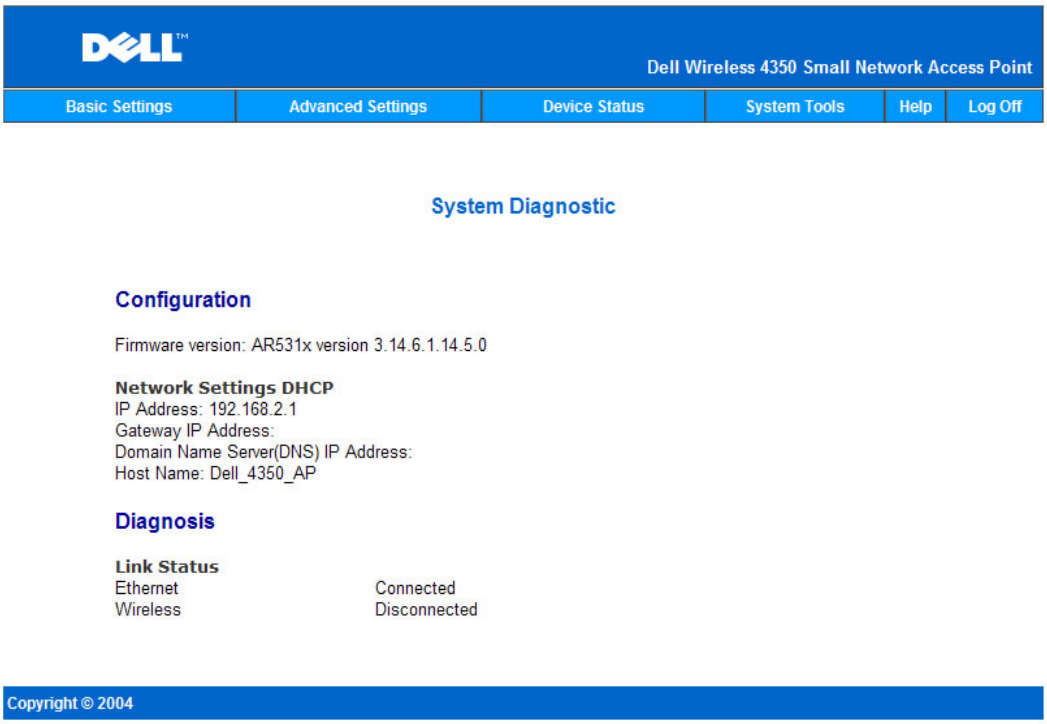
System Diagnostic

The Systems Diagnostic page is for your information only. This page displays both the configuration settings and diagnostic information for the Dell Wireless 4350 Small Network Access Point. The configuration settings include firmware version and device settings that have been configured for your network.

The Diagnostic section shows the status of the wireless and Ethernet connections for your Dell Wireless 4350 Small Network Access Point.

System Diagnostic

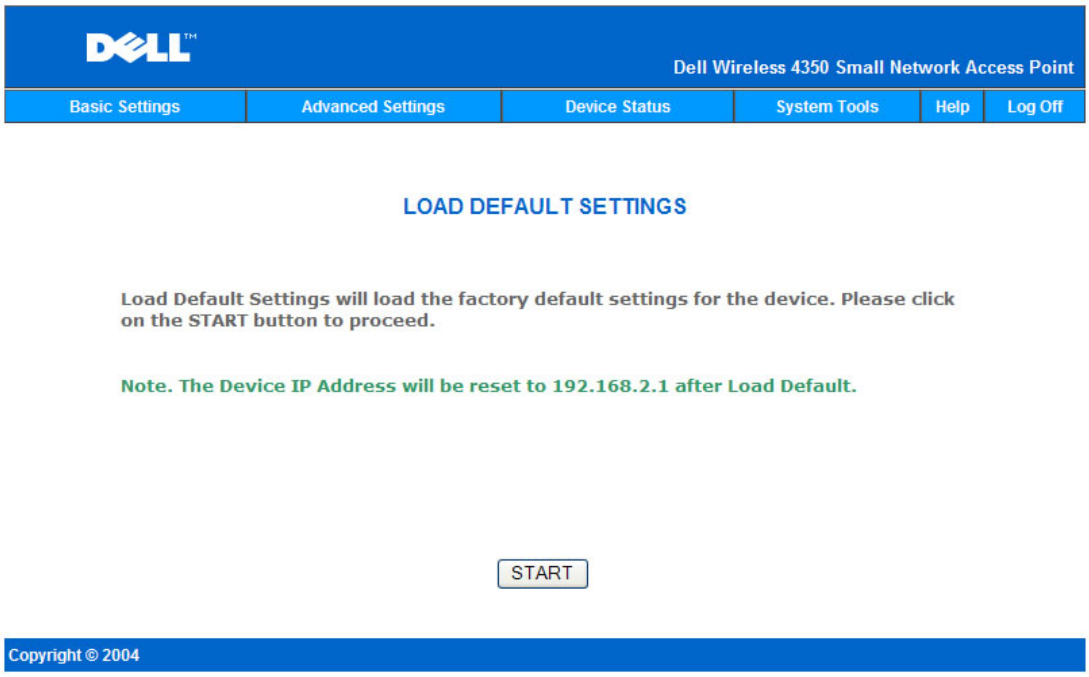


Load Default Settings

The Load Default Settings page allows you to reload the factory default configurations that came with the device. When this option is used, all settings are reset to the factory default value. This is equivalent to pressing and holding the **Reset** button on the back panel of the device for more than 5 seconds (for more details, refer to A Look at the Hardware).

NOTICE: Loading the default settings option will cause the current settings for your Dell Wireless 4350 Small Network Access Point to be lost.

Load Default Settings



Click the **Start** button to reload the default settings.

