CHAPTER 13

Cisco Spectrum Expert Software Local Settings

Local Settings Overview

There are a number of settings you can change to determine how Cisco Spectrum Expert Software operates and presents data. The available settings are for:

- **Sensors and Antennas**—Determine which Sensor card Cisco Spectrum Expert Software uses to obtain data. For the internal Sensor card, you can also indicate the type of antenna in use.
- **Console Settings**—Use this to change the date formats seen on screen.
- **Band and Channel Settings**—Determines which 802.11 channels and how wide a bandwidth will be monitored by Cisco Spectrum Expert Sensor card.
- **Alert Settings**—Used to enable or disable security and performance alerts for an interferer type or category.
- **SNMP Option**—Cisco Spectrum Expert Software has an ability to send SNMP traps when it detects interfering devices. This screen is used to configure the trap filters and threshold levels that will trigger the sending of an SNMP trap. The **Settings – SNMP** screen is used to configure the trap filters and threshold levels that will trigger the sending of an SNMP trap.

Note The following MIB files are installed with Cisco Spectrum Expert Software under [install dir]\Cognio\Spectrum Expert\MIB and are used by the trap receiver:

File	Description
COGNIO-SMI.mib	**Enterprise OID**
COGNIO-TRAPS-MIB.mib	**Trap definition. Refer to this file for the complete trap OID information.**
INET-ADDRESS.mib	**MIB file that traps are dependent on**
SNMP-FRAMEWORK-MIB.mib	**MIB file that traps are dependent on**
SNMPv2-CONF.mib	**MIB file that traps are dependent on**
SNMPv2-SMI.mib	**MIB file that traps are dependent on**
SNMPv2-TC.mib	**MIB file that traps are dependent on**

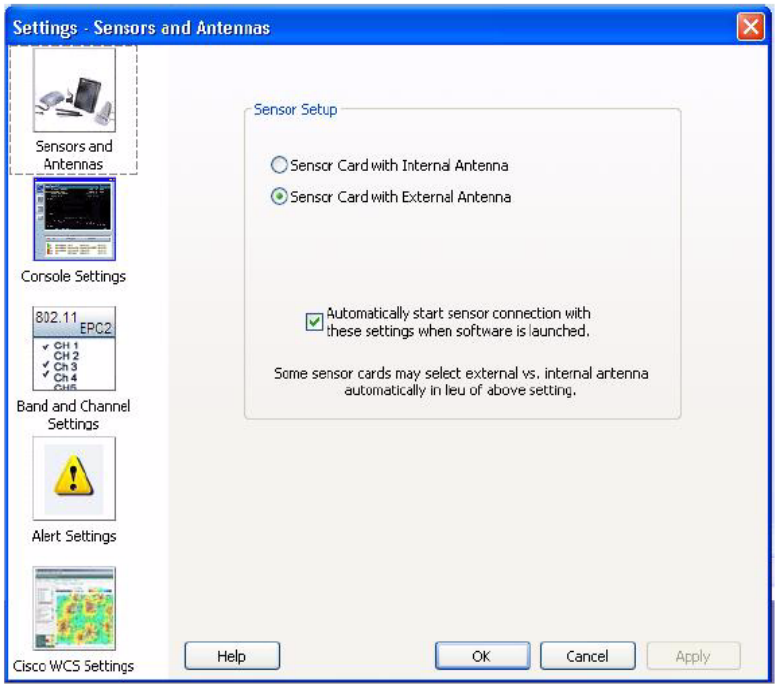
Sensors and Antennas

To modify which Spectrum Sensor card and/or antennas are used by Cisco Spectrum Expert Software, follow these steps:

Step 1 Select **Tools > Settings**.

The **Sensor Setup** panel should be displayed by default. If it is not, select the **Sensors and Antennas** button on the tool bar at left.

Step 2 Select the Sensor card/antenna combination of interest. Your choices are:



Sensor Setup

○ Sensor Card with Internal Antenna

● Sensor Card with External Antenna

☑ Automatically start sensor connection with these settings when software is launched.

Some sensor cards may select external vs. internal antenna automatically in leu of above setting.

