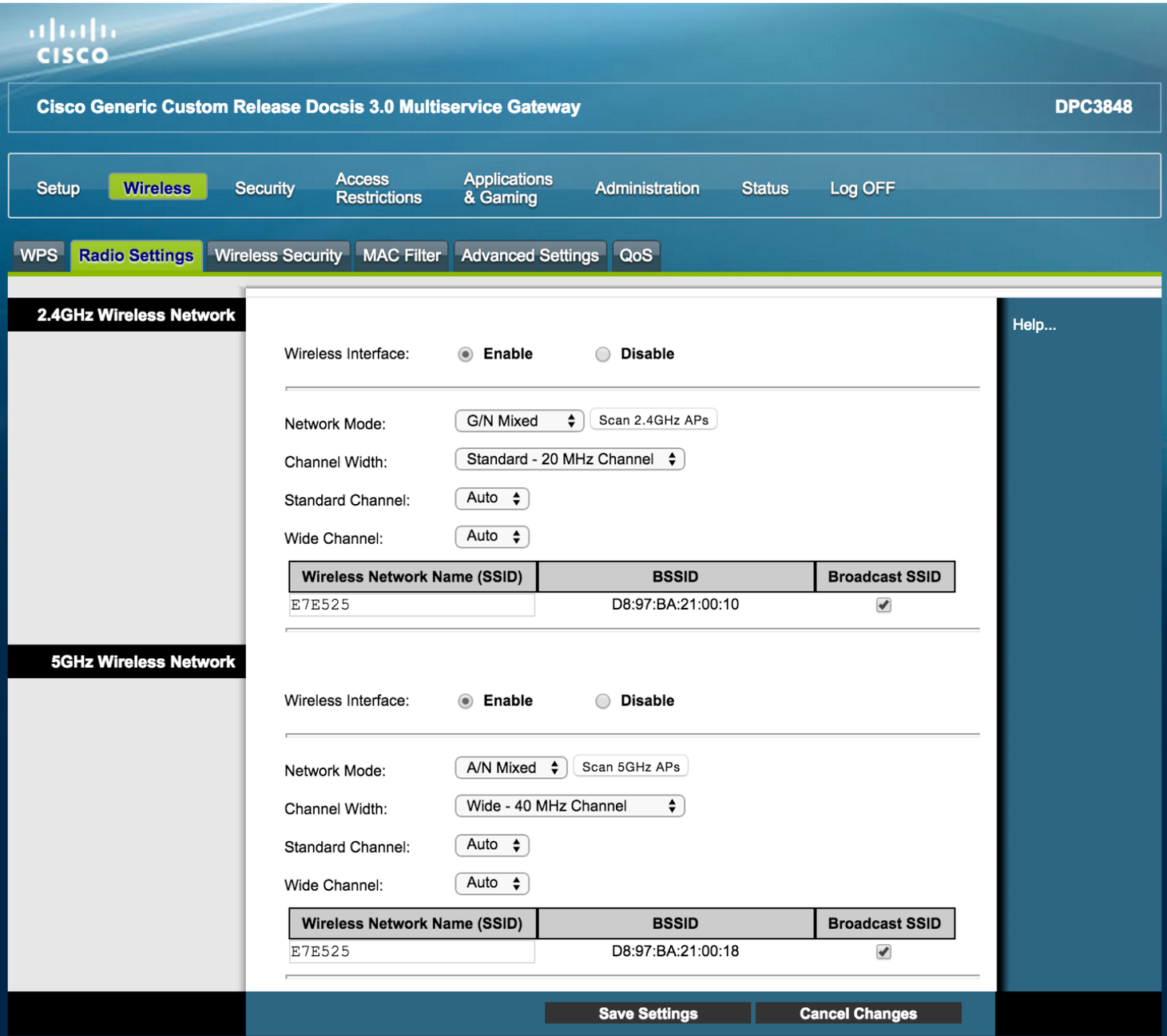
- This page allows configuration of the internal DHCPv6 server for the LAN.

Wireless Tab / WPS



- This screen allows you to choose your wireless network mode and other basic features.

Wireless Tab / Radio Settings



- This screen allows you to choose your wireless network mode and other basic features.

Wireless Network: You can enable or disable wireless network with this radio button.

Wireless Configuration: The default is Manual. Select Wi-Fi Protected Setup to set up your network using this option. The Wi-Fi Protected Setup feature automatically configures an encryption-secured, wireless network. To use Wi-Fi Protected Setup, you must have at least one other device that supports Wi-Fi Protected Setup in your network. After you have configured your Wi-Fi Protected Setup devices, you can manually configure other devices. Scroll down to the end of the help page for more information.

Network Mode: Determines which Mode the N card will run in.

Radio Band: You can select the radio band.If you select Enabled 2.4GHz, the device can support B/G/N Mixed mode.And if you select Enabled 5GHz,it can support A/N mixed mode.

Channel Width: You can select the channel bandwidth manually for Wireless-N connections. For best performance in a network using Wireless-N, Wireless-G, and Wireless-B devices, keep the Wide - 40MHz Channel. Wireless-N connections will use the 40 MHz channel, while Wireless-G and Wireless-B will still use the 20 MHz channel. For Wireless-G and Wireless-B networking only, select Standard - 20MHz Channel. Then only the 20 MHz channel will be used.

Standard Channel: If you selected Wide - 40 MHz Channel for the Radio Band setting, then the appropriate Standard Channel setting will be automatically selected, depending on the Wide Channel setting. If you selected Standard - 20 MHz Channel as the Radio Band setting, select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must broadcast on the same channel in order to communicate.

Wide Channel: If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu, and then the appropriate Standard Channel setting will be automatically selected.

Wireless Network Name (SSID): You may choose an easy remember name for your wireless network or simply use the default value. The value you enter here will be viewable on PCs and other wireless client devices as the wireless network name.

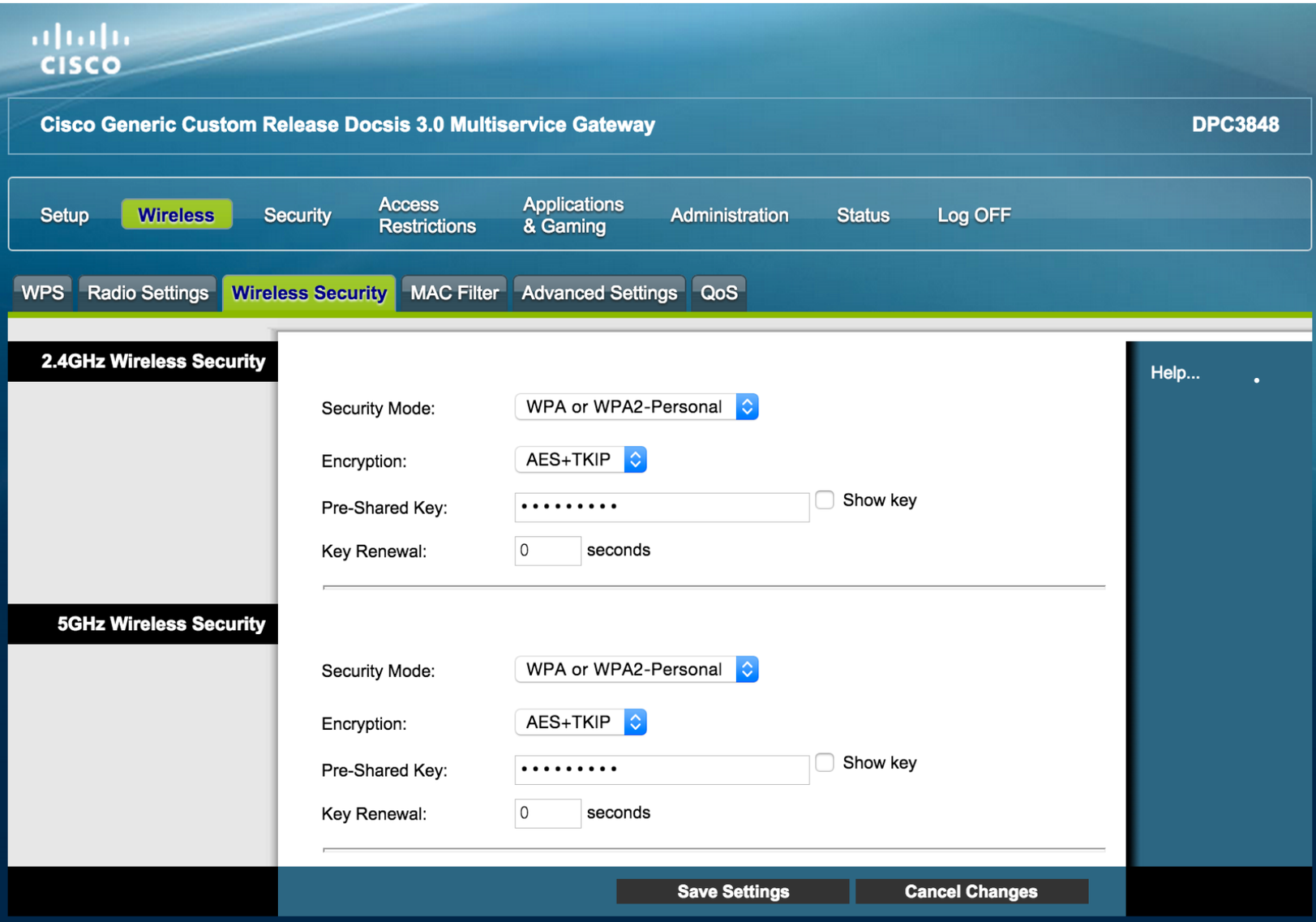
Wireless SSID Broadcast: If this feature is enabled, wireless clients will detect the SSID broadcast by the device when they survey the local area for wireless networks to join. To broadcast the devices SSID, keep the default setting, Enable. If you do not want to broadcast the devices SSID, then select Disable.

Wi-Fi Protected Setup Option 1: An administrator can push the Wi-Fi Protected Setup button on the Basic Wireless Settings screen or the button on the front panel of the Gateway to allow a user to register a wireless client with the Gateway. The user needs to push the Wi-Fi Protected Setup software button on the client side at the same time as the Wi-Fi Protected Setup button is pushed on the Gateway. The connection will be automatically set up.

Wi-Fi Protected Setup Option 2: This is the most secure option for an administrator to register a user's wireless client with the Gateway. The user needs to give the administrator their Wi-Fi Protected Setup PIN number, which is found in the client Wi-Fi Protected Setup utility. After entering the client's Wi-Fi Protected Setup PIN number, the administrator registers the user. The user can then connect to the Gateway.

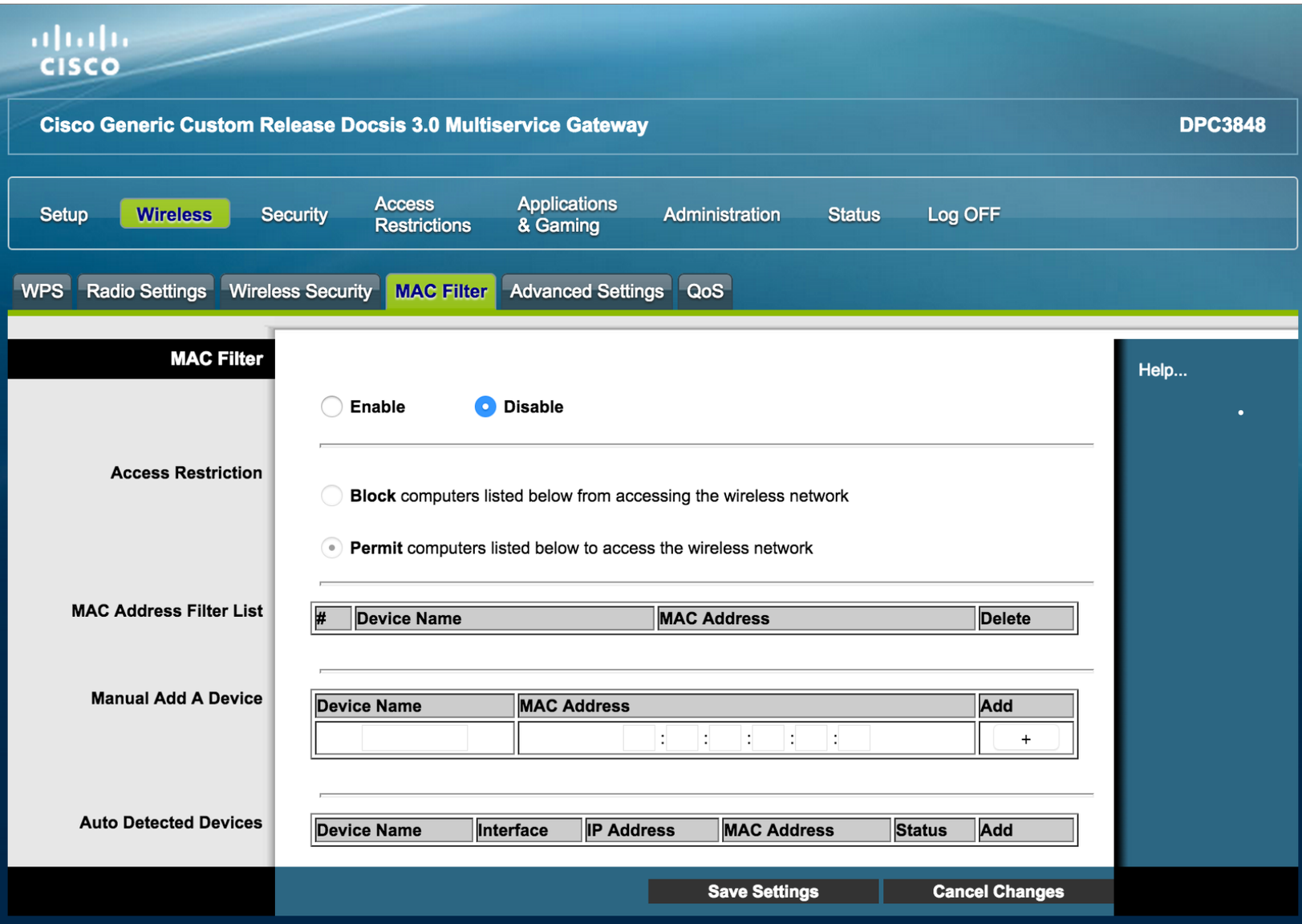
Wi-Fi Protected Setup Option 3: The Gateway's Wi-Fi Protected Setup PIN number is on the label on its bottom panel. Using any Wi-Fi Protected Setup client utility or Microsoft Vista, the user needs to enter the Gateway's Wi-Fi Protected Setup PIN number into the client device.