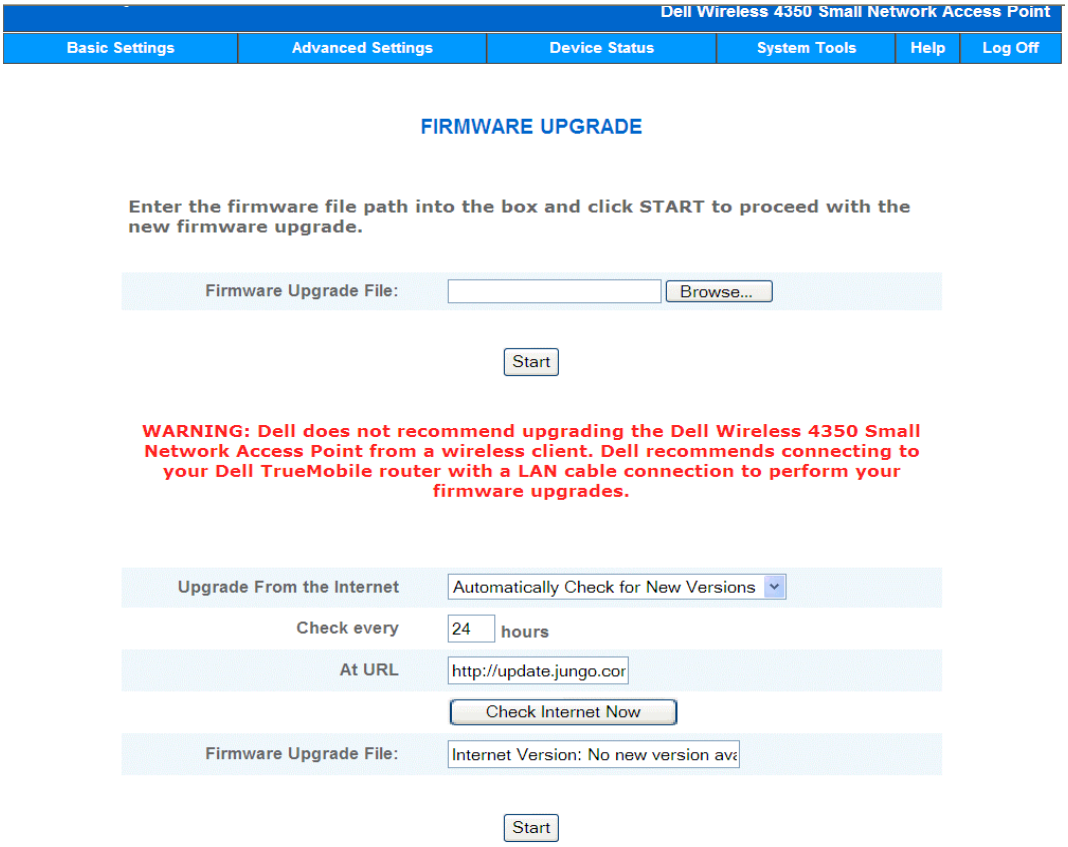
Upgrade Firmware

Dell periodically releases firmware updates to provide improved performance or capabilities. Use the firmware upgrade feature to easily upgrade the firmware on your Dell Wireless 4350 Small Network Access Point.

The Upgrade firmware page supports two methods for upgrading the firmware onto the access point (a) local file upgrade (b) Internet file upgrade.

NOTE: Make sure the file you choose is an actual Dell Wireless 4350 Small Network Access Point firmware file.

Upgrade the Firmware



Upgrade Firmware – Local File

You can check the Dell support website, support.dell.com, to see if there are any new upgrades. Download the new firmware first before upgrading and save it to one of the clients in your network. To upgrade the firmware:

1. Type the firmware file path into the **Firmware Upgrade File:** box, or click the **Browse** button to choose a firmware file to upgrade to.
2. Click the **Start** button when you have chosen a file. After the firmware is written to the Dell Wireless 4350 Small Network Access Point, the home page will be loaded automatically. While the access point is resetting, the **Power** light on the front panel of the device blinks.

Upgrade Firmware – Internet File

The other option to upgrade firmware is through the Internet.

The Dell Wireless 4350 Small Network Access Point can be configured to automatically check the internet for upgrades by entering the URL ftp.us.dell.com/network in the URL field and the number of hours to automatically check for upgrades into the hours field. The user can also click **Check Internet Now** to see if there is new firmware available for upgrading.

The drop-down menu gives the user the option to enable automatic checking of the Internet. These options are:

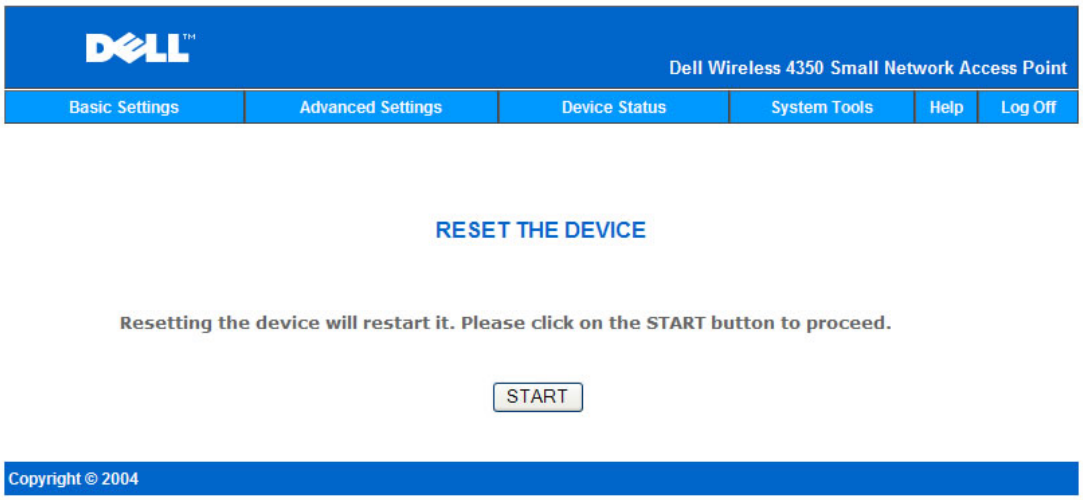
1. **Automatic Check for New Versions**: The access point automatically checks the Internet to determine if a new a firmware file is available.
2. **Automatic Check Disabled**: The Internet firmware checking function is disabled.

Click the **Start** button when a new firmware file is available for upgrading the access point. After the firmware is written to the Dell Wireless 4350 Small Network Access Point, the home page will be loaded automatically. While the access point is resetting, the **Power** light on the front panel of the device blinks

NOTE:	Make sure the file you choose is an actual Dell Wireless 4350 Small Network Access Point firmware file.
NOTE:	Dell does not recommend upgrading the Dell Wireless 4350 Small Network Access Point from a wireless client. Dell recommends connecting to your Dell Wireless access point with a wired network connection to perform firmware upgrades.

