APPENDIX B

Rogue Management

This appendix describes security issues and solutions for rogue access points.

This appendix contains the following sections:

Rogue Access Point Challenges

Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain text or other denial of service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as passwords and usernames. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an access point informing a particular wireless LAN client adapter to transmit and instructing all others to wait. This scenario results in legitimate clients being unable to access the wireless LAN resources. Thus, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the "Rogue Access Point Location, Tagging, and Containment" section on page B-1.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using the NCS, the NCS generates the flags as rogue access point traps and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the access points closest to each rogue access point. The next step is to mark them as Known or Acknowledged rogue access points (no further action), Alert rogue access points (watch for and notify when active), or Contained rogue access points (have between one and four access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points
- Receive new rogue access point notifications, eliminating hallway scans
- Monitor unknown rogue access points until they are eliminated or acknowledged
- Determine the closest authorized access point, making directed scans faster and more effective
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or wireless LAN security
  - Accept rogue access points when they do not compromise the LAN or wireless LAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
  - Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Detecting and Locating Rogue Access Points

When the access points on your wireless LAN are powered up and associated with controllers, the NCS immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies the NCS, which creates a rogue access point alarm.

When the NCS receives a rogue access point message from a controller, an alarm monitor appears in the lower left corner of all the NCS user interface page.

To detect and locate rogue access points, follow these steps:

Step 1 Click the Rogues indicator to display the Rogue AP Alarms page. This page lists the severity of the alarms, the rogue access point MAC addresses, the rogue access point types, the date and time when the rogue access points were first detected, and their SSIDs.

Step 2 Click any Rogue MAC Address link to display the associated Alarms > Rogue - AP MAC Address page. This page shows detailed information about the rogue access point alarm.

Step 3 To modify the alarm, choose one of these commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assigns the selected alarm to the current user.
- Unassign—Unassigns the selected alarm.
- Delete—Deletes the selected alarm.
- Clear—Clears the selected alarm.
- Event History—Enables you to view events for rogue alarms.
- Detecting APs (with radio band, location, SSID, channel number, WEP state, short or long preamble, RSSI, and SNR)—Enables you to view the access points that are currently detecting the rogue access point.
- Rogue Clients—Enables you to view the clients associated with this rogue access point.

- Set State to `Unknown - Alert'—Tags the rogue access point as the lowest threat, continues to monitor the rogue access point, and turns off containment.

  Set State to `Known - Internal'—Tags the rogue access point as internal, adds it to the known rogue access points list, and turns off containment.

  Set State to `Known - External'—Tags the rogue access point as external, adds it to the known rogue access points list, and turns off containment.

- 1 AP Containment through 4 AP Containment—When you select level 1 containment, one access point in the vicinity of the rogue unit sends deauthenticate and disassociate messages to the client devices that are associated to the rogue unit. When you select level 2 containment, two access points in the vicinity of the rogue unit send deauthenticate and disassociate messages to the rogue's clients and so on up to level 4.

Step 4 From the Select a command drop-down list, choose **Map (High Resolution),** and click **Go** to display the current calculated rogue access point location in the Maps > Building Name > Floor Name page.

If you are using the NCS Location, the NCS compares RSSI signal strength from two or more access points to find the most probable location of the rogue access point and places a small skull-and-crossbones indicator at its most likely location. In the case of an underdeployed network for location with only one access point and an omni antenna, the most likely location is somewhere on a ring around the access point, but the center of likelihood is at the access point. If you are using the NCS Base, the NCS relies on RSSI signal strength from the rogue access point and places a small skull-and-crossbones indicator next to the access point receiving the strongest RSSI signal from the rogue unit.

Monitoring Alarms

This section contains the following topics:

Monitoring Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco lightweight access points. This page displays rogue access point alarms based on the severity you clicked in the Alarm Monitor.

To access the Rogue AP Alarms page, do one of the following:

- Choose **Monitor** > **Alarms**. Click **Search** and choose **Rogue AP** from the Alarm Category drop-down list. Click **Go** to display the matching alarms.
- Choose **Monitor** > **Security**. From the left sidebar, choose **Rogue AP**.
- Click the **Malicious AP number** link in the Alarm Summary box of the left sidebar menu.

Note If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use the scroll arrows to view additional alarms.

Table N-1 describes the parameters found in the Rogue Access Point Alarms page.

Table N-1 Alarm Parameters

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear, Color coded.
Rogue MAC Address	Media Access Control address of the rogue access points. See Monitor Alarms > Rogue AP Details.
Vendor	Rogue access point vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue access point.
Strongest AP RSSI	Indicates the strongest Received Signal Strength Indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this access point.
Owner	Indicates the `owner' of the rogue access point.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known or Removed.
SSID	Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
Map Location	Indicates the map location for this rogue access point.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

Note The alarm remains in the NCS, and you can search for all Acknowledged alarms using the alarm search functionality.