Wireless Tab / Wireless Security



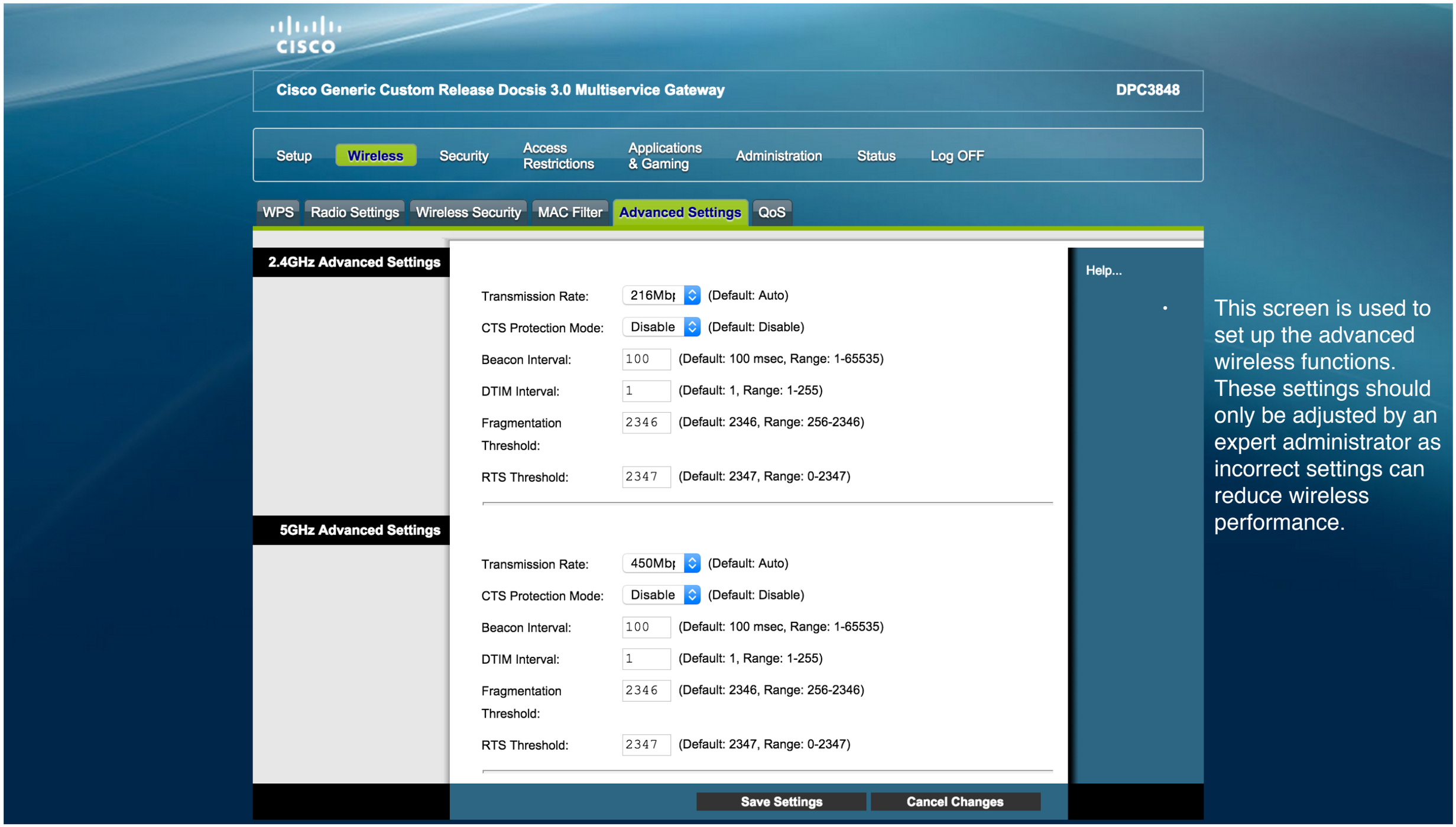
The following wireless security mode options are supported: Disable, WEP, WPA-Personal, WPA2-Personal, WPA2-Mixed, WPA-Enterprise, and WPA2-Enterprise.

Wireless Tab / MAC Filter



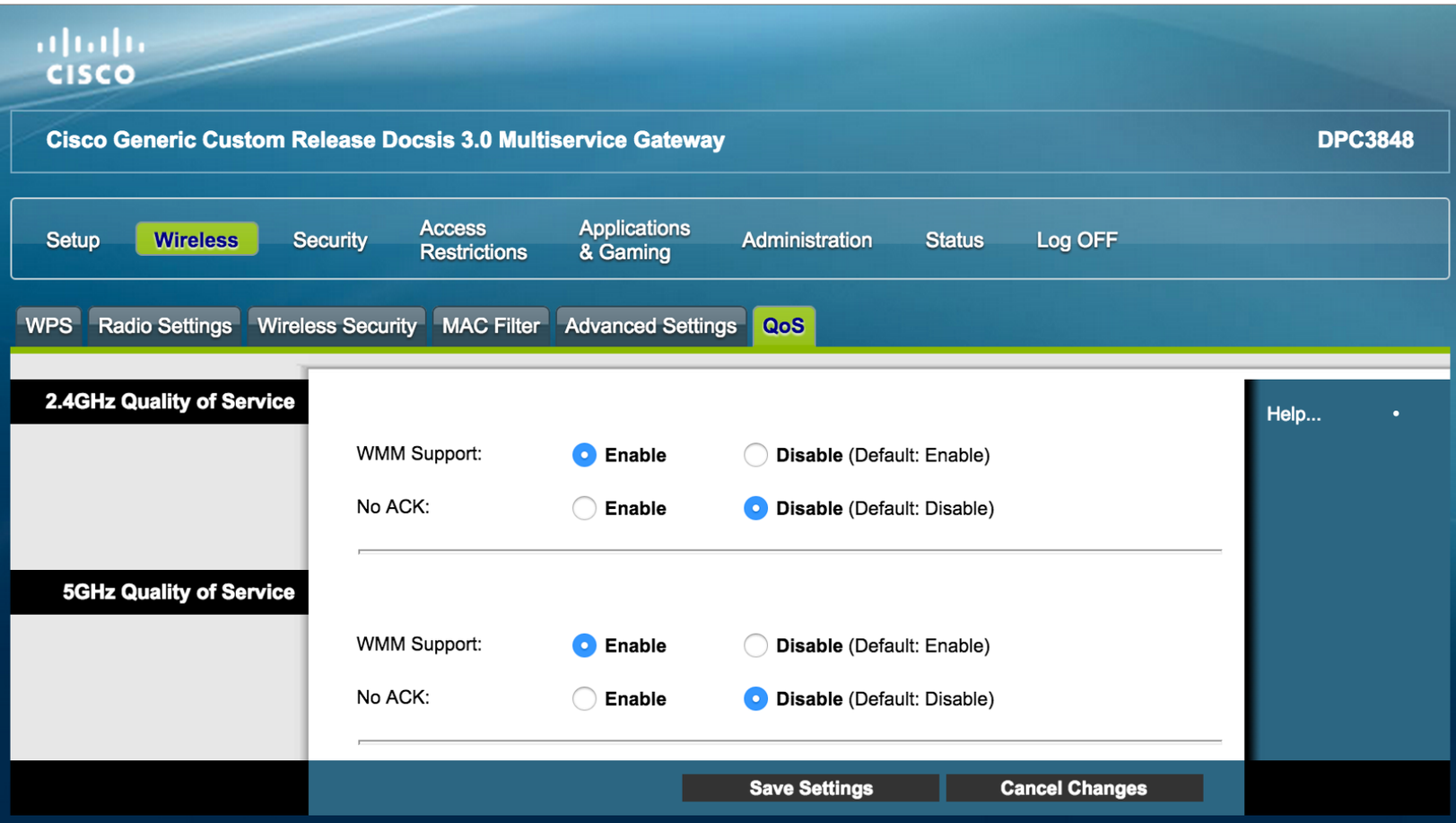
Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network radius.

Wireless Tab / Advanced Settings



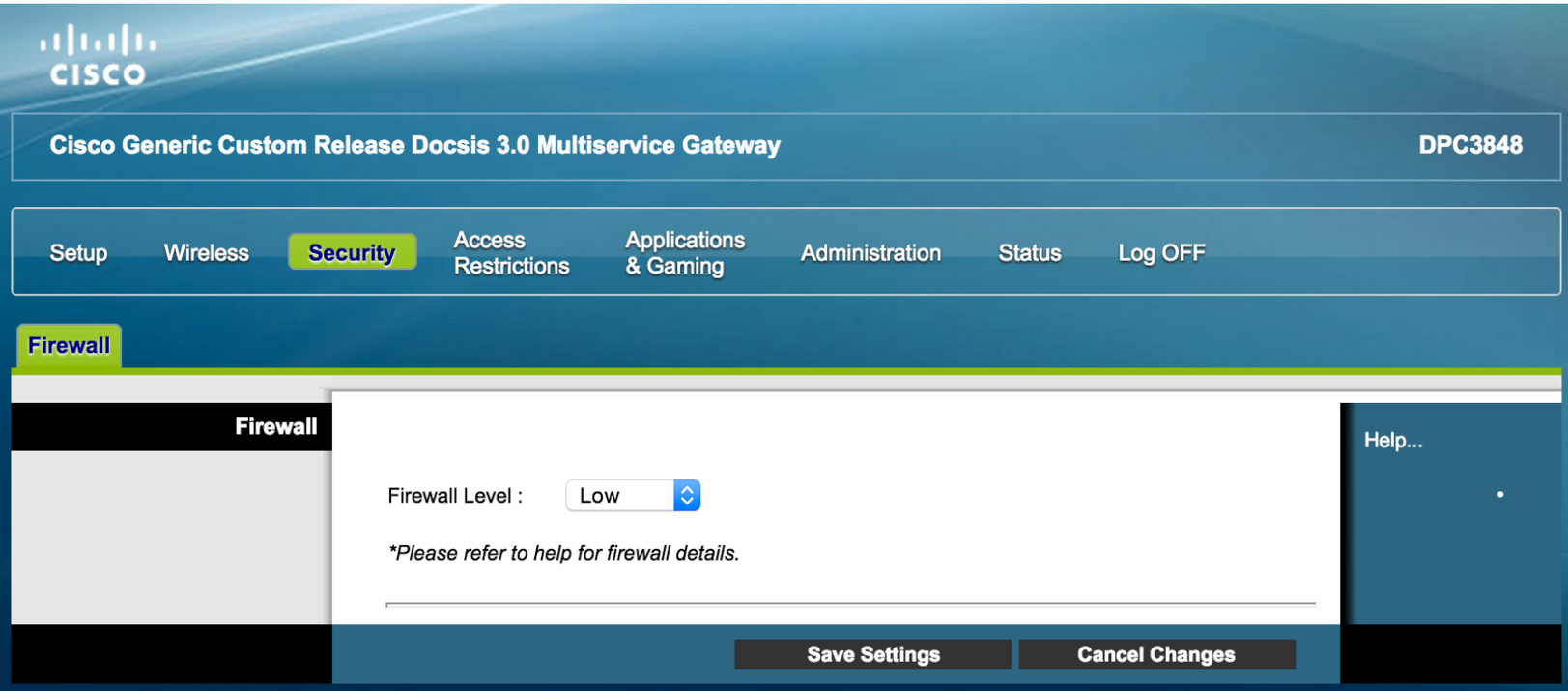
This screen is used to set up the advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Wireless Tab / QoS