Reset Device

Use the Reset Device function if a system failure occurs. This feature does **not** reload the factory default settings. It simply resets the device to the network settings that existed on the device before the system failure occurred. This is equivalent to unplugging the device and plugging it back in or pressing the reset button for less than 3 seconds until the **Power** light starts to blink. No configuration settings are lost.



NOTICE: If you were in the process of updating the network settings, those changes are lost when the device is reset.

Click the **Start** button to reset the Dell Wireless 4350 Small Network Access Point to its **current firmware settings**. While the access point is resetting, the **Power** light on the front of the device blinks.

Advanced Settings:

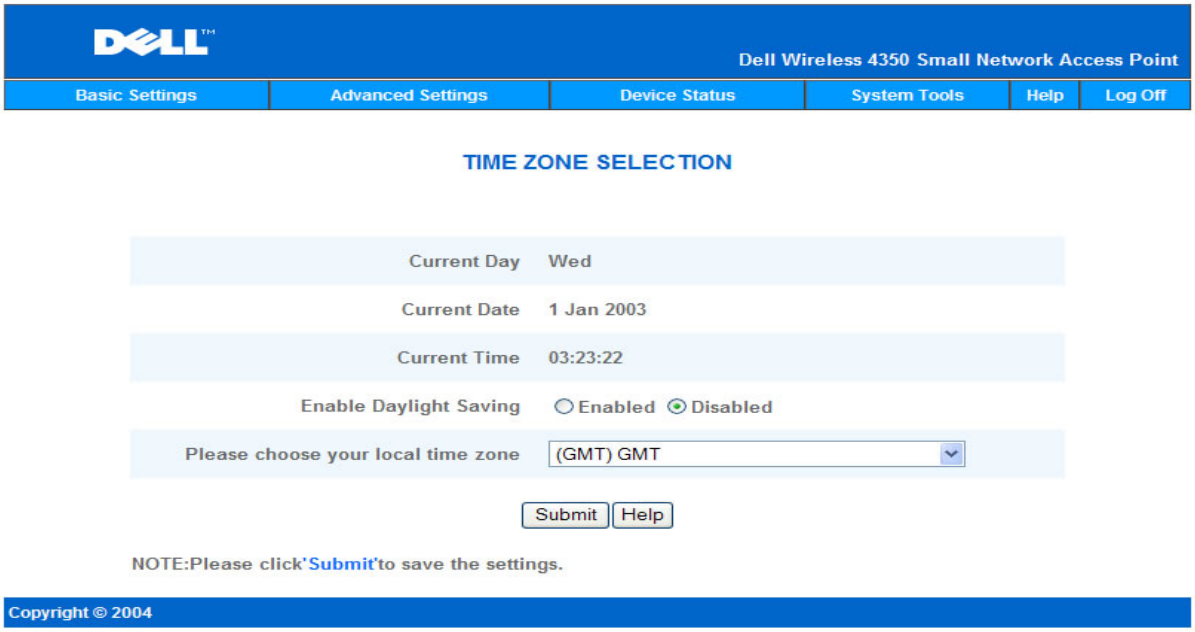
- Time Zone
- Advanced Wireless
- Access Control Settings
- Administration Settings
- Wired Settings
- SSID Manager
- SNMP
- Rogue AP Detection

NOTE: Dell technical support representatives do not support the configuration options in the Advanced Settings portion of the configuration program. These options are provided for your convenience only. However, the advanced settings are fully

	documented and explained in this guide.

Time Zone

Time Zone



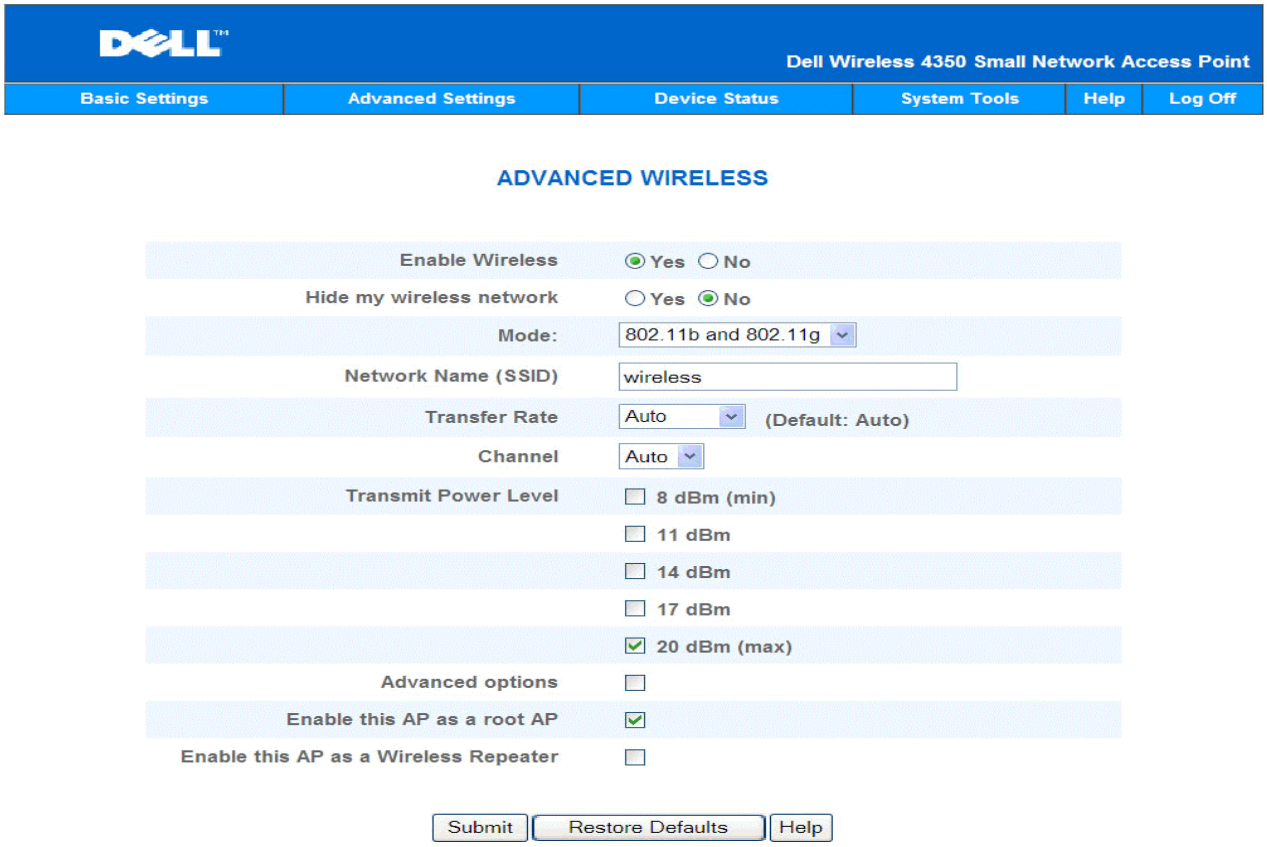
The **Time Zone** page is used to set the time on the Dell Wireless 4350 Small Business Access Point.