- **Sensor Card With Internal Antenna**—Tells the application to use data from the internal Sensor card. Also tells the Sensor to use its internal antenna.
- **Sensor Card With External Antenna**—Tells the application to use data from the internal Sensor card. Also tells the Sensor to use its external antenna.
- **Spectrum Capture File**— Enables you to select a CSC file for playback. Select the **[Browse…]** button to browse for a particular CSC file. See "Spectrum Recording and Playback" for more information.

Step 3 Optionally, select the **Automatically Use These Settings At Startup** check box. If you select this option, the application will automatically use these settings each time the application is started.

If left unchecked, the Cisco Spectrum Expert Software present a dialog box each time the program starts, asking you which Sensor card to use.

Step 4 Select **[OK]** to confirm your changes and close the dialog box. You can also select **[Apply]** to apply your changes while leaving the dialog box open for further work.

Console Settings

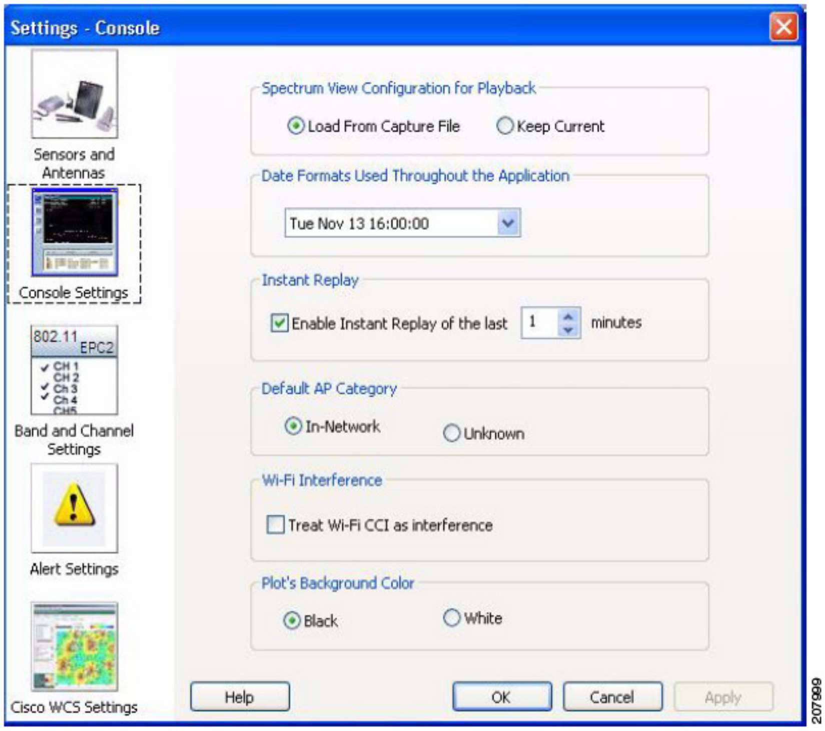
To fine-tune how the Cisco Spectrum Expert Software displays data, follow these steps:

Step 1 Select **Tools > Settings.**

Step 2 From the tool bar on the left side of the dialog box, select **Console Settings**

Step 3 You can change the following settings:

- **Spectrum View Configuration for Playback**
- **Date Formats Used Throughout the software**—Select from the drop-down menu.
- **Instant Replay—** Select the checkbox and the number of minutes (1 to 60) you want available for use as an instant replay.
- **Default AP Category—** In-Network or Unknown.
- **Plot's Background Color—**Black or White as the background color.



Spectrum View Configuration for Playback

● Load From Capture File ○ Keep Current

Date Formats Used Throughout the Application

Tue Nov 13 16:00:00

Instant Replay

☑ Enable Instant Replay of the last 1 minutes

Default AP Category

● In-Network ○ Unknown

Wi-Fi Interference

□ Treat Wi-Fi CCI as interference

Plot's Background Color

● Black ○ White

Step 4 Select **OK** to confirm your changes and close the dialog box. You can also select **Apply** to apply your changes while leaving the dialog box open for further work.

Band and Channel Settings

Here you can configure the bands and channels that Cisco Spectrum Expert Software will monitor and report on. You can select band and channel settings by Regulatory Domain or define the bands and channels individually by selecting the User Defined option.