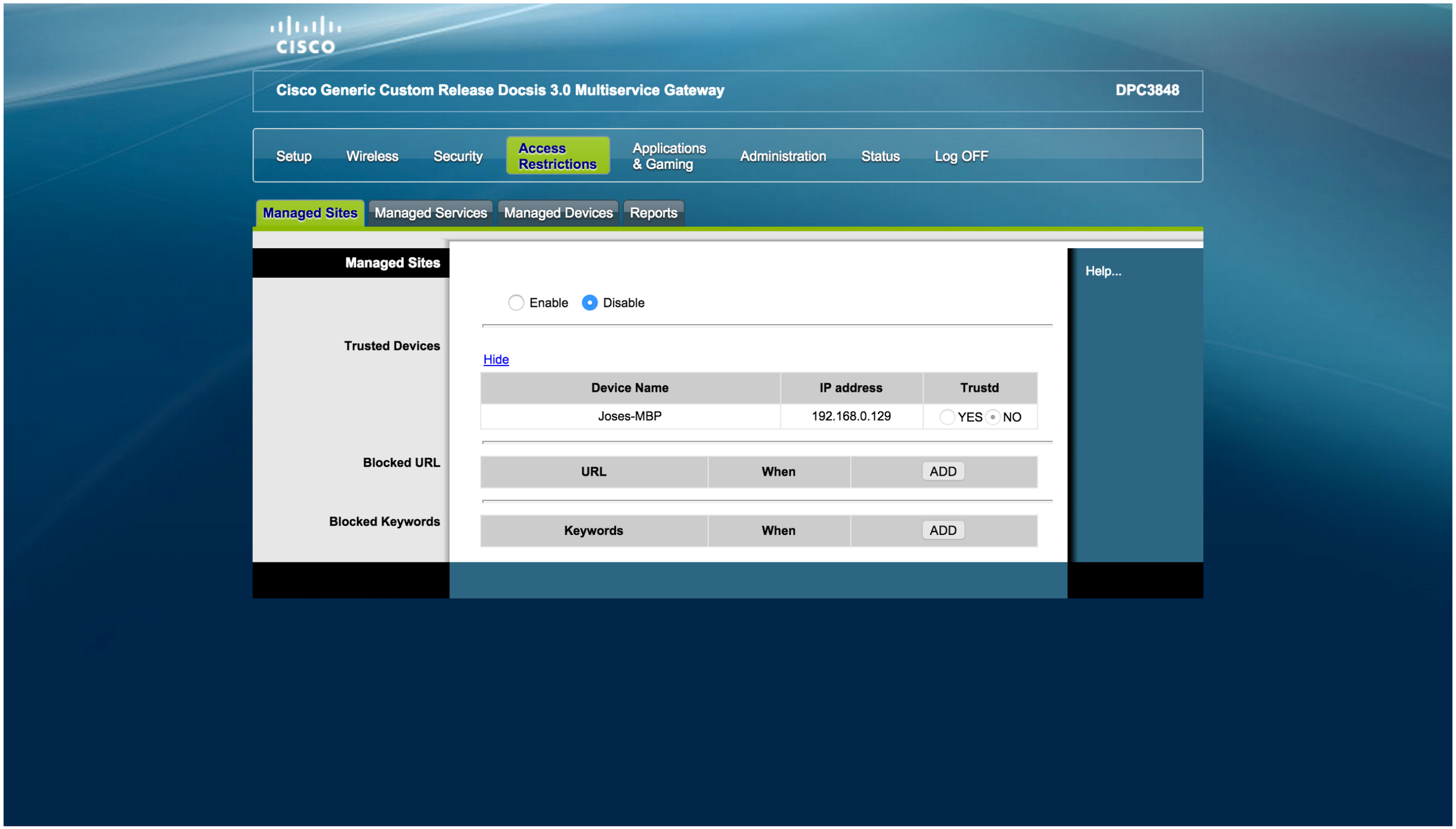
The Quality of Service (QoS) settings allow you to specify priorities for different types of traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic.

Security Tab / Firewall

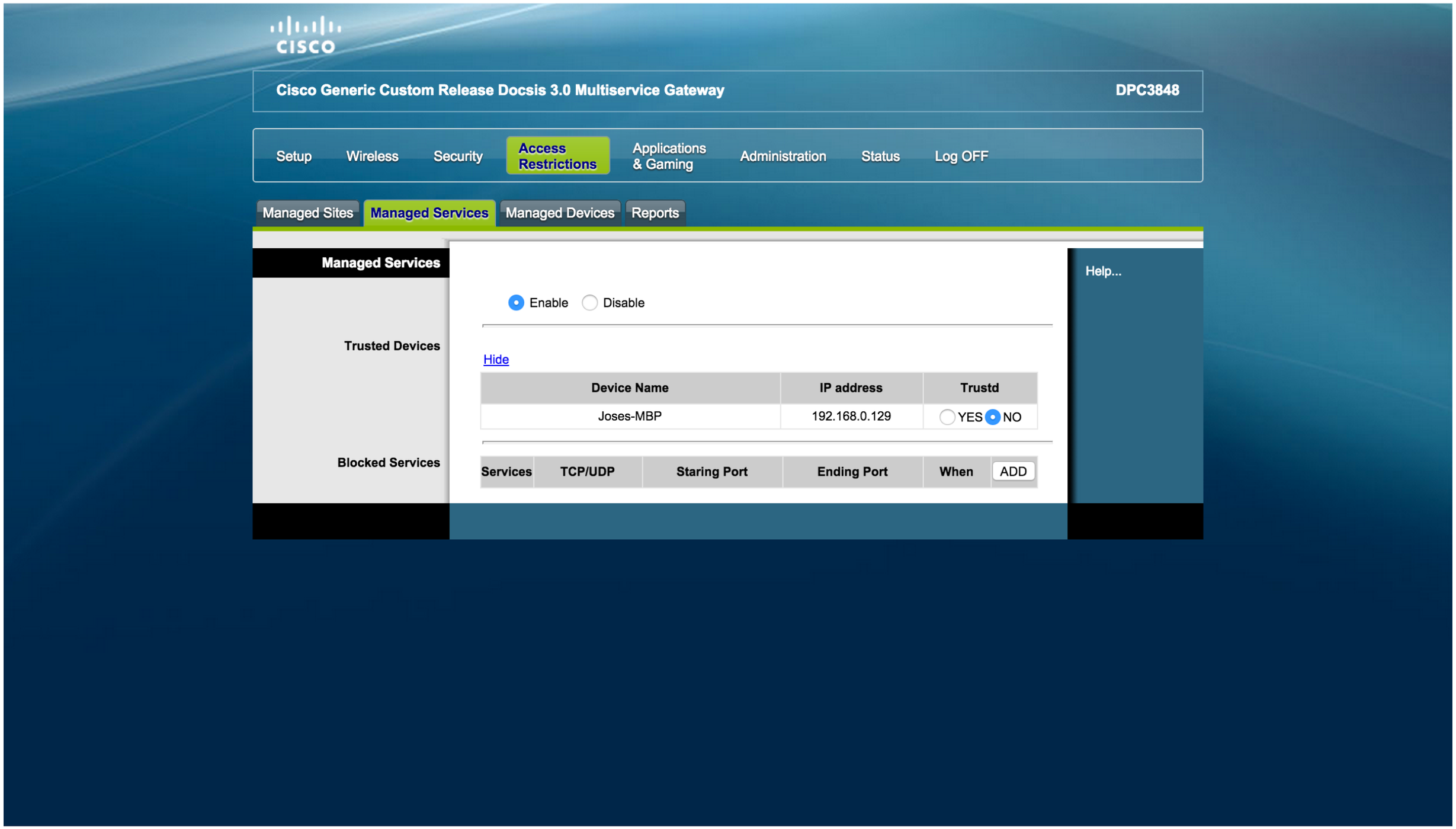


The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Gateway local network.