Select your local time zone from the pull-down list, **Please choose your local time zone**. During the summer months, the clock will move one or several hours ahead (depending on geographical location). Different countries have different change dates, in most of the U.S and Canada, daylight saving time begins on the last Sunday of October and reverts back to standard time on the first Sunday of April. To enable daylight saving, click **Yes** for **Enable Daylight Saving**.

The Time Zone settings will affect the time stamp on IP packets in the Intruder Detection Log. The time setting overrides the time stamp on IP packets that are in Greenwich Mean Time (GMT).

Advanced Wireless

Advanced Wireless



The **Advanced Wireless** page is used to configure advanced wireless features in the Dell Wireless 4350 Small Network Access Point.

Enable Wireless

This setting enables radio transmission and reception on the Dell Wireless 4350 Small Network Access Point allowing wireless clients to connect to the access point.

Click **Yes** to allow wireless clients to connect to the access point (default setting).

Click **No** to prevent wireless clients connecting to the access point.

Hide my wireless network

This setting enables the transmission of beacon packets from the Dell Wireless 4350 Small Network Access Point to the wireless network. The beacon packets are transmitted by default allowing other wireless clients to easily find and connect to the access point with the use of a site survey tool. If you want to increase wireless network security, you can disable the transmission of the beacon packets.

Click **No** to allow transmission of beacon packets from the access point.

Click **Yes** to disable the transmission of beacon packets from the access point.

Mode

The setting allows the user to select the 802.11 mode that the Dell Wireless 4350 Small Network Access Point will use when communicating with wireless clients.

Select **802.11b and 802.11g** if the access point is to support both 802.11g and 802.11b compatible wireless clients (default setting).

Select **802.11b** if the access point is to support only 802.11b compatible wireless clients.

Select **802.11g** if the access point is to support only 802.11g compatible wireless clients.

Network Name(SSID)

This setting allows the user to change the Network Name (SSID) of the Dell Wireless 4350 Small Network Access Point. The Service Set Identifier (SSID) is a 32-character name that uniquely identifies all the computers and equipment that make up the wireless network. The default value is “wireless”.

Transfer Rate

This setting allows the user to set the wireless throughput rate from the Dell Wireless 4350 Small Network Access Point to the wireless clients. The transfer rate can be set to automatic or some other fixed value. It is recommended that you set the transfer rate to automatic (Auto) to allow the wireless network devices to transmit at a rate they deem optimum.

Channel

This setting allows the user to set the radio channel that the Dell Wireless 4350 Small Network Access Point will operate on. The range of available radio channels depends on the regulatory domain (e.g. 11 channels for U.S. and Canada & 13 channels for Europe). It is recommended that you set the channel setting to Auto to allow the access point to locate the most suitable radio channel for operation.

Transmit Power Level

This setting allows the user to select the transmit radio power level of the Dell Wireless 4350 Small Network Access Point. The access point supports five different transmit power levels and these are 8 dBm, 11 dBm, 14 dBm, 17 dBm and 20 dBm.

Advanced Options

This setting allows the user to configure specific radio transmission parameters for the Dell Wireless 4350 Small Network Access Point.

NOTE: If you want to configure the settings of Beacon Interval, RTS Threshold, Fragmentation Threshold, DTIM Interval and CTS Protection, ensure that **Advanced Options** is selected first.

Beacon Interval

The Beacon Interval is the amount of time in Kusecs (one Kusec equals 1,024 microseconds) between radio beacons from the Dell Wireless 4350 Small Network Access Point to its client stations. The available range is from 1 to 65535, with the default value being 100.

RTS Threshold

The RTS Threshold is the maximum packet size that the Dell Wireless 4350 Small Network Access Point will transmit without prior transmission of a RTS (Request To Send) signalling packet. The available range is from 1 to 2346, with the default value being 2346.

The RTS (Request to Send) mechanism prevents the **Hidden Node** problem. A hidden node occurs when two stations are within range of the same Access Point (AP) but are not within range of each other, they are “hidden” from each other. The packets from these two stations may collide if they arrive at the AP at the same time. To prevent data collision with the hidden node, you can activate the RTS mechanism. If the RTS mechanism is activated, the station will send a RTS first to inform the AP that it is going to transmit the data. Then, the AP will reply with a CTS (Clear to Send) to all stations within its range to notify all other stations and reserve the bandwidth for your data.

The RTS threshold controls what size data packet will cause an RTS to be transmitted. Only when the packet exceeds the RTS threshold will the device send a RTS before sending the packet. There is a trade-off to consider when choosing a value for the RTS threshold. Low values will cause the RTS to be sent more often which would waste the bandwidth. However, the more often RTS packets are sent, the quicker the system can recover from data collisions. It is recommended to use the default value or only minor reductions of this default value.

Fragmentation Threshold

The fragmentation threshold determines the size of data packets that will be fragmented before transmission. The available range is from 1 to 2346, with the default value being 2346 (Note: The fragmentation threshold is specified in bytes).

Data packets that are smaller than the specified fragmentation threshold value will not be fragmented. Data packets that are larger than the fragmentation threshold will be fragmented into smaller packets and transmitted one at a time instead of all at once. The purpose of fragmentation is to reduce the need for retransmission and improve overall network performance. Fragmentation is normally activated when there is heavy traffic on the wireless network or the network is operating in a high interference environment. It is recommended to use the default value or only minor reductions of this default value.

DTIM Interval

The DTIM (Delivery Traffic Indication Message) Interval setting determines how often a beacon contains a traffic indicator map (TIM). The TIM is used to alert stations in sleep mode that date is available for reception. The DTIM Interval is always a multiple of the beacon period and the available range is from 1 to 255, with the default value being 1.