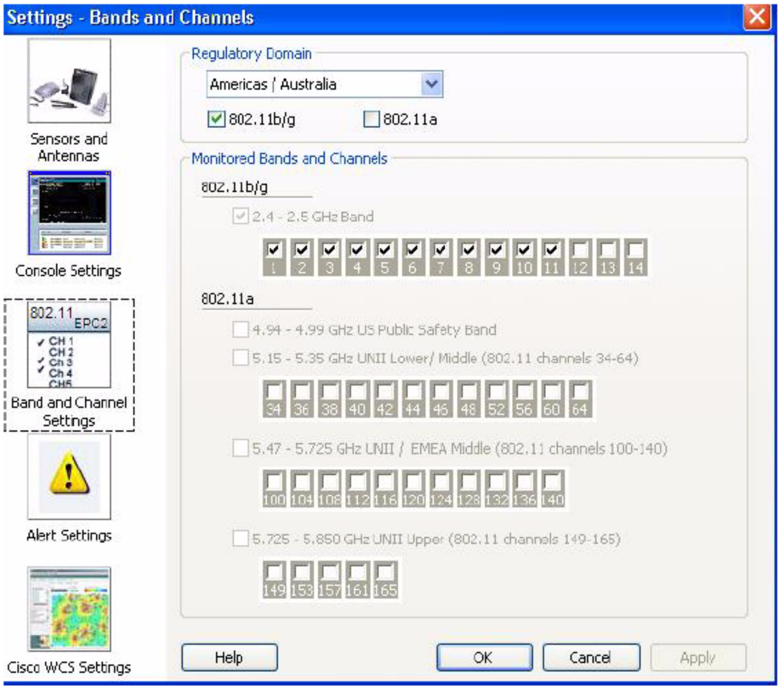
Regulatory Domain Options

To use a Regulatory Domain option to select the bands and channels, follow these steps:

Step 1 Select **Tools > Setting.**

Step 2 From the tool bar on the left side of the dialog box, select **Band and Channel Settings.**

Step 3 From the **Regulatory Domain** pane drop-down pick list, select the regulatory domain to monitor. You have the following options**:**



Regulatory Domain

Americas / Australia

☑ 802.11b/g ☐ 802.11a

Monitored Bands and Channels

802.11b/g

☑ 2.4 - 2.5 GHz Band

☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☐ 12 ☐ 13 ☐ 14

802.11a

☐ 4.94 - 4.99 GHz US Public Safety Band

☐ 5.15 - 5.35 GHz UNII Lower/ Middle (802.11 channels 34-64)

☐ 34 ☐ 36 ☐ 38 ☐ 40 ☐ 42 ☐ 44 ☐ 46 ☐ 48 ☐ 52 ☐ 56 ☐ 60 ☐ 64

☐ 5.47 - 5.725 GHz UNII / EMEA Middle (802.11 channels 100-140)

☐ 100 ☐ 104 ☐ 108 ☐ 112 ☐ 116 ☐ 120 ☐ 124 ☐ 128 ☐ 132 ☐ 136 ☐ 140

☐ 5.725 - 5.850 GHz UNII Upper (802.11 channels 149-165)

☐ 149 ☐ 153 ☐ 157 ☐ 161 ☐ 165

- For **Wi-Fi**, the options include: **Americas/Australia**, **EMEA/Asia/Pacific**, **Japan**, **All Wi-Fi Channels**. For Wi-Fi, it is further possible to select the Wi-Fi standard to be covered (802.11 a, 802.11 b/g, or both) using the checkboxes. The single regulatory domain pick will apply to both Wi-Fi standards.

Note The controls in the **Monitored Bands and Channels** control pane also display the bands and channels that will be monitored when a Regulatory Domain is picked.

Step 4 Select **OK** to confirm your changes and close the dialog box. You can also select **[Apply]** to apply your changes while leaving the dialog box open for further work**.**

Note Regulatory Domains are subject to change without notice.

User Defined Option

To use the **User Defined** option to select the bands and channels, follow these steps:

Step 1 Select **Tools > Settings…**

Step 2 From the tool bar on the left side of the dialog box, select **Band and Channel Settings.**

Step 3 From the **Regulatory Domain** pane drop-down pick list, select the User Defined option.

Step 4 When you selected **User Defined**, the individual band and channel monitoring check boxes are enabled and you can select the bands and corresponding channels to monitor.

Step 5 Select one or more of the available bands from the **Monitored Bands and Channels** control pane.