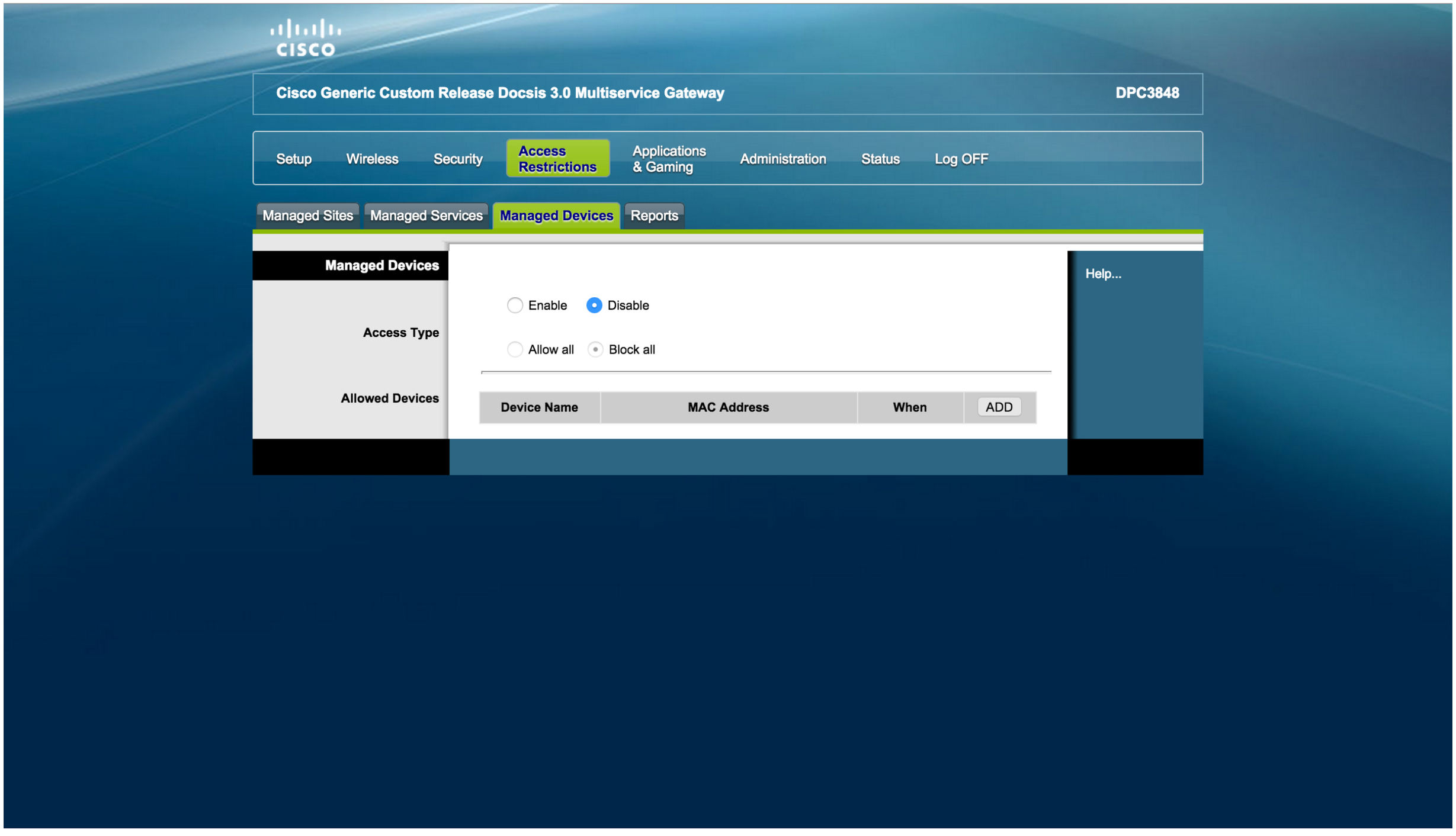
Access Restrictions Tab / Managed Sites



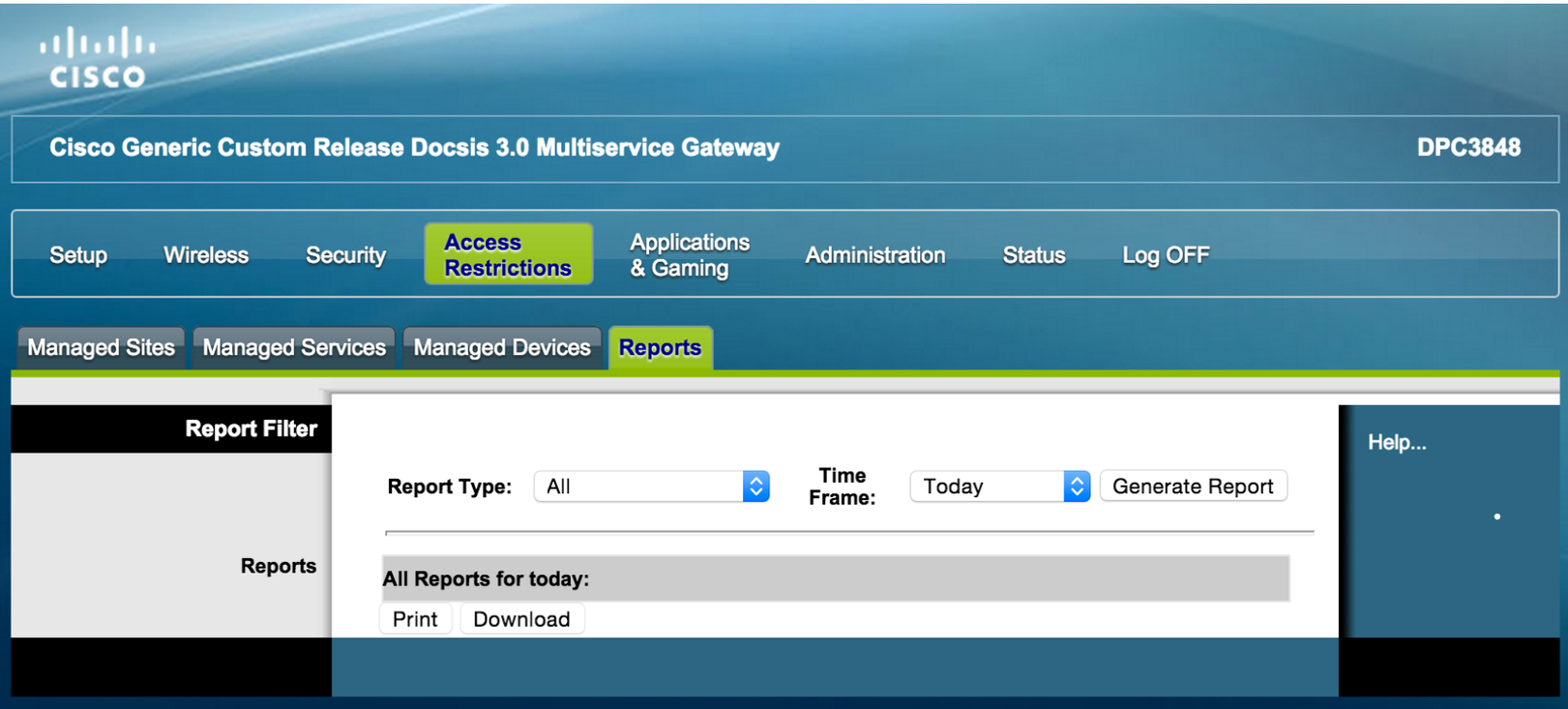
Access Restrictions Tab / Managed Services



Access Restrictions Tab / Managed Devices

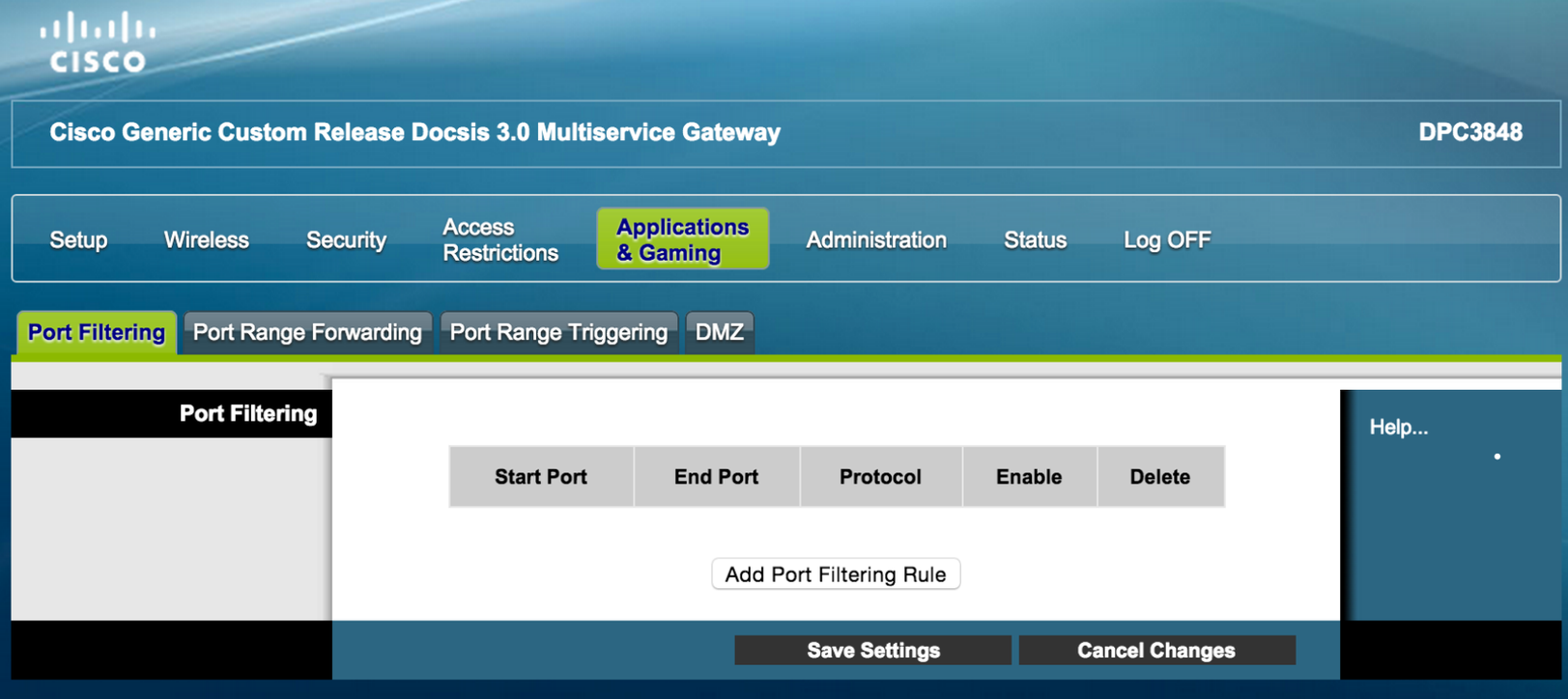


Access Restrictions Tab / Reports



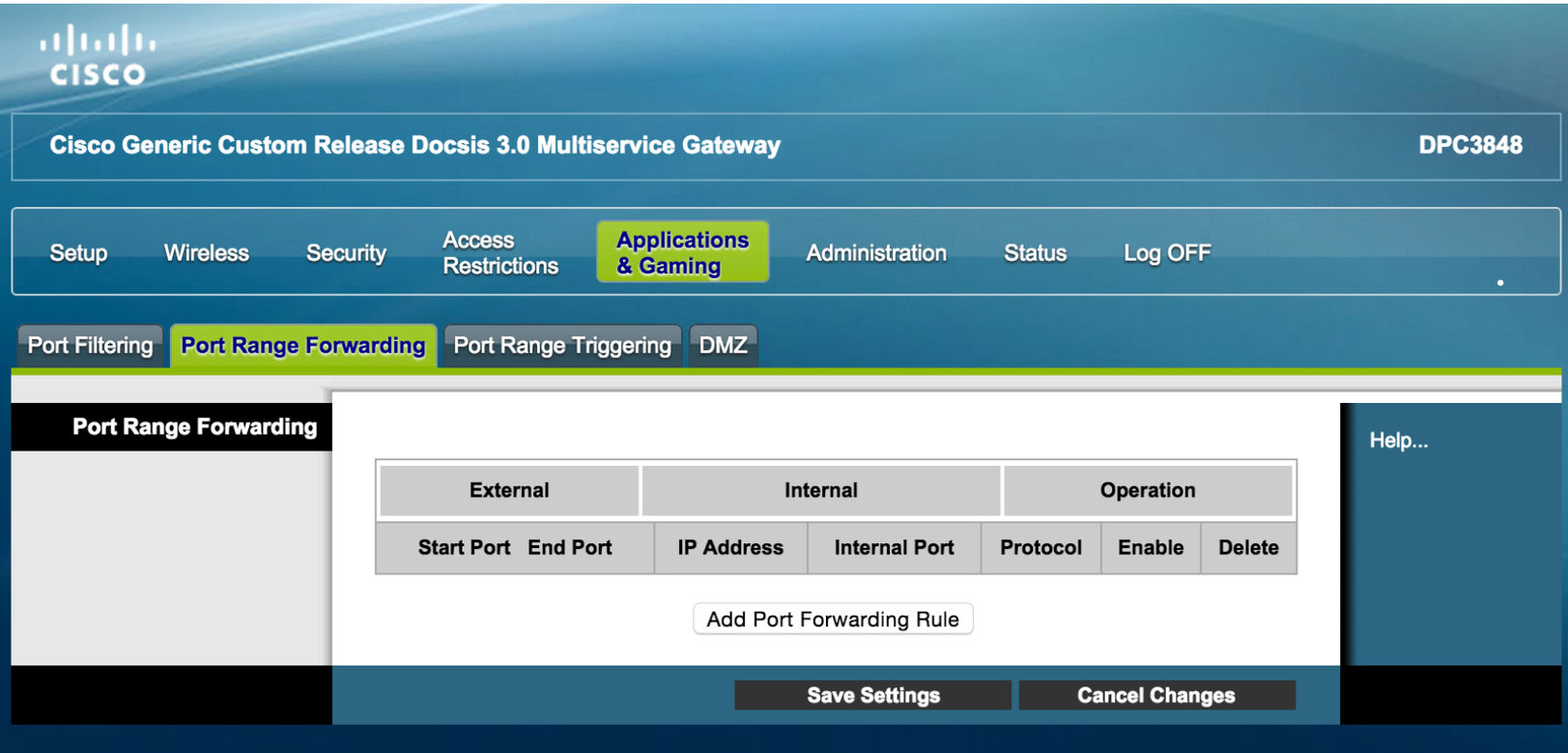
The log displayed on this page provides detailed information for all user restriction events.

Applications & Gaming Tab / Port Filtering



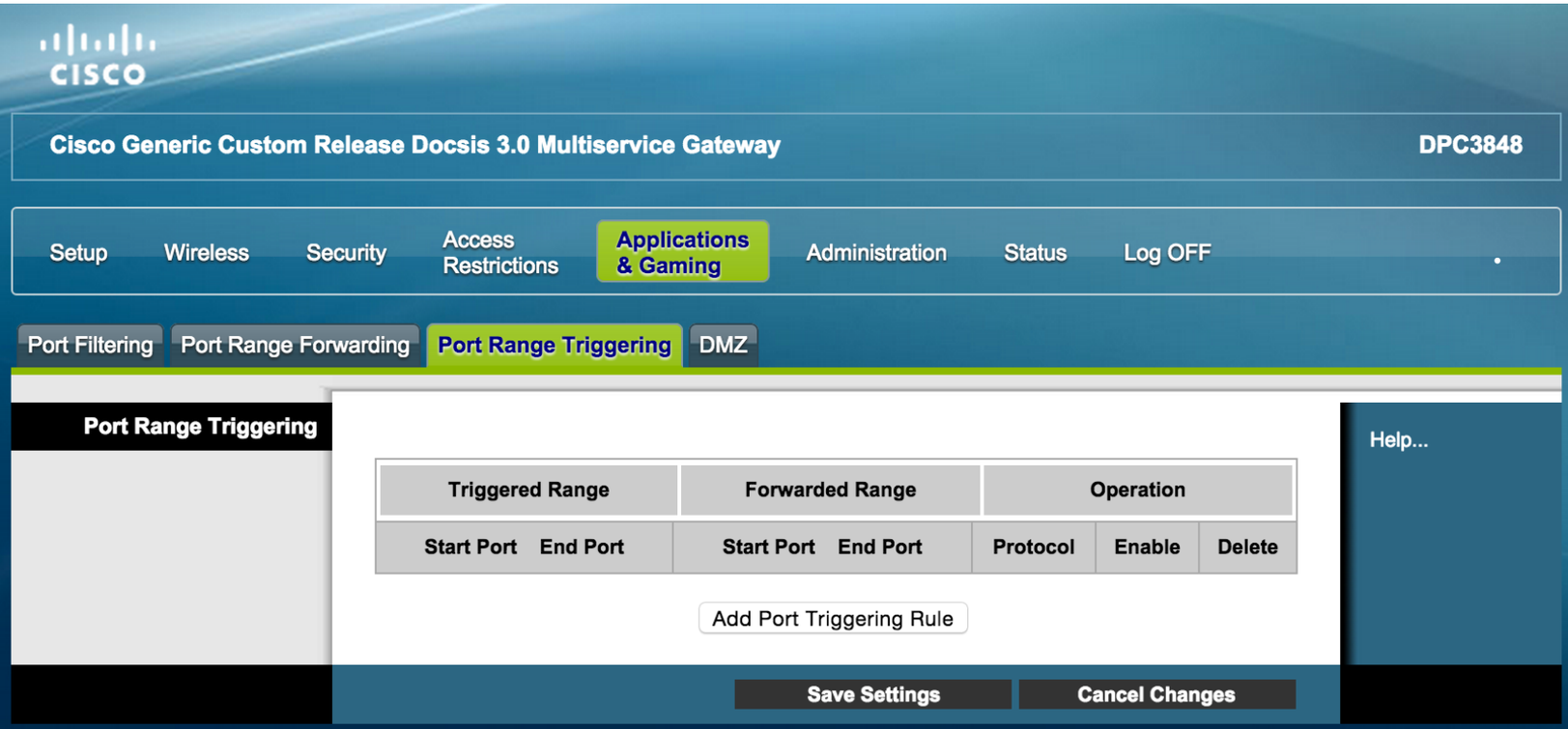
Use the Port Filtering page to configure and enable TCP and UDP port filters. These filters prevent a range of TCP/UDP ports from accessing the Internet.