CTS Protection mode

The CTS Protection mechanism allows interoperability of 802.11b & 802.11g devices in the same location. When the CTS Protection mechanism is enabled, 802.11g devices will inform 802.11b devices (using either a CTS/RTS or CTS-Self broadcast message) whenever a 802.11g data transmission is to occur. Enabling CTS Protection will reduce the throughput performance of your access point.

The options available for CTS Protection mode are **none**, **always** and **auto** (with the default being auto). In Auto mode, the Dell Wireless 4350 Small Network Access Point will only enable CTS Protection if any 802.11b devices exist within it's wireless range. If the mode is set to none, CTS Protection is disabled. If the mode is set to always, the CTS protection mode is always on.

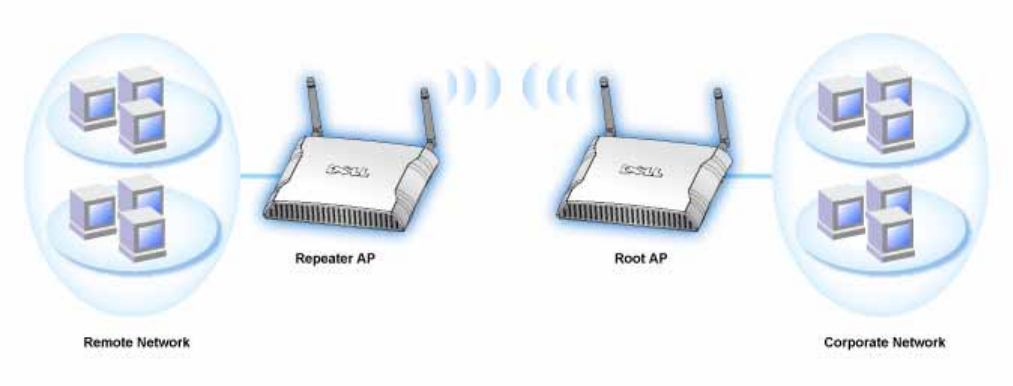
The options available for CTS Protection Type are **CTS/RTS** and **CTS-Self** (with the default being CTS-Self). The CTS/RTS mechanism results in a lower throughput performance than the CTS-Self mechanism.

Wireless Repeater

The Wireless Repeater setting can be used to increase the coverage of your wireless network. You need two or more Dell Wireless 4350 Small Network Access Point to set up wireless

repeating. The access point that is connected to the network is known as the “root AP”, the access points that extend the coverage of this root AP are known as “repeater AP’s”.

Wireless Repeater Link



To Configure your Access Point as a Wireless Repeater:

1. Click the option **Enable this AP as a Wireless Repeater.**
2. Type the wireless network name (SSID) of the root AP in the **SSID of root AP** field.
3. Set the “Network Encryption” mode as **None,** If the root AP does not provide wireless security.
4. set the “Network Encryption” mode as **WEP,** If the wireless security mode of the root AP is WEP. Then, set the proper key value, key length, key format, and default key.
5. Click the **Submit** button.

The repeater AP must be located within the coverage of your root AP in order to associate with the root AP and extend it's coverage. The repeater AP should not be connected into the wired network.

NOTE: Ensure all Dell Wireless 4350 Small Network Access Points are set to same wireless settings.

To Configure your Access Point back as a root AP:

There are 2 options available to configure your access point back as a root AP (a) reset the device back to it's defaults by pressing the reset button on the device for at least 5 seconds or (b) connect a computer to the repeater AP via an ethernet cable and browse to the AP's default IP address of 192.168.2.1 and perform the following steps.

1. Click the option **Enable this AP as a Root AP**
2. Click the **Submit** button.

Restore Defaults

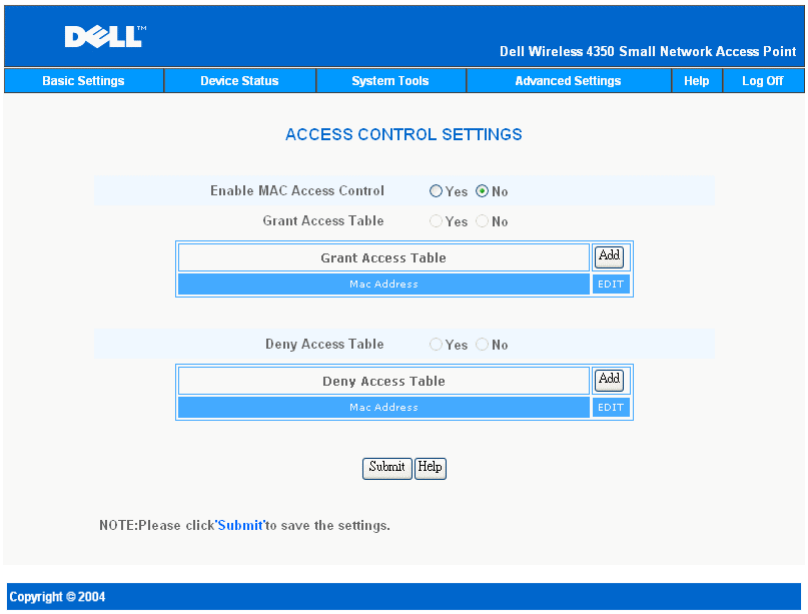
If you have customized your wireless system configuration, you can restore the wireless settings to factory defaults by clicking the **Restore Defaults** button.

Access Control Settings

The Access Control Settings page allows you to control which local client computer is allowed to access the network through the Dell Wireless 4350 Small Network Access Point based on the client computer's MAC address. The default setting is to allow any client computer to access the network through the access point.

There are two tables for the Access Control Settings, the Grant Access Table and the Deny Access Table. Each table is able to support up to 32 entries. Only one table can be active at any time. Selecting the checkbox for the Grant Access Table will disable the Deny Access Table and vice versa. The Grant Access Table will only allow clients that are listed in the table to access the network. The Deny Access table will prevent any clients that are listed in the table from accessing the network.