Step 6 Select one or more of the available channels check boxes for each band selected.

Step 7 Select **[OK]** to confirm your changes and close the dialog box. You can also select **[Apply]** to apply your changes while leaving the dialog box open for further work**.**

Monitoring

The Sensor card is capable of monitoring up to 1 GHz of RF bandwidth at a time. In practice, however, monitoring this much of the spectrum can result in some performance issues for Cisco Spectrum Expert Software. Moreover, for most practical software, it is rarely necessary to monitor that much of the spectrum at one time.

The **Band and Channel** settings enable you to determine how much bandwidth is actually monitored by the Sensor card. Monitoring only the bandwidth you need to monitor—rather than trying to have the Sensor card scan its full potential range—will result in more effective system performance.

- If you change the settings for monitored bands and channels, the Cisco Spectrum Expert Software automatically restarts, clearing all internal buffers. The display does not close down, but you lose any data currently shown on the spectrum plots, **Channel Summary**, **Devices View**, and so on.
- The bands and channels you define here determine which bands and channels are available for selection on the spectrum plots. See "Band and Channel Settings" for more information.
- If you select two bands which are adjacent or which overlap (for example, 5.47 to 5.725 GHz, and 5.725 to 5.850 GHz), Cisco Spectrum Expert Software will automatically consolidate the two bands into one band.

You can select one or more of the bands, such as the 2.4 to 2.5 GHz band, the 5.15 to 5.35 GHz band (for Wi-Fi). Selecting all or most of the bands shown may result in reduced performance or data quality, so we suggest that you select only those bands that are essential for your current monitoring and testing needs.

Alert Settings

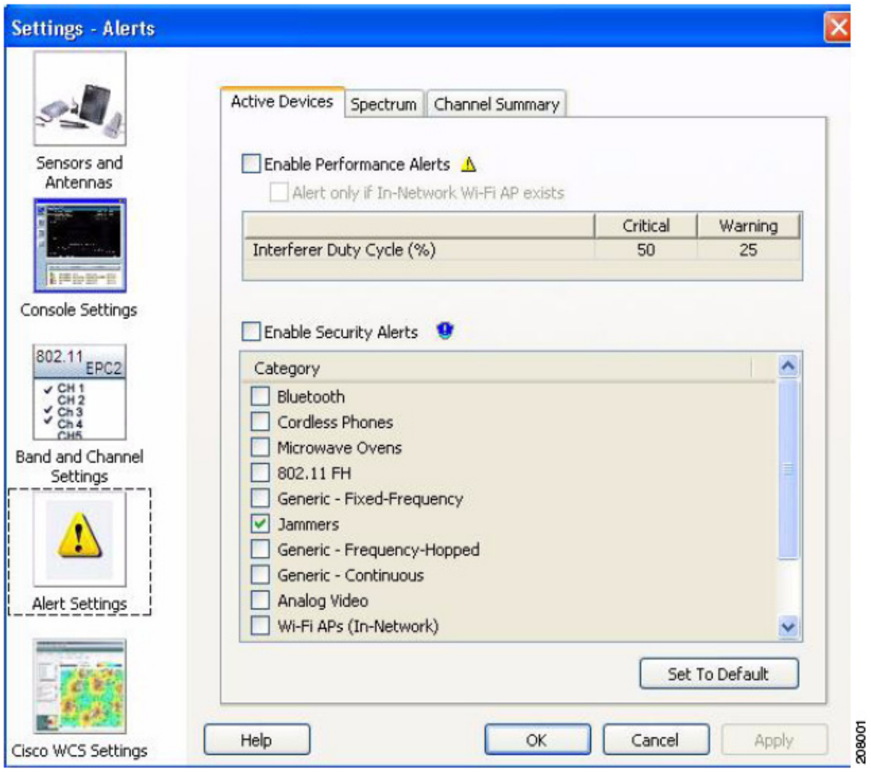
The **Settings - Alert** screen is used to configure security and performance alerts. This screen consists of three tabs:

- **Active Devices—**This tab is used to enable or disable a security alert for an interferer type or category. Security alerts can be enabled/disabled for one, multiple, or all interferer categories.
- **Spectrum—**This tab is use to enable or disable alerts.
- **Channel Summary—**This tab is used to enable or disable alerts for channels devices being displayed on the Channel Summary view.