Applications & Gaming Tab / Port Range Forwarding



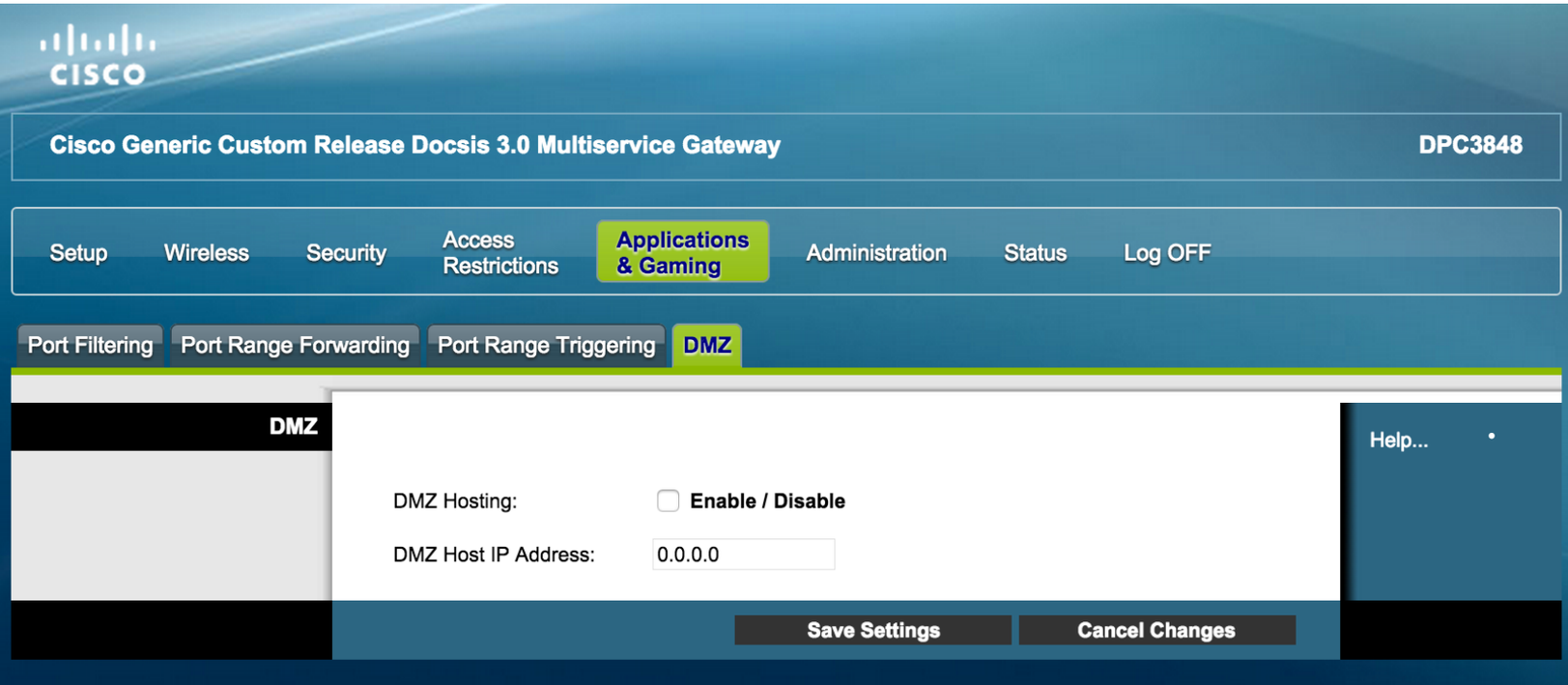
This screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as video conferencing or online gaming. Some Internet applications may not require any forwarding.)

Applications & Gaming Tab / Port Range Triggering



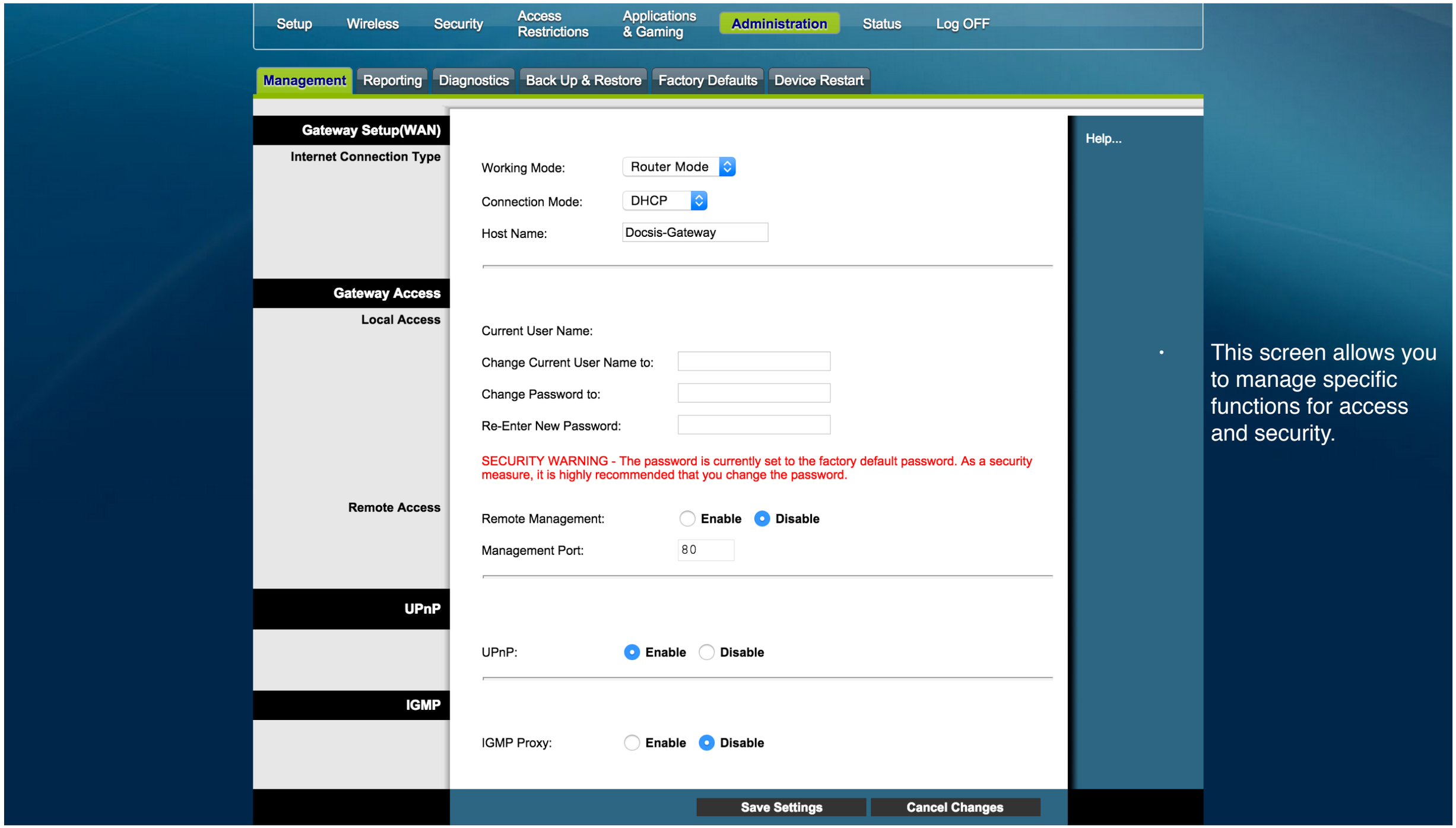
This screen allows the device to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the device, so that when the requested data returns through the device, the data is sent back to the proper computer by way of IP address and port mapping rules. To trigger a port range, enter the information on each line for the criteria required.

Applications & Gaming Tab / DMZ



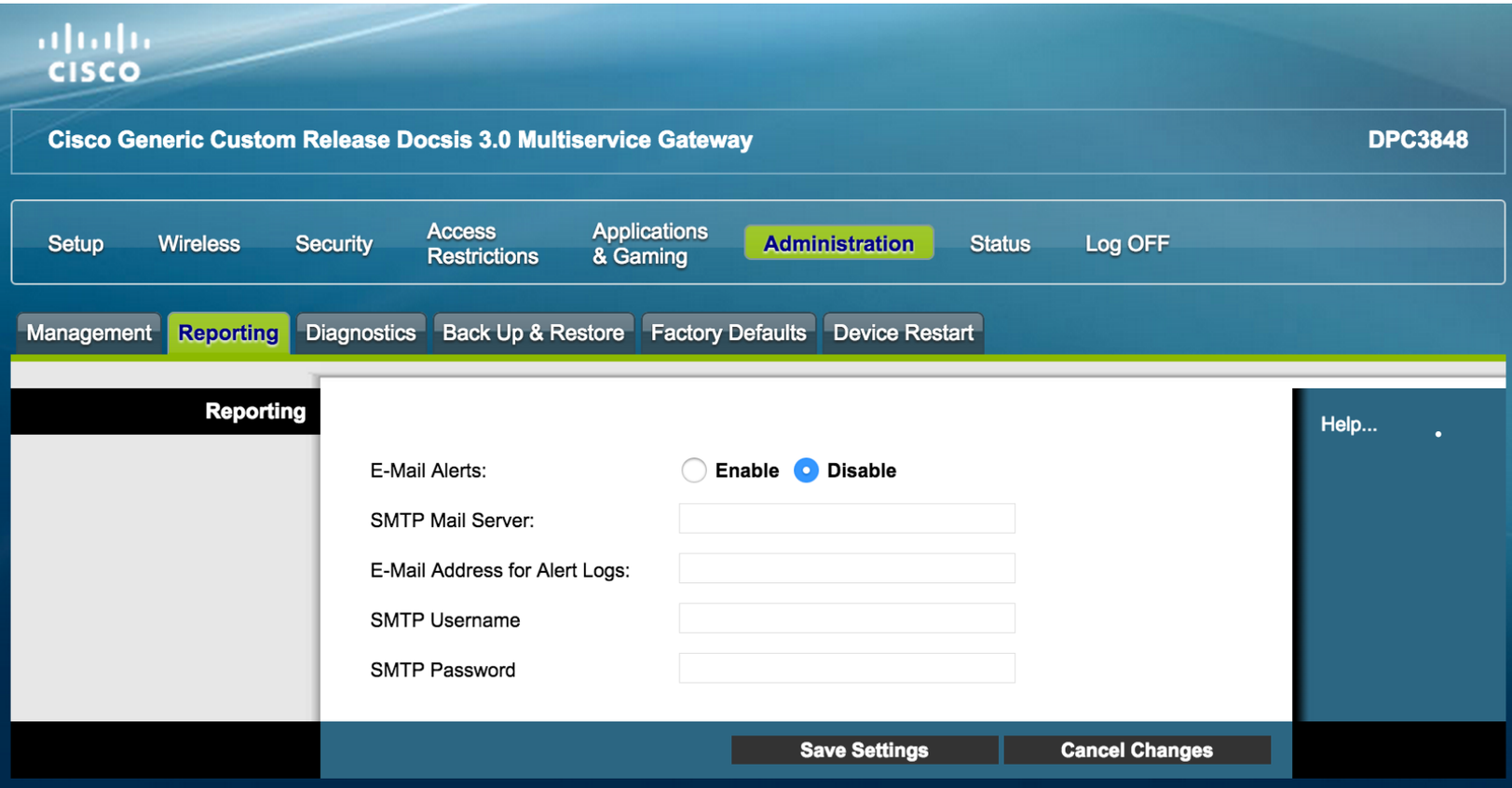
The DMZ feature allows one network user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or video conferencing. DMZ hosting forwards all the ports at the same time to one computer.