Rogue AP Alarms page includes the following additional fields:

- Unacknowledge—Unacknowledge an already acknowledged alarm.
- E-mail Notification—Takes you to the All Alarms > E-mail Notification page to view and configure e-mail notifications. See Monitor Alarms > E-mail Notification for more information.
- Severity Configuration—Change the severity level for newly-generated alarms. See Monitor Alarms > Severity Configuration for more information.
- Detecting APs—View the Cisco lightweight access points that are currently detecting the rogue access point.
- Map (High Resolution)—Click to display a high-resolution map of the rogue access point location.

- Rogue Clients—Click to view a list of rogue clients associated with this rogue access point. The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the rogue access point.
- Set State to `Unclassified - Alert'—Choose this command to tag the rogue access point as the lowest threat, continue monitoring the rogue access point, and to turn off containment.
- Set State to `Malicious - Alert'—Choose this command to tag the rogue access point as Malicious.
- Set State to `Friendly - Internal'—Choose this command to tag the rogue access point as internal, add it to the Known Rogue APs list, and to turn off containment.
- 1 AP Containment—Target the rogue access point for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Target the rogue access point for containment by two Cisco lightweight access points.
- 3 AP Containment—Target the rogue access point for containment by three Cisco lightweight access points.
- 4 AP Containment—Target the rogue access point for containment by four Cisco lightweight access points. (Highest containment level.)

Caution Attempting to contain a rogue access point may lead to legal consequences. When you select any of the AP Containment commands and click Go, a message "Containing a Rogue AP may have legal consequences. Do you want to continue?" appears. Click **OK** if you are sure, or click **Cancel** if you do not want to contain any access points.

Monitoring Rogue Access Point Details

Alarm event details for each rogue access point are available in the Rogue AP Alarms page.

To view alarm events for a rogue access point radio, in the Rogue AP Alarms page, click an item under Rogue MAC Address.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco lightweight access points. The following information is available:

- General Info:
  - Rogue MAC Address—Media Access Control address of the rogue access points.
  - Vendor—Rogue access point vendor name or Unknown.
  - On Network—Indicates whether or not the rogue access point is located on the network.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue access point.
  - Containment Level—Indicates the containment level of the rogue access point or Unassigned.

  - Radio Type—Indicates the radio type for this rogue access point.
  - Strongest AP RSSI—Indicates the strongest received signal strength indicator in dBm.
  - No. of Rogue Clients—Indicates the number of rogue clients associated to this access point.
  - Created—Indicates when the alarm event was created.
  - Modified—Indicates when the alarm event was modified.
  - Generated By—Indicates how the alarm event was generated.
  - Severity—The severity of the alarm: Critical, Major, Minor, Clear, Color coded.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear, Color coded.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the Monitor Alarms > Events page.
- Annotations—Lists existing notes for this alarm.

Detecting Access Points on a Network

Use the Detecting Access Points feature to view information about the Cisco lightweight access points that are detecting a rogue access point.

To access the Rogue AP Alarms page, follow these steps:

Step 1 To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs. See the "Using the Search Feature" section on page 2-34 for more information about the search feature.
- From the NCS home page, click the Security dashboard. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the **Malicious AP** number link in the Alarm Summary box.

Step 2 From the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page appears.

Step 3 From the Select a command drop-down list, choose **Detecting AP on Network**.

Step 4 Click **Go.**

Click a list item to display data about that item:

- AP Name
- Radio
- Map Location
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio.
- Channel Number—The channel on which the rogue access point is broadcasting.
- WEP—Enabled or disabled.

- WPA—Enabled or disabled.
- Pre-Amble—Long or short.
- RSSI—Received signal strength indicator in dBm.
- SNR—Signal-to-noise ratio.
- Containment Type—Type of containment applied from this access point.
- Containment Channels—Channels that this access point is currently containing.

Monitoring Rogue Ad hoc Alarms

The]rogue Ad hoc Alarms page displays alarm events for rogue ad hocs.

To access the Rogue Adhoc Alarms page, do one of the following:

- Choose **Monitor > Alarms**. From the left sidebar menu, choose **New Search** and choose **Rogue Adhoc** from the Alarm Category drop-down list. Click **Go** to display the matching alarms.
- Choose **Monitor** > **Security**. From the left sidebar menu, choose **Rogue Adhocs**.

Note If there are multiple alarm page, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

Table N-2 describes the fields found in the Rogue Ad hoc Alarms page.