To enable performance alerts, follow these steps:

Step 1 Select **Tools > Settings…**

Step 2 From the tool bar on the left side of the dialog box, select **Alert Settings**.



□ Enable Performance Alerts ⚠

□ Alert only if In-Network Wi-Fi AP exists

	Critical	Warning
Interferer Duty Cycle (%)	50	25

□ Enable Security Alerts

Category
- □ Bluetooth
- □ Cordless Phones
- □ Microwave Ovens
- □ 802.11 FH
- □ Generic - Fixed-Frequency
- ☑ Jammers
- □ Generic - Frequency-Hopped
- □ Generic - Continuous
- □ Analog Video
- □ Wi-Fi APs (In-Network)

To enable alerts for active devices, follow these steps:

Step 1 Select the **Active Devices** tab.

Step 2 Check **Enable Performance Alerts**.

Step 3 Check **Alert only if In-Network Wi-Fi access points exists**.

Step 4 Check **Enable Security Alerts**.

Step 5 In the **Category** pane, check one or multiple device categories for performance monitoring and alerts.

Note The default settings are **Jammers** and **Wi-Fi Ad Hocs** boxes checked.

Step 6 Select **Apply** or **OK**.

When the **Enable Performance Alerts** and the **Alert only if In-Network Wi-Fi access point exists** fields are checked (selected) on the **Active Devices** tab, and at least one In-Network Wi-Fi access point is present on the same channel as the interferer, all active interferers display with or with out a security alert icon in the **Active Device** pane on the **Main** window.

- If the interferer duty cycle is greater than 50% (default critical threshold value), the device displays in **Red**.

If the total duty cycle is greater than 25% (default warning threshold value), but less than 50, the device displays in **Yellow**.

To enable Security Alerts for Spectrum, follow these steps:

Step 1 Select the **Spectrum** tab.

Step 2 Check the Enable Spectrum Alerts check box. The default settings are shown in the figure.

Step 3 Select **Apply** or **OK**.

To enable alerts for Channel Summary, follow these steps:

Step 1 Select the **Channel Summary** tab.

Step 2 Check the **Enable Channel Summary Alerts** check box. The default settings are shown in the figure.

Step 3 Check the **Alert only if In-Network Wi-Fi access point exists** check box if you want this condition to be met before having Spectrum generate a Channel Summary alert.

Step 4 Select **Apply** or **OK**.

SNMP Option Settings

The **SNMP Option** icon appears in the Cisco Spectrum Expert Software standard version. Use section SNMP Option Settings to configure the SNMP settings. If you are using the Cisco enabled Cisco Spectrum Expert Software version, then refer to section 12.6 WCS Settings**.**

The **Settings - SNMP** screen is used to enable and configure the trap filters and threshold levels that will trigger the sending of an SNMP trap for detected interferers to the designated IP Address. The screen consists of the following two tabs:

- Basic Settings
- Filters

Basic Settings Tab

The **Basic Settings** tab has two primary functions; a) to enable SNMP Traps and b) identify the designated devices using filters.

Send Spectrum Data to a Remote Computer

The **Send Spectrum Data to a Remote Computer** area contains a checkbox titled **Enable SNMP Traps for Interfering Devices** to enable the SNMP trap function and the IP Address and Computer Name fields.

IP Address or Computer Name of the Remote Computer

The **IP Address or Computer Name of the Remote Computer** area provides IP Address and Computer name fields to identify the target system for SNMP traps.

Filters Tab

The **Filters** tab provides criteria an interferer must meet to trigger sending a trap. The four selectable criteria are:

- Active Channel Filter - is there an active In-Network Wi-Fi access point on at least one of the affected channels? The default state is DISABLED.
- Interference Channel Utilization Filter - does an affected channel have an interferer utilizing more than the user set channel utilization percentage? The default state is ENABLED and default threshold value is 10%.
- Interference Power Filter - does an affected channel have cumulative power of all interference devices at a power level within or exceeding a user set level in dBm? The default state is ENABLED. The default value for the within range is 16 dB and the exceeding default value is -70 dBm.
- Interferer Type - are there specific interferer device types that you want to trigger SNMP traps? **The type of Interferer is selected on the following list:** check box, when checked, enables the scrollable list of devices check boxes for inclusion in the trap. The default setting is DISABLED.