Administration Tab / Management



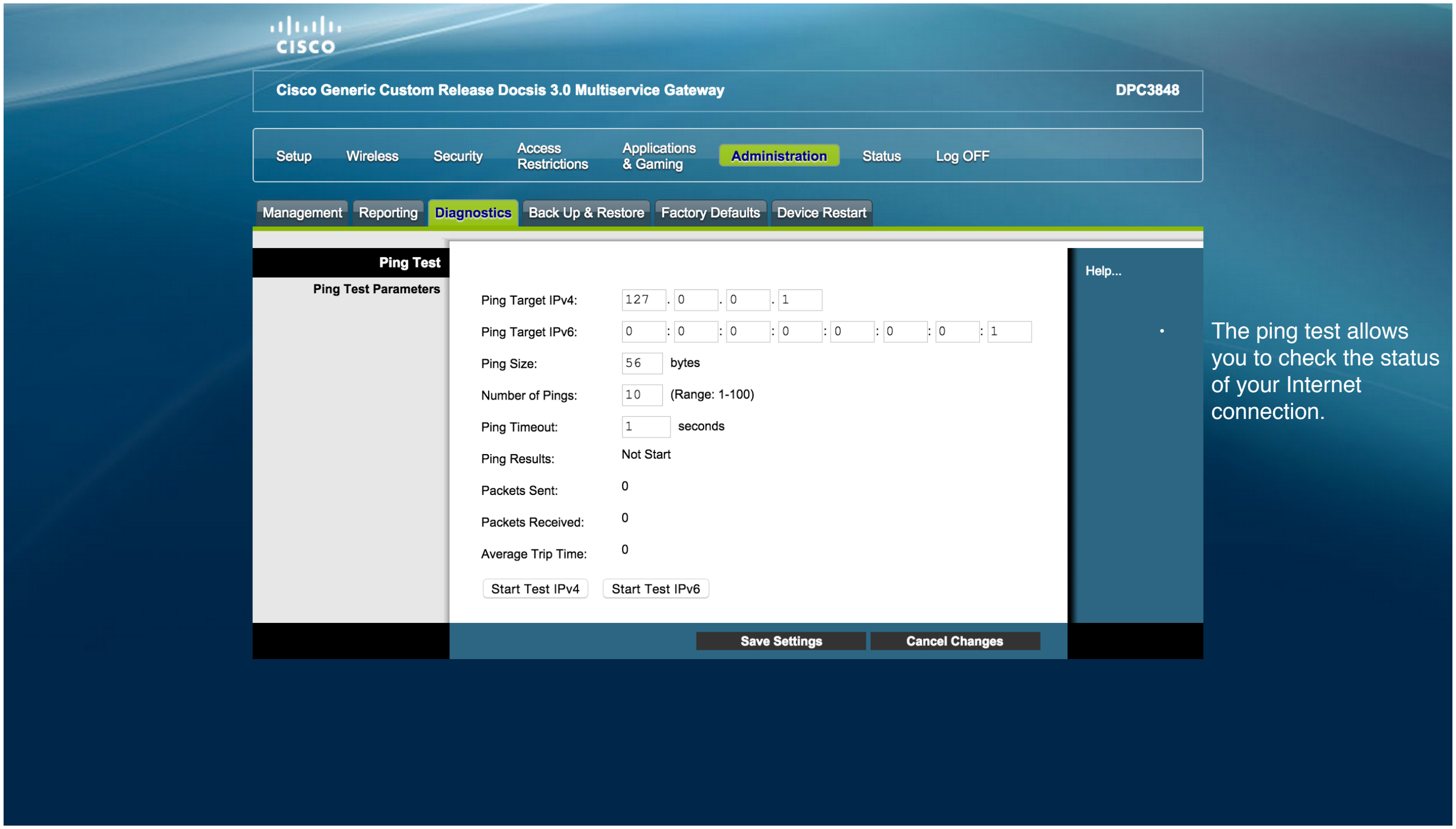
This screen allows you to manage specific functions for access and security.

Administration Tab / Reporting



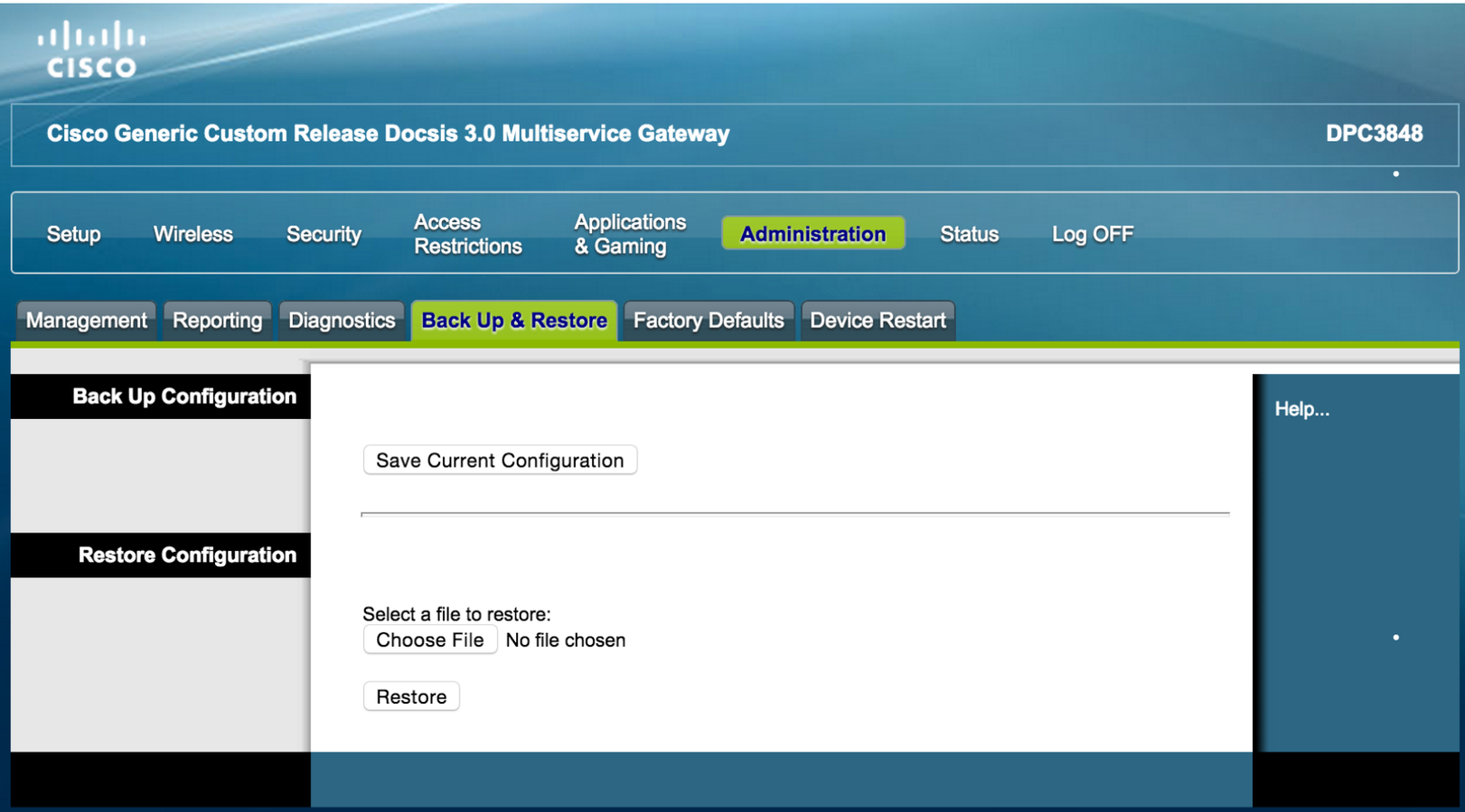
If enabled, an e-mail will be sent immediately if a Denial of Service (DoS) attack is detected. To use this feature, provide the necessary e-mail address information.

Administration Tab / Diagnostics



The ping test allows you to check the status of your Internet connection.

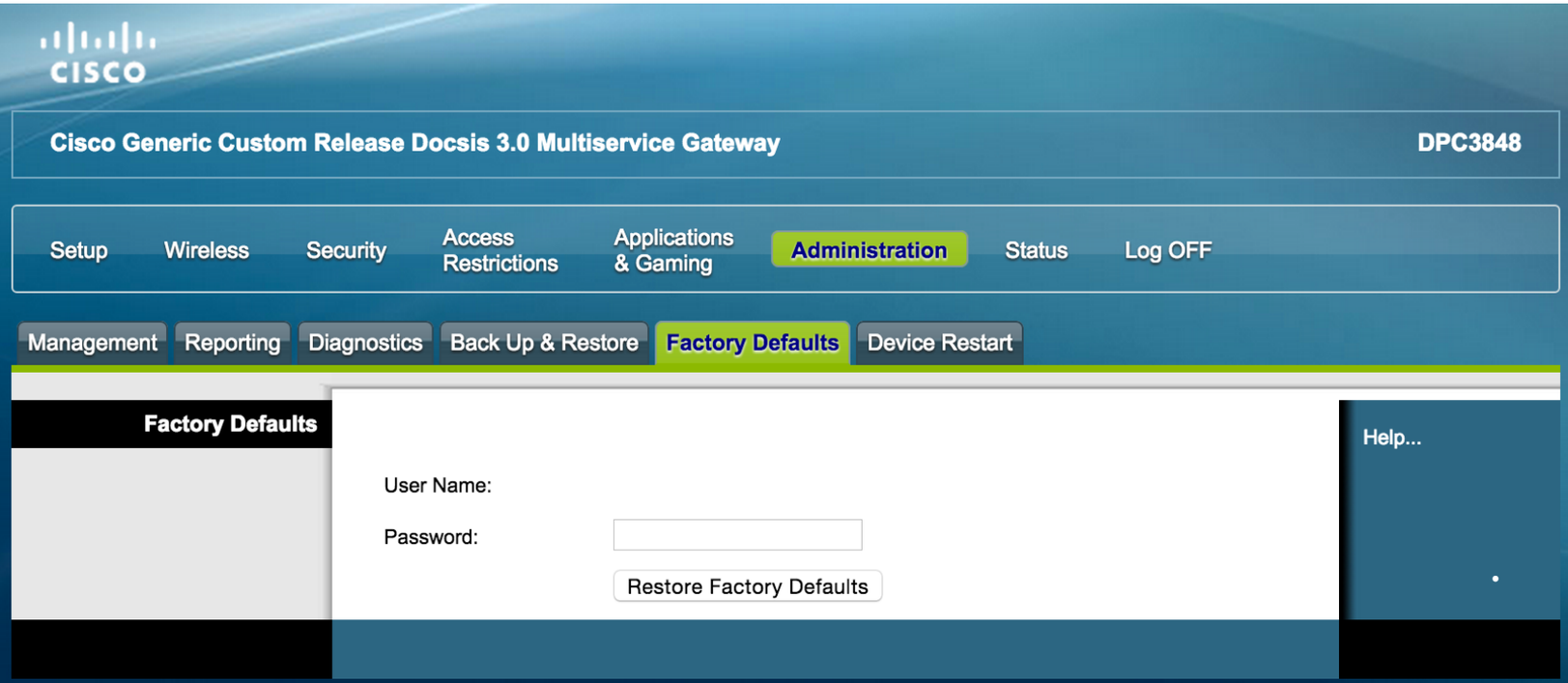
Administration Tab / Back Up & Restore



Back Up Configuration: Use this feature to download a copy of the current configuration, and store the file on your computer. Click the Backup button to start the download.