Access Control Settings



To enable access control in the access point, perform the following steps:

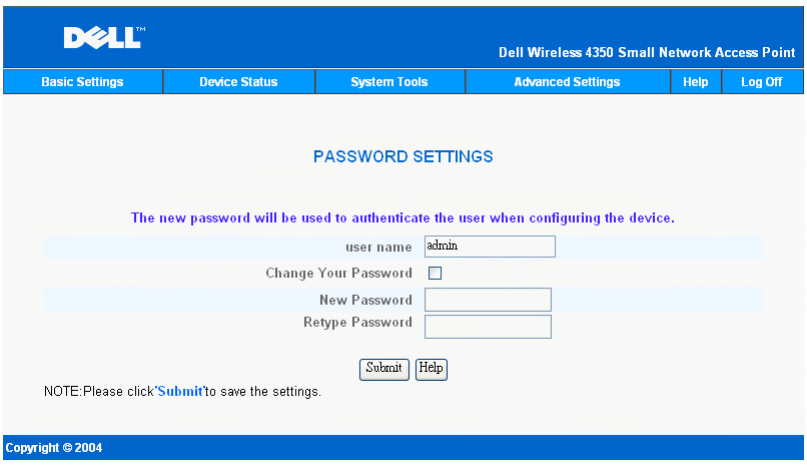
1. Click **Yes** to enable **Enable MAC Access Control**.
2. Click **Yes** to enable the appropriate table, the **Grant Access Table** or the **Deny Access Table**.
3. Click the **Add** button, a pop-up window will open, then enter the MAC address of the network card on the computer that you wish to add to the table.
4. Click **Submit** to enter the MAC address into the table.
5. Click **Submit** to enable the new table's entries.
6. To remove an existing rule, click to select **edit** beside **MAC address**.
7. A pop-up window will open and click the **DEL** button to remove it.

NOTE: The Access Control Settings apply to wireless client computers.

Administration Settings

The Administration Settings page allows the user to change the password settings for administrator access to the Dell Wireless 4350 Small Network Access Point.

Administration Settings



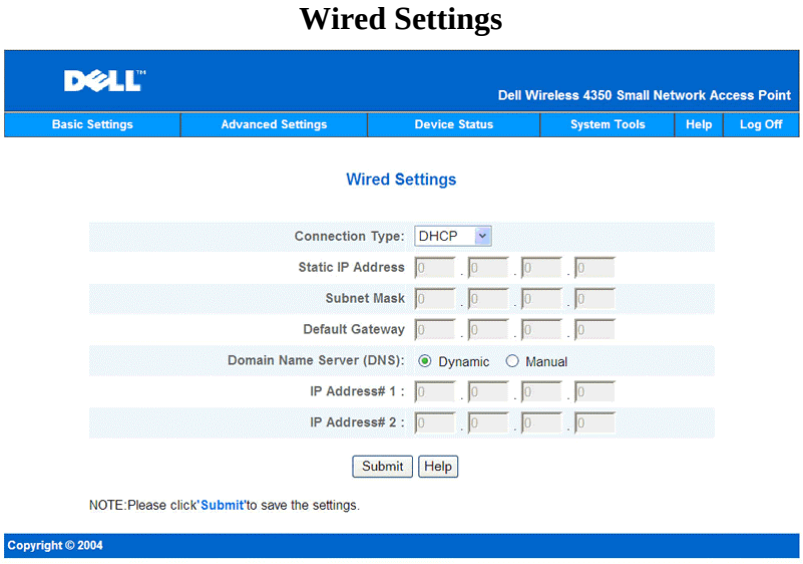
Password Settings

The Dell Wireless 4350 Small Network Access Point uses a password to authenticate the user before allowing the user access to the web configuration tool or Control Utility.

If you would like to change the current password, click to select **Change Your Password** and enter the new password in both **New Password** and **Retype Password** fields. Write down the password and keep it in a secure location for future reference.

Wired Settings

The Wired Settings page allows the user to configure the IP and DNS settings for the network port of the Dell Wireless 4350 Small Network Access Point.



If the access point will obtain an IP address automatically from a DHCP server, select the **Connection Type** as **DHCP**. If you would like to assign the access point a static IP address, select the **Connection Type** as **Static IP** and enter an IP address, Subnet Mask and Default Gateway in the corresponding fields.

If the access point will obtain DNS server information automatically from the network, select the **Domain Name Server (DNS)** as **Dynamic.** If you would like to assign the DNS server addresses, select the **Domain Name Server (DNS)** as **Manual** and enter either one or two DMS server IP addresses in the corresponding fields.

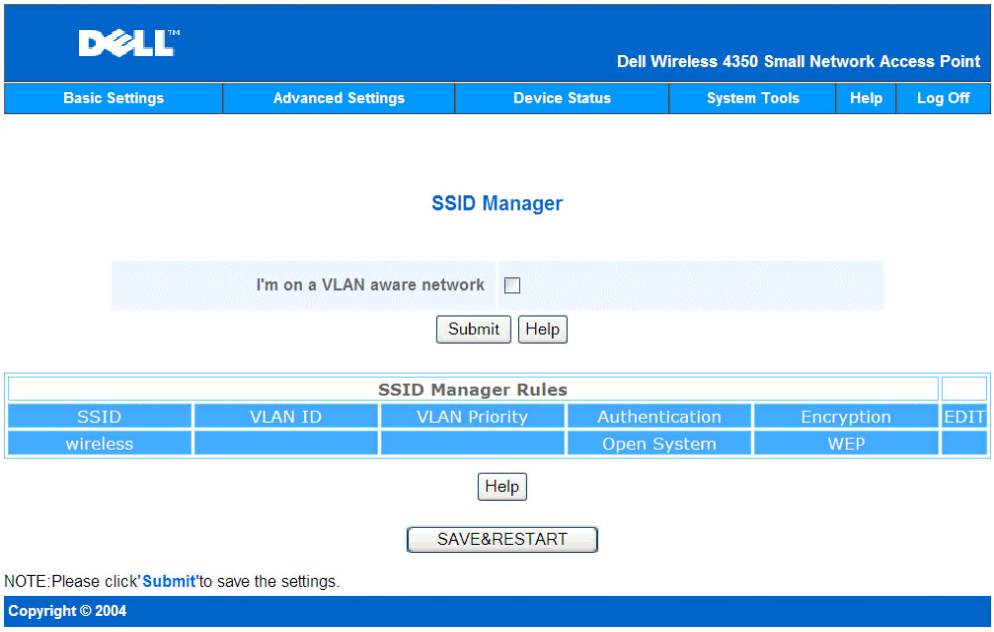
SSID Manager

The SSID Manager page allows the user to configure up to a maximum of three different SSID’s that the Dell Wireless 4350 Small Network Access Point supports. One of these three SSID’s is the Guest Access SSID, which will allow guest users to connect to the network with controlled access to network resources.