Modifying Trap Filters Default Settings

All threshold values are editable, meaning they can be changed to reflect differing criteria.

To modify the SNMP Traps and trap filters settings, follow these steps:

Step 1 Left-click in the box adjacent to the trap criteria to apply.

Step 2 Edit the existing value or enter a new value.

Step 3 Left-click the box adjacent to the next trap criteria to apply.

Step 4 Select **<Apply>**.

Step 5 Select **<OK>**.

Trap Filter Information Content

The trap will include the following information:

- Device Uptime
- MAC Address and Power level of top five access points
- Unique Instance ID of device
- Type of Device (Numeric code)
- Filter Parameters (when filter is enabled)
- Channel Number, Interference Utilization
- Access point MAC Address, Access point Power, Interference Power
- Device Parameters (when appropriate – not all devices will have all parameters):

- Center Frequency
- Bandwidth
- Power in dBm
- Duty Cycle
- Channels affected
- Network address
- Pulses per second
- Pulse duration
- Modulation Type: Tone, video, AM, FM, QAM, OFDM, Chirp (Numeric code)
- PLL offset
- Frequency Deviation
- Symbol rate
- Bits per symbol
- Guard interval
- Peak to average power
- Period
- Phase
- Transmit type

Set SNMP Traps

To enable SNMP traps, follow these steps:

Step 1 Select **Tools > Settings…**

Step 2 From the tool bar on the left side of the dialog box, select **SNMP Option**.

Step 3 On the **Basic Settings** tab, select the **Enable SNMP Traps for Interfering Devices**: checkbox to enable sending SNMP traps.

Step 4 In the **IP Address or Computer Name of the Remote Computer** area, enter either the IP Address or Computer Name in the appropriate field to identify the target system that will receive the SNMP trap data.

Step 5 Select **Apply.**

Step 6 Select the **Filters** tab.

Step 7 In the **Filters** tab, select the trap filter parameters that will trigger sending an SNMP trap for a detected interferer.

Step 8 Check the **The type of Interferer is selected on the following list:** check box, as required, to select specific device types from the scrollable list of device type check boxes.

Step 9 Select **Apply** or **OK.**

Cisco WCS Settings

Note The **Cisco WCS Settings** icon appears in the Cisco WCS-enabled Cisco Spectrum Expert Software version. Use Configure WCS Settings to configure the WCS enabled settings. If you are using the Spectrum Expert standard version with SNMP Option, refer to "SNMP Option Settings."

The **Settings – WCS Settings** screen is used to enable and configure the filters and threshold levels that will trigger the sending of Cisco Spectrum Expert Software data to the designated WCS IP Address. The screen consists of the following four tabs:

- Basic Settings
- Filters Tab
- Security
- Advanced

Basic Settings

The **Basic Settings** tab has two primary functions. One function is to enable SNMP Traps or Cisco WCS functions and also to identify the designated IP Address of the remote computer where Cisco Spectrum Expert Software data will be sent. The functions are supported by these two areas on the **Basic Settings** tab:

- Send Spectrum Data to a Remote Computer - the **Send Spectrum Data to a Remote Computer** area contains two check boxes:
  - A checkbox labeled **Enable SNMP Traps for Interfering Devices**, to enable the SNMP trap function and,
  - A checkbox labeled **Enable Cisco WCS Transmission of Spectrum Data**, to enable the Cisco WCS function and the IP Address and Computer Name fields.
- IP Address or Computer Name of the Remote Computer - the **IP Address or Computer Name of the Remote Computer** area provides IP Address and Computer name fields to identify the target system for either the SNMP traps or Cisco WCS transmission of Cisco Spectrum Expert Software data.

Filters Tab

The **Filters** tab provides four selectable channel affecting acceptance criteria an interferer must meet to trigger sending a trap. The four selectable criteria are:

- **Active Channel Filter** - is there an active In-Network Wi-Fi Access point on at least one of the affected channels? The default state is DISABLED.
- **Interference Channel Utilization Filter** - does an affected channel have an interferer utilizing more than the user set channel utilization percentage? The default state is ENABLED and default threshold value is 10%.
- **Interference Power Filter** - does an affected channel have cumulative power of all interference devices at a power level within or exceeding a user set level in dBm? The default state is ENABLED. The default value for the within range is 16 dB and the exceeding default value is -70 dBm.