Table N-2 Rogue Ad hoc Alarms

Parameter	Description
Check box	Select the alarms on which you want to take action.
Severity	The severity of the alarm: Critical, Major, Minor, Clear, Color coded.
Rogue Adhoc MAC Address	Media Access Control address of the rogue ad hoc.
Vendor	Rogue ad hoc vendor name, or Unknown.
Classification Type	Malicious, Friendly, or Unclassified.
Radio Type	Indicates the radio type for this rogue ad hoc.
Strongest AP RSSI	Indicates the strongest Received Signal Strength Indicator in dBm.
No. of Rogue Clients	Indicates the number of rogue clients associated to this rogue ad hoc.
Owner	Indicates the ‘owner’ of the rogue ad hoc.
Date/Time	Date and time the alarm occurred.
State	State of the alarm: Alert, Known or Removed.
SSID	Service Set Identifier being broadcast by the rogue ad hoc radio. (Blank if the SSID is not broadcast.)
Map Location	Indicates the map location for this rogue ad hoc.
Acknowledged	Displays whether or not the alarm is acknowledged by the user.

Select a Command

Select one or more alarms by selecting their respective check boxes, choosing one of the following commands from the Select a command drop-down list, and click **Go**.

- Assign to me—Assigns the selected alarm(s) to the current user.
- Unassign—Unassigns the selected alarm(s).
- Delete—Deletes the selected alarm(s).
- Clear—Clears the selected alarm(s).
- Clear—Clears the selected alarm.
- Acknowledge—Acknowledges the alarm to prevent it from showing up in the Alarm Summary page.

Note The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.

- Unacknowledge—Unacknowledges an already acknowledged alarm.
- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.
- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue ad hoc. See Detecting Access Points on a Network for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue ad hoc location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue ad hoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue ad hoc.
- Set State to ‘Alert’—Choose this command to tag the rogue ad hoc as the lowest threat, continue monitoring the rogue access point, and to turn off Containment.
- Set State to ‘Internal’—Choose this command to tag the rogue ad hoc as internal, add it to the Known Rogue APs list, and to turn off Containment.
- Set State to ‘External’—Choose this command to tag the rogue ad hoc as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Targets the rogue ad hoc for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Targets the rogue ad hoc for containment by two Cisco Aironet 1000 Series lightweight access points.
- 3 AP Containment—Targets the rogue ad hoc for containment by three Cisco Aironet 1000 Series lightweight access points.
- 4 AP Containment—Targets the rogue ad hoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

Caution Attempting to contain a rogue AP may lead to legal consequences. When you select any of the AP Containment commands and click **Go**, a message “Containing a Rogue AP may have legal consequences. Do you want to continue?” appears. Click **OK** if you are sure, or click **Cancel** if you do not want to contain any access points.

Monitoring Rogue Ad hoc Details

Alarm event details for each rogue ad hoc are available in the Rogue Adhoc Alarms page.

To view alarm events for a rogue ad hoc radio, in the Rogue Adhoc Alarms page, click an item under Rogue MAC Address.

This page displays alarm events for a rogue access point radio. Rogue access point radios are unauthorized access points detected by Cisco Aironet 1000 Series lightweight access points. The following information is available:

- General:
  - Rogue MAC Address—Media Access Control address of the rogue ad hoc.
  - Vendor—Rogue ad hoc vendor name or Unknown.
  - On Network—Indicates whether or not the rogue ad hoc is located on the network.
  - Owner—Indicates the owner or left blank.
  - Acknowledged—Indicates whether or not the alarm is acknowledged by the user.
  - Classification Type—Malicious, Friendly, or Unclassified.
  - State—Indicates the state of the alarm: Alert, Known, or Removed.
  - SSID—Service Set Identifier being broadcast by the rogue ad hoc radio. (Blank if the SSID is not broadcast.)
  - Channel Number—Indicates the channel of the rogue ad hoc.
  - Containment Level—Indicates the containment level of the rogue ad hoc or Unassigned.
  - Radio Type—Indicates the radio type for this rogue ad hoc.
  - Strongest AP RSSI—Indicates the strongest Received Signal Strength Indicator in dBm.
  - No. of Rogue Clients—Indicates the number of ogue clients associated to this ad hoc.
  - Created—Indicates when the alarm event was created.
  - Modified—Indicates when the alarm event was modified.
  - Generated By—Indicates how the alarm event was generated.
  - Severity—The severity of the alarm: Critical, Major, Minor, Clear, and Color coded.
  - Previous Severity—The previous severity of the alarm: Critical, Major, Minor, Clear, and Color coded.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm.
- Message—Displays descriptive information