NOTE: In order to support multiple SSID's, the Dell Wireless 4350 Small Network Access Point must be part of a VLAN-aware network, as the VLAN aware router will control

the network access of the multiple wireless networks.

SSID Manager



To configure multiple SSID's (VLAN-aware network):

In a VLAN-aware network, the Dell Wireless 4350 Small Network Access Point can support three SSID's (one of which is the Guest Access SSID). In this network, the user has the option of configuring VLAN tags to be associated with wireless traffic from each SSID. To add an extra SSID:

1. Click to select **I'm on a VLAN aware network**.
2. Click the **Submit** button.
3. A warning message appears informing the user that the network must be a VLAN aware network. Click **OK**.
4. Click the **Add** button in the SSID Manager Rules table.
5. A pop-up window is displayed to the user. Populate the following fields with the appropriate information (a) Network Name (SSID) (b) VLAN ID (c) VLAN Priority (d) Hide my wireless Network (e) Enable Intra-AP traffic blocking and (f) Network Encryption.
6. Click **Submit** to save the settings for the new SSID.
7. Click **Save & Restart** to enable the new SSID.

NOTE: If the VLAN ID of an SSID is different from the default SSID, then wireless clients

	associated with this SSID network will not be able to manage the Dell Wireless 4350 Small Network Access Point.

To enable the Guest Access SSID (VLAN-aware network):

To enable Guest Access mode, the Dell Wireless 4350 Small Network Access Point must be part of a VLAN-aware network. Perform the following steps to enable the feature.

1. Click to select **I'm on a VLAN-aware network**.
2. Click to select **Enable Guest Access**.
3. Click the **Submit** button.
4. A pre-configured Guest Access SSID is created with the following default values (a) SSID = Guest Wireless 4350 (b) Network Encryption = None (c) VLAN ID = 4094 (d) VLAN Priority = 0 (e) Intra-AP blocking = off. These values can be altered by selecting the **Edit** button and changing the appropriate fields.
5. Click **Save & Restart** to enable the Guest Access SSID

NOTE:	In order to support Guest Access mode, the Dell Wireless 4350 Small Network Access Point must be part of a VLAN-aware network. The VLAN aware router must implement the appropriate restrictions that are applicable to a guest user (e.g. the router will only allow the user access to the Internet and prevent access to any network resource).

To disable the Guest Access SSID (VLAN-aware network):

The Guest Access SSID cannot be deleted, to disable Guest Access, Click to unselect **Enable Guest Access** and click **Submit.**l

A brief description of the SSID configuration parameters is as follows:

SSID:

The Service Set Identifier (SSID) is a 32-character name that uniquely identifies all the computers and equipment that make up the wireless Network.

VLAN ID:

The VLAN ID is a tag that is used to identify each VLAN on the network.

VLAN Priority:

The VLAN priority is a tag that is used to perform QoS between VLANs on a network.

Hide my wireless network:

This setting will disable the transmission of beacon packets (i.e. The AP will no longer broadcast it's SSID).

Enable Intra-AP Traffic Blocking:

This setting will prevent clients on the same wireless network from communicating with each other.

Network Encryption:

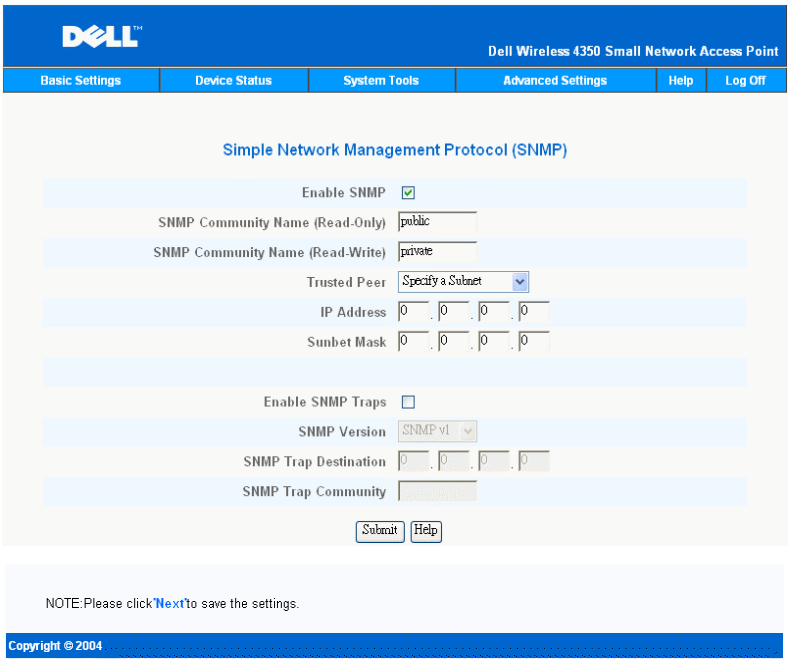
The access point supports the following methods of data encryption (a) WEP (b) WPA-PSK & (c) WPA-802.1x.

The following are possible security levels that can be configured in a multiple SSID environment. (1) WEP & No encryption (2) WPA-PSK & No encryption (3) WPA-PSK & WEP (4) WPA-802.1x & No encryption (5) WPA-802.1x & WEP (6) WPA-PSK, WEP & No encryption (7) WPA-802.1x, WEP & No encryption

SNMP

The Dell Wireless 4350 Small Network Access Point also supports the SNMP protocol for remote management of the access point. Simple Network Management Protocol (SNMP) is a popular network protocol for remotely configuring and monitoring devices. This feature requires an external SNMP management station to control and access the device. The SNMP protocol versions supported by the access point are v1, v2c and v3.

SNMP



To enable SNMP protocol support:

1. Click to select **Enable SNMP**.
2. The **SNMP Community Names** are passwords used in SNMP messages between

the access point and the SNMP management system. A **Read-Only** community allows the management system to monitor the device, while a **Read-Write** community can both monitor and configure the device. Enter the Get and Set community names in the appropriate fields.

3. The **Trusted Peer** identifies which remote managements stations are allowed to perform SNMP operations on the device. The options available for a trusted peer are (a) Any Address (b) Specify an IP Address & (c) Specify a Subnet. Select the appropriate option and enter the **IP Address** and **Subnet Mask** into the appropriate fields.