- **Interferer Type** - are there specific interferer device types that you want to include in the data sent to WCS? **The type of Interferer is selected on the following list:** check box, when checked, enables the scrollable list of devices check boxes for inclusion in the data sent to WCS. The default setting is DISABLED.

Modifying Filters Default Settings

All threshold values are editable, meaning they can be changed to reflect differing criteria.

To modify the filters settings, follow these steps:

Step 1 Left-click in the box adjacent to the filter criteria to apply.

Step 2 Edit the existing value or enter a new value.

Step 3 Left-click the box adjacent to the next filter criteria to apply.

Step 4 Select **Apply**.

Step 5 Select **OK**.

Security

The **Security** tab provides the ability to enable security measures, using certificates, for communications between Cisco Spectrum Expert Software and a Cisco WCS. Several selectable security level configurations are available to provide lower or higher security levels for the remote and local computers engaged in a Cisco WCS connection.

There are two selectable certificate options available for a remote computer (server), and two selectable certificate options available for a local computer. The user can define the combination of certificate criteria required in order to authorize a WCS connection. The selectable certificate-based security options are:

- Remote computer authorization for Cisco WCS Connections - having the following options:
  - Allow self-signed certificate for remote server (lower security level)
  - Require CA-signed certificate from remote server (higher security level)
- Identifying this computer for Cisco WCS Connections - having the following options:
  - Present self-signed certificate for this computer (lower security level)
  - Present the following CA-signed certificate for this computer (higher security level)

There are two fields available for identifying the specific CA-certificate to be used if the CA-signed option is selected for either the remote or local computer.

The Action if certificate information is not valid drop-down menu provides selectable actions to be taken upon receipt of invalid certificate information.

Advanced Tab

The **Advanced** tab provides an additional user definable setting for SNMP and four user definable WCS communication polling settings in two areas on the tab. SNMP and Cisco WCS Communication protocols function independently and can operate simultaneously. The settings are:

- Advanced Settings for SNMP - displays the **SNMP Trap Destination Port** number. The state is grayed-out (SNMP port can't be changed).
- Advanced Settings for Cisco WCS Communication - provides four user definable settings for Cisco WCS Communication parameters. The default state is ENABLED and is disabled by deselecting the **Enable Cisco WCS Transmission of Spectrum Data** checkbox on the Basic Settings tab. The user definable parameters are:
  - Transmit Devices information every ___ seconds. The default value is 10 seconds.
  - Limit the number of Device Update records to a maximum of ___ per transmission. The default value is 15 per transmission.
  - Consider a Cisco WCS to be temporarily unavailable after ___ unsuccessful attempts. The default value is 10 unsuccessful connection attempts.
  - Attempt reconnection to an unavailable server every ___ minutes. The default value is 10 minutes.

Configure WCS Settings

To configure WCS Settings, follow these steps:

Step 1 Select **Tools > Settings**

Step 2 From the tool bar on the left side of the dialog box, select **WCS Settings**.

Step 3 On the **Basic Settings** tab, select the **Enable Cisco WCS Transmission of Spectrum Data**: checkbox to enable sending Cisco Spectrum Expert Software data to the WCS

OR

On the **Basic Settings** tab, select the **Enable SNMP Traps for Interfering Devices**: checkbox to enable sending SNMP traps.

Step 4 In the **IP Address or Computer Name of the Remote Computer** area, enter either the IP Address or Computer Name in the appropriate field to identify the target system that will receive the Cisco Spectrum Expert Software data.

Step 5 Select **Apply**.

Step 6 Select the **Filters** tab.

Step 7 In the **Filters** tab, select the trap filter parameters that will define a detected interferer.

Step 8 Check **The type of Interferer is selected on the following list:** check box, as required, to select specific devices from the scrollable list of device check boxes.

Step 9 Select **Apply**.

Step 10 Select the **Security** tab.

Step 11 Select the desired certificate security option for the remote computer and add the CA-signed certificate as required.

Step 12 Select the desired certificate security option for the local computer and add the CA-signed certificate as required.

Step 13 Select the action to be taken if certificate information is not valid or leave the default action (**Warn**) active.

Step 14 Select **Apply** to continue to the **Advanced** tab or **OK** to complete the procedure.