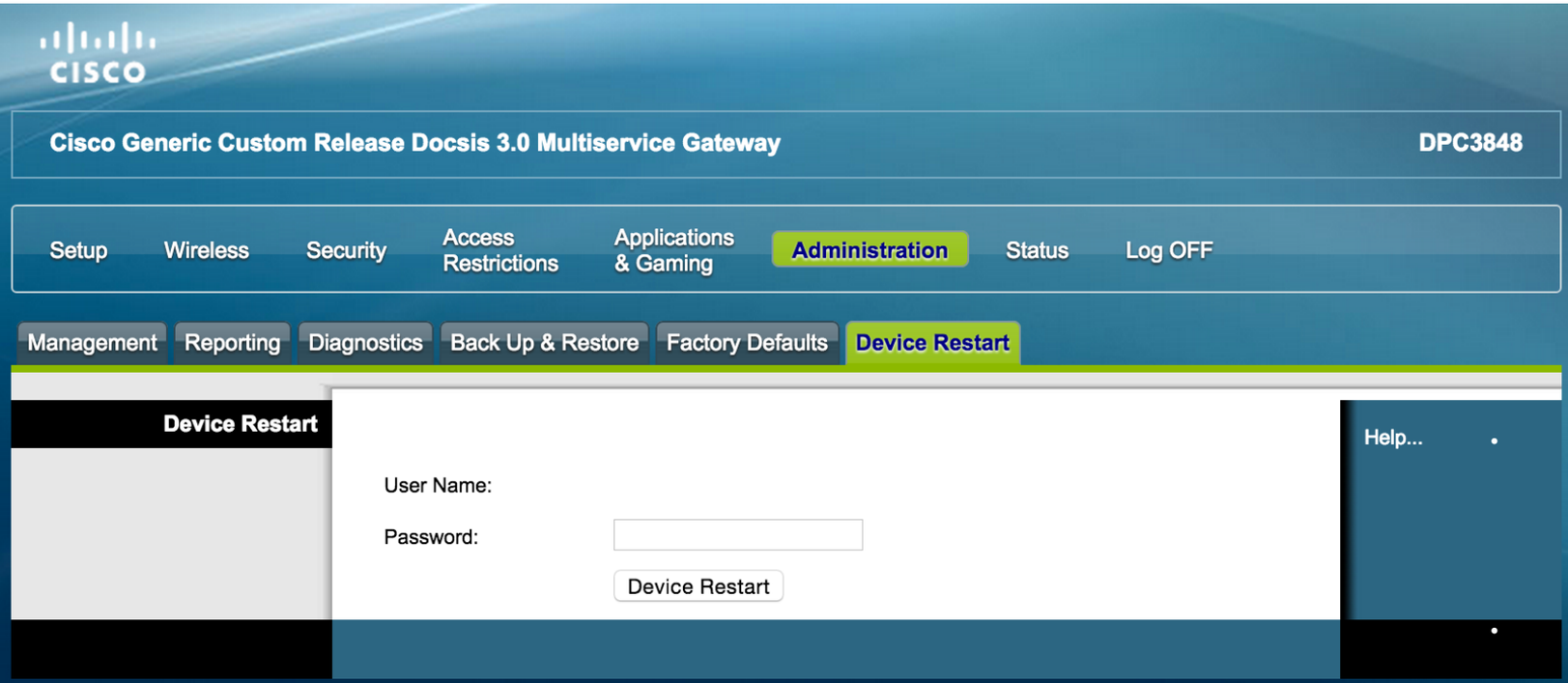
Restore Configuration: Use this feature to restore a previously saved configuration file. Click the Browse button to select the configuration file, and then click the Restore button to upload the configuration file to the device.

Administration Tab / Factory Defaults



- Use this feature to restore all modem into its factory defaults

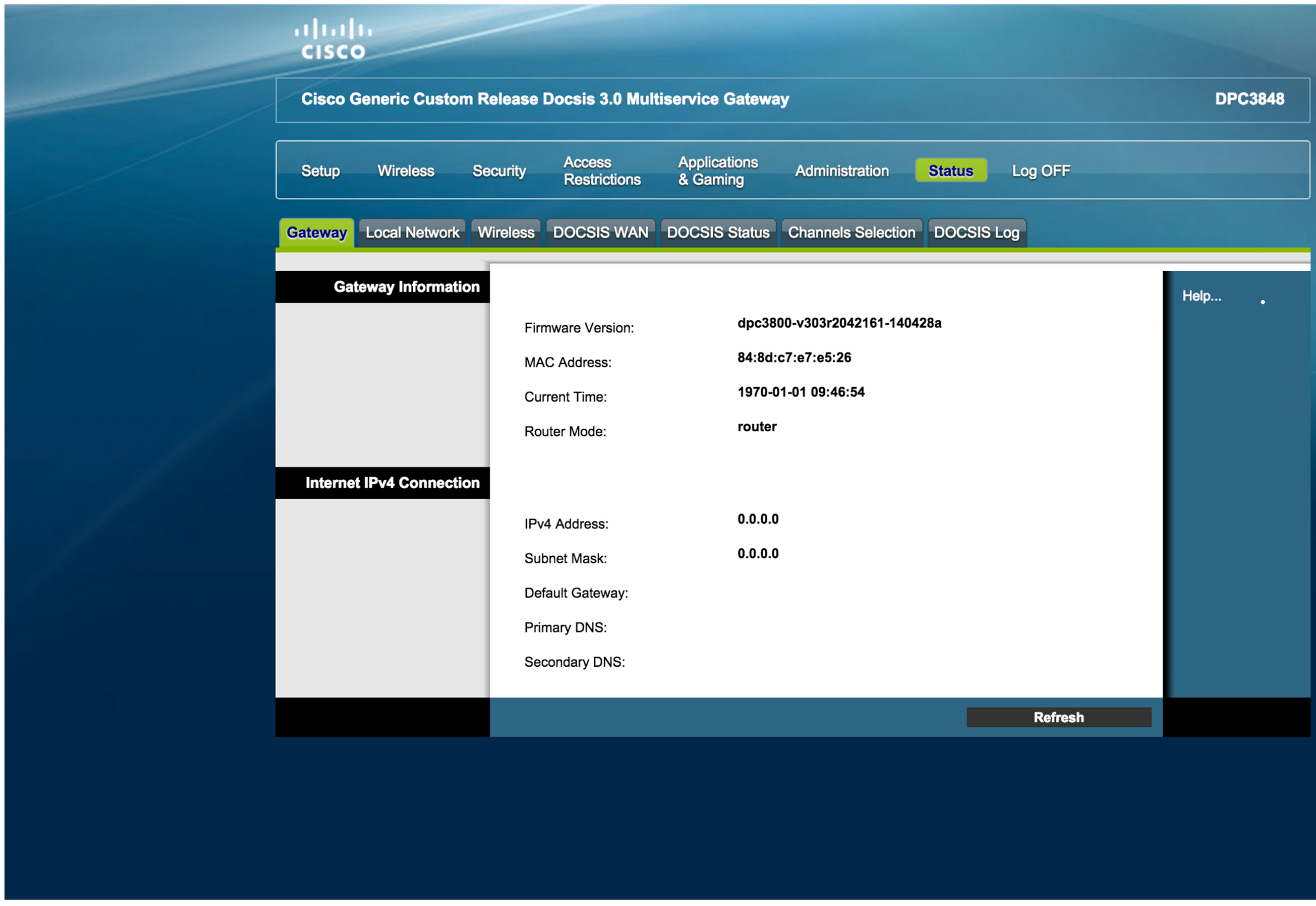
Administration Tab / Device Restart



This screen allows you to reboot the DUT.

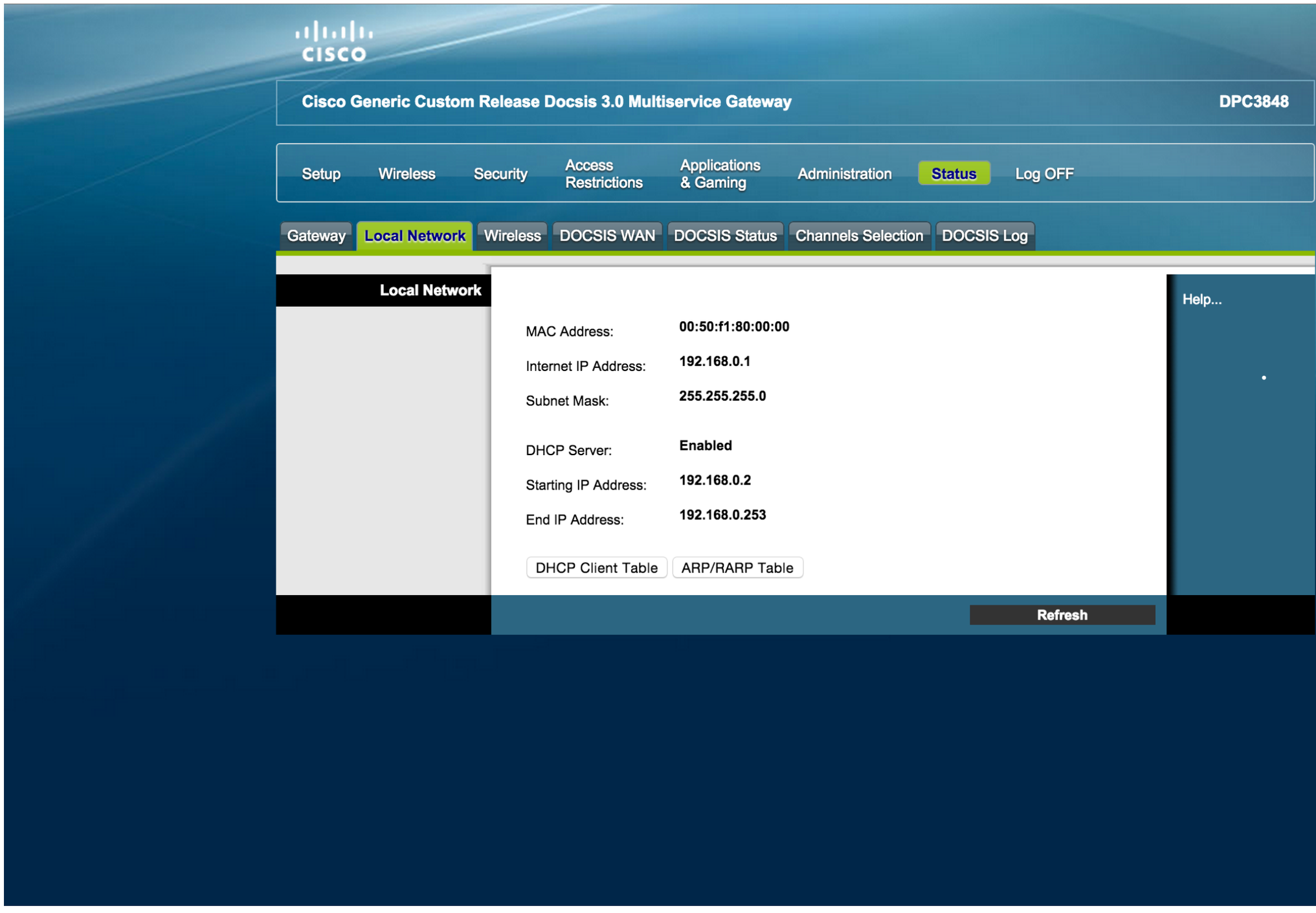
Note: This is just reboot , all configuration settings will not lost.

Status Tab / Gateway



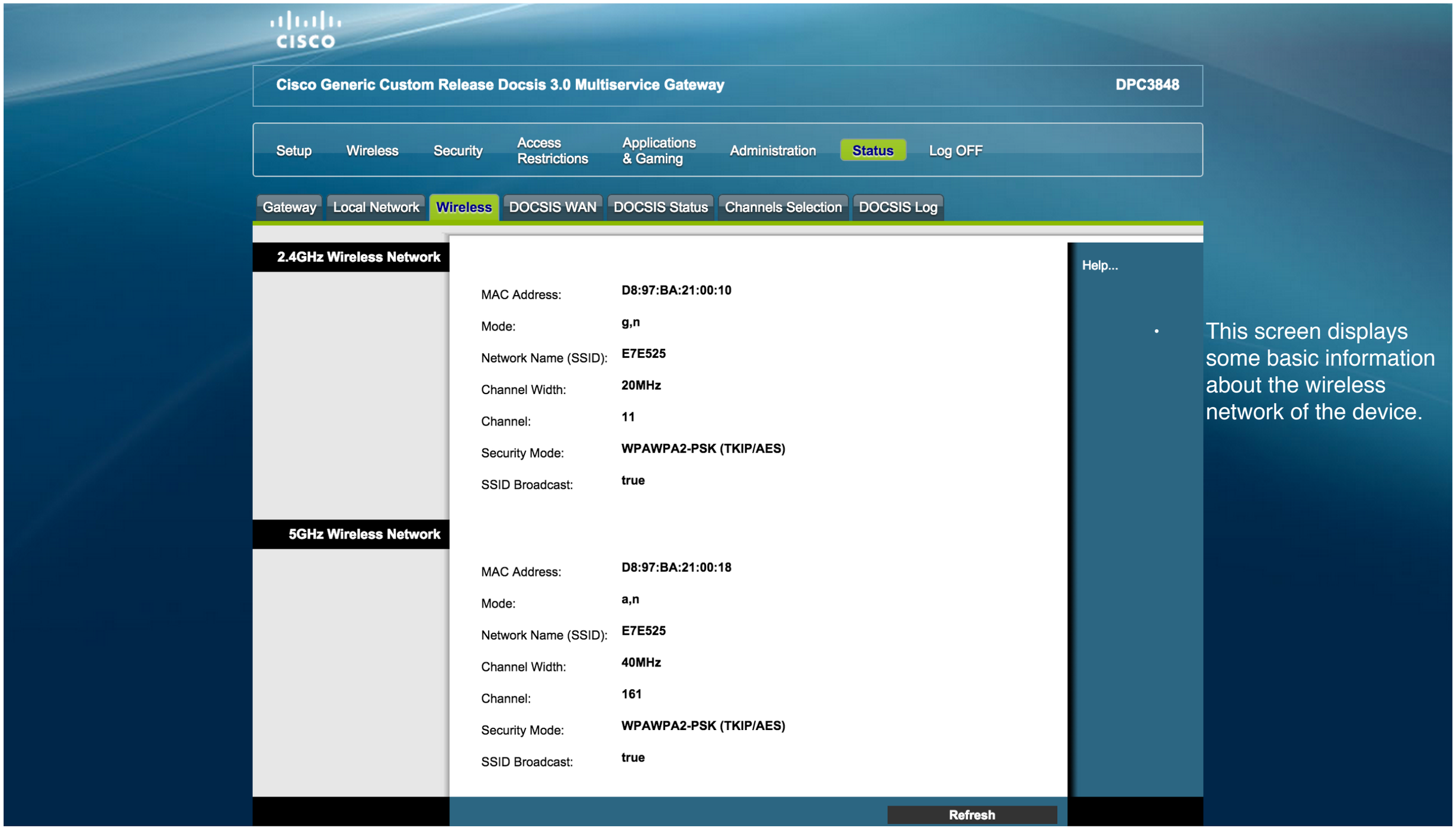
This screen displays information about the Gateway and its current settings. The on-screen information will vary depending on the Internet Connection Type you use.