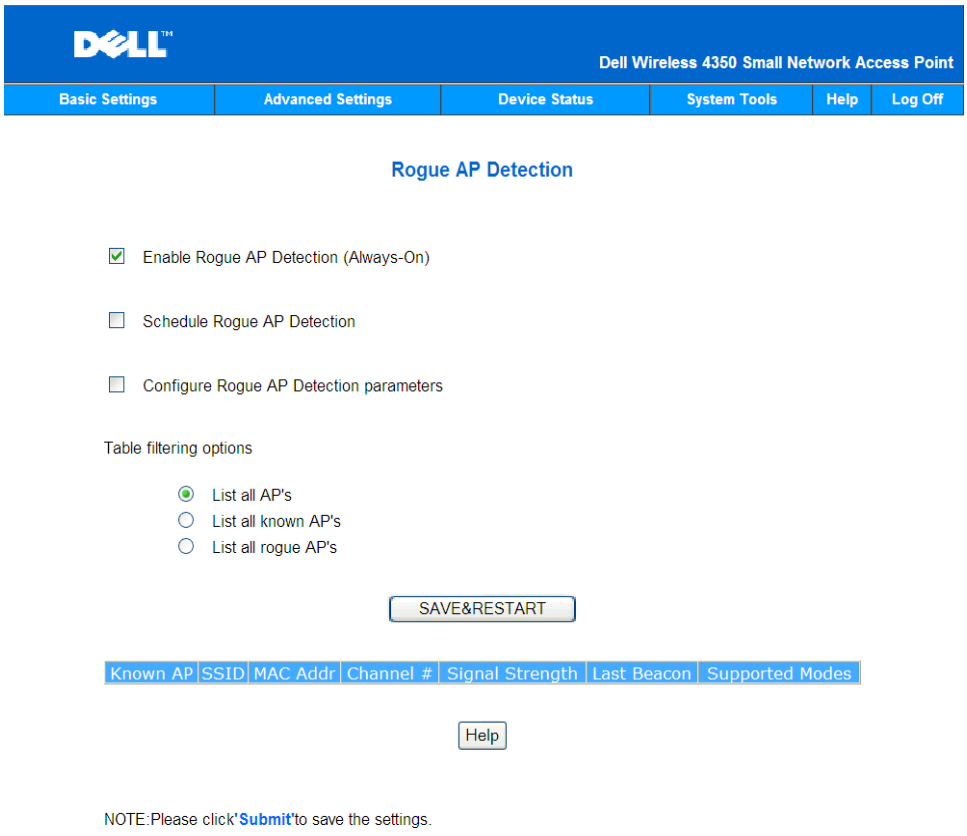
To enable SNMP Trap support:

1. **SNMP Traps** are messages sent by the access point to a SNMP management station in order to notify it about the occurrence of important events or conditions on the device. To enable SNMP Traps, click **Enable SNMP Traps**.
2. The access point supports SNMP version 1, version 2c and version 3 traps. Select the appropriate version for your management station in the **SNMP Version** list.
3. Enter the appropriate information on your management station into the **SNMP Trap Destination** and **SNMP Trap Community** fields

Rogue AP Detection

The Rogue AP Detection feature is an advanced feature that is used by network administrators to scan for adjacent access points. A table of detected access points is presented to the administrator and a determination if any rogue access points are present on the network can be made by verifying the SSID and MAC addresses.

Rogue AP Detection



There are three modes of operation for Rogue AP detection (a) Background scan (always-on), (b) Background scan (scheduled) & (c) Foreground scan.

When the background scan is enabled, the access point will periodically scan the wireless channels (a single channel at a time for 400 ms) if and only if certain load conditions are met. Any wireless stations that are associated to the AP may experience a loss of the AP during the scan interval. The background scan can either be running continuously or scheduled to run during specific periods. If scheduled, the background scan should run during periods of inactivity (e.g. during the night or at weekends).

When a foreground scan occurs, the AP will immediately reset and upon reboot will scan all the available wireless channels for an extended period. A foreground scan will cause immediate termination of all and any wireless clients.

Enable Rogue AP Detection - Background Scan (always-on):

To enable the background scan (always-on) mode of Rogue AP detection, perform the following steps:

1. Click to select **Enable Rogue AP Detection (Always-On).**
2. Click **Save & Restart**.

NOTE: Any wireless stations that are associated to the Dell Wireless 4350 Small Network Access Point may experience a loss of connection to the access point during the scan interval.

Enable Rogue AP Detection - Background Scan (Scheduled):

To enable the background scan mode of Rogue AP detection, perform the following steps:

1. Click to select **Enable Rogue AP Detection (Always-On).**
2. Click to select **Schedule Rogue AP Detection** and populate the relevant fields (i.e. Start time, Stop time and specific day of the week).
3. Click **Save & Restart**.

NOTE: Any wireless stations that are associated to the Dell Wireless 4350 Small Network Access Point may experience a loss of connection to the access point during the scan interval.

Enable Rogue AP Detection - Foreground Scan:

To enable the foreground scan mode of Rogue AP detection, the user must:

1. Click to select **Enable Rogue AP Detection (Always-On).**
2. Click the **Scan Now** button.

NOTE: Any wireless stations that are associated to the Dell Wireless 4350 Small Network Access Point will loss connection to the access point during the scan interval.

The Rogue AP detection parameters can be varied from their default values. The default values are (a) Rogue AP Detection Scan Interval = 1 minute. (b) Table Entry Removal of Absent Access Points = 1440 minutes (i.e. 24 hours). The Rogue AP Detection Scan Interval parameter determines how often a background scan may be performed by the access point. The Table Entry Removal of Absent Access Points parameter determines how long an entry will appear in the table before it is removed.

To configure the Rogue AP Detection Parameters:

1. Click to select **Enable Rogue AP Detection (Always-On)**.
2. Click to select **Configure Rogue AP Detection Parameters.**
3. Change the appropriate parameter(s) to the desired value(s).
4. Click **Save & Restart**.

The Table filtering options available are (a) List all AP's (b) List all known AP's & (c) List all rogue AP's. The table of detected AP's contains a column "Known AP" that allows the user to

select whether this AP is either a known or rogue AP (this would normally be based on information such as SSID & MAC Address). The option “List all AP’s” lists all the AP’s detected. The option “List all known AP’s” lists all the known AP’s detected. The option “List all rogue AP’s” lists all the rogue AP’s detected.

To change the Table Filtering Options:

1. Click to select **Enable Rogue AP Detection (Always-On)**.
2. Click to select the appropriate table filtering option**.**
3. Click **Save & Restart**.