Status Tab / Local Network



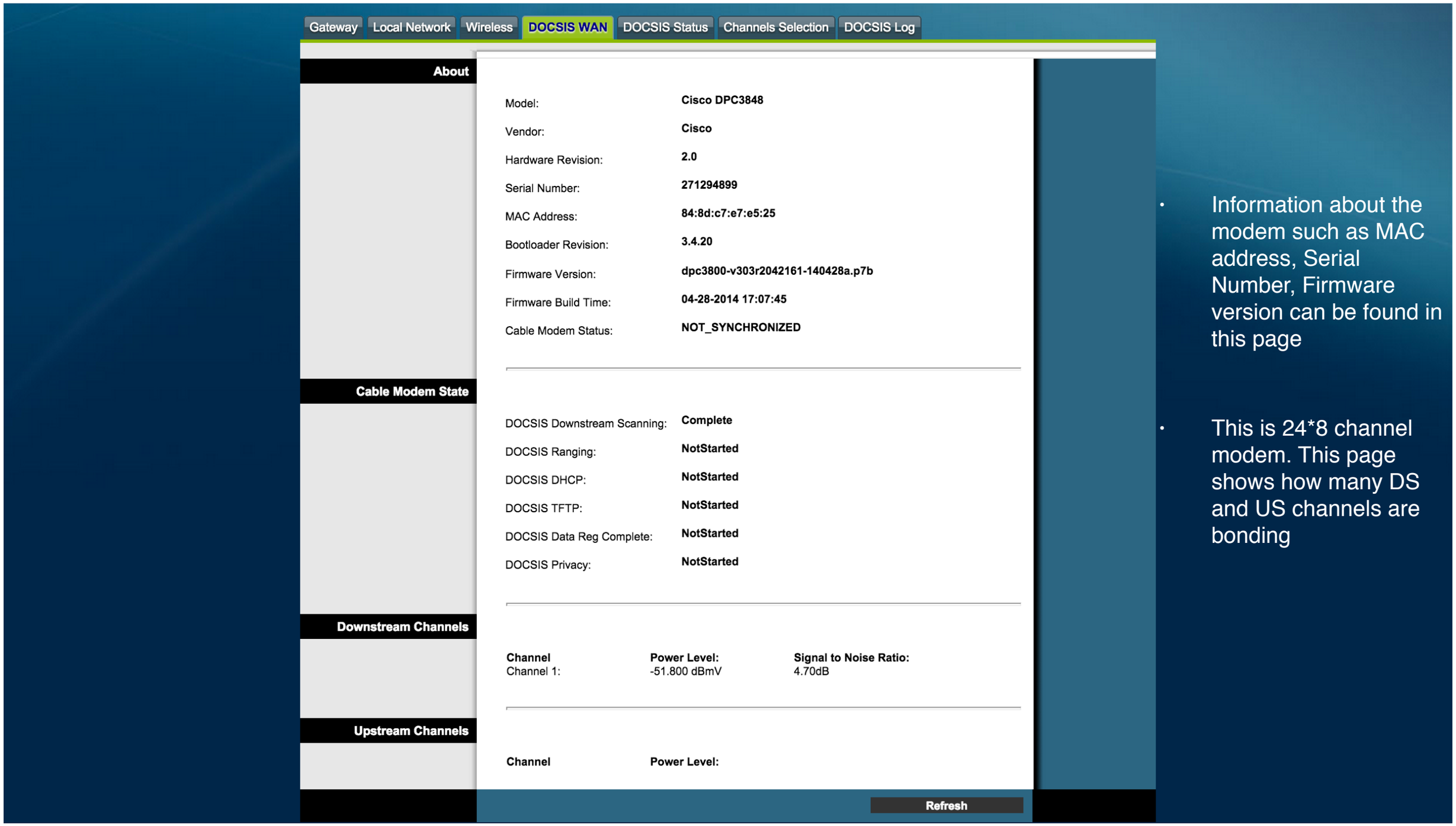
- This screen displays the status of your Local Area Network.

Status Tab / Wireless



This screen displays some basic information about the wireless network of the device.

Status Tab / DOCSIS Status



- Information about the modem such as MAC address, Serial Number, Firmware version can be found in this page
- This is 24*8 channel modem. This page shows how many DS and US channels are bonding

Status Tab / DOCSIS Status

Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway DPC3848

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status | Log OFF

Gateway | Local Network | Wireless | DOCSIS WAN | DOCSIS Status | Channels Selection | DOCSIS Log

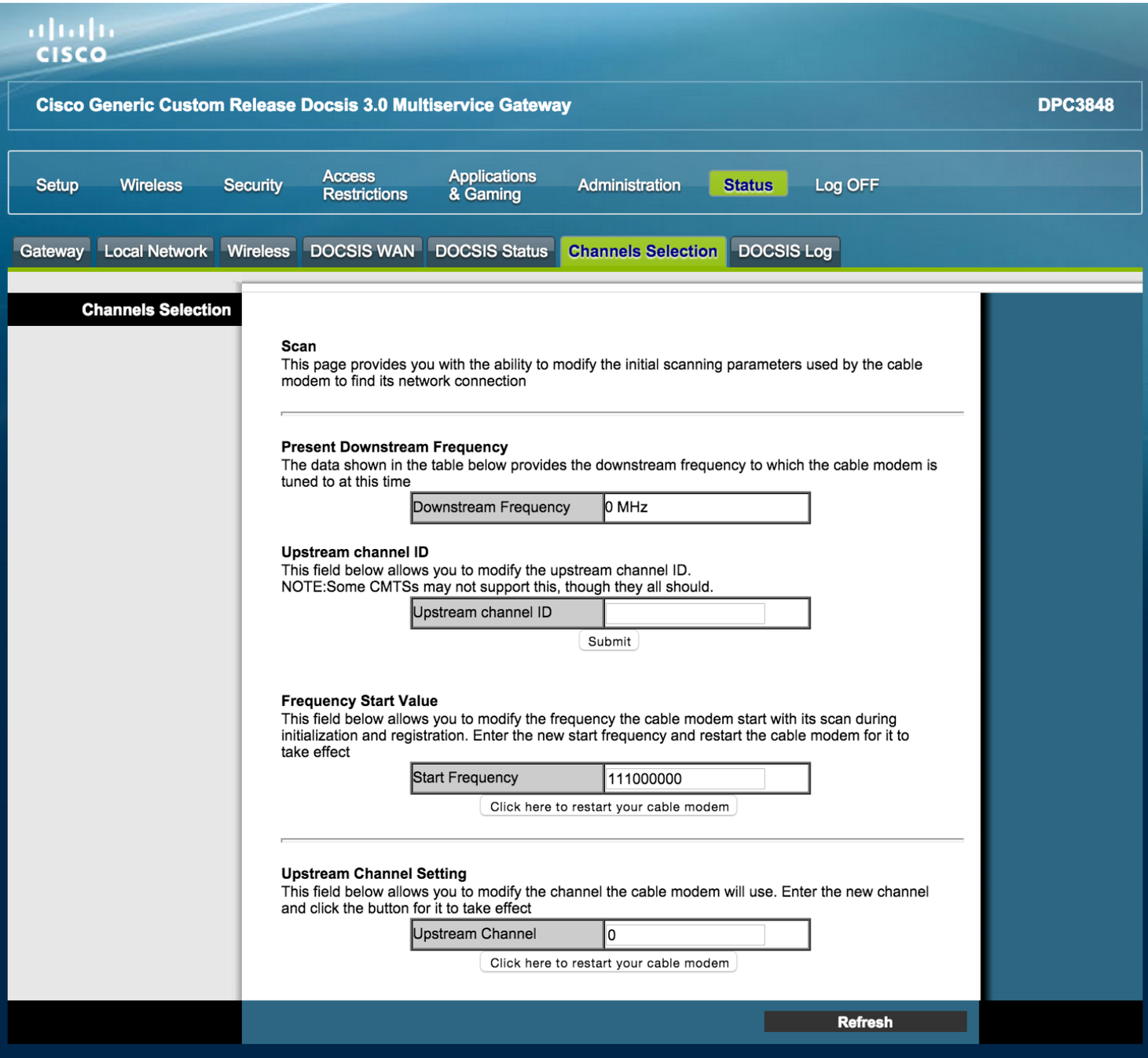
DOCSIS Status

Cable Modem Status:	**Scanning**
Cable Modem IPv4 Address:	**0.0.0.0**
Cable Modem IPv6 Address:	**::**
Cable Modem Mask:	**0.0.0.0**
Cable Modem Gateway:	**0.0.0.0**
Cable Modem TFTP Server:	**0.0.0.0**
Current Time:	**1970-01-01 09:49:30**
Time Server:	**0.0.0.0**
Time Offset:	**0**
Time Since Last Reset:	**35371**
Configuration File:	
Cable Modem Certificate:	**Not Installed**
IP Time Lease:	**0**
IP Time Rebind:	**D: 91 H: 4 M: 22 S: 4**
IP Time Renew:	**D: 91 H: 4 M: 37 S: 24**

Ethernet

Interface Name	LINK Status	LINK Speed	LINK Duplex
Interface1	Up	100 MBits	Full
Interface2	Down	0 MBits	Auto
Interface3	Down	0 MBits	Auto
Interface4	Down	0 MBits	Auto
Interface5	Down	1000 MBits	Auto

Status Tab / Channel Selection



- This page provides you with the ability to modify the initial scanning parameters used by the cable modem to find its network connection

Status Tab / DOCSIS Log

Cisco Generic Custom Release Docsis 3.0 Multiservice Gateway DPC3848

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status | Log OFF

Gateway | Local Network | Wireless | DOCSIS WAN | DOCSIS Status | Channels Selection | DOCSIS Log

DOCSIS Log

Time	ID	Level	Description
Wed May 13 08:25:48 2015	90000000	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.0;CM-VER=3.0;
Thu Jan 1 00:02:22 1970	82000800	Critical (3)	16 consecutive T3 timeouts while trying to range on upstream channel 4;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:02:22 1970	82000300	Critical (3)	Ranging Request Retries exhausted;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:40 1970	82000200	Critical (3)	No Ranging Response received - T3 time-out;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:26 1970	84020200	Warning (5)	Lost MDD Timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:26 1970	84020300	Warning (5)	MDD message timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Wed May 13 08:19:34 2015	90000000	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.0;CM-VER=3.0;
Thu Jan 1 00:01:20 1970	84020200	Warning (5)	Lost MDD Timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:19 1970	84020300	Warning (5)	MDD message timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Wed May 13 08:16:19 2015	69011200	Notice (6)	SW download Successful - Via Config file
Wed May 13 08:12:53 2015	69010200	Notice (6)	SW Download INIT - Via Config file main.cfg
Wed May 13 08:11:19 2015	90000000	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.0;CM-VER=3.0;
Thu Jan 1 00:02:11 1970	82000800	Critical (3)	16 consecutive T3 timeouts while trying to range on upstream channel 4;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:02:11 1970	82000300	Critical (3)	Ranging Request Retries exhausted;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:41 1970	82000200	Critical (3)	No Ranging Response received - T3 time-out;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;
Thu Jan 1 00:01:27 1970	84020200	Warning (5)	Lost MDD Timeout;CM-MAC=84:8d:c7:e7:e5:25;CMTS-MAC=00:0c:31:f4:c8:01;CM-QOS=1.1;CM-VER=3.0;

- This page provides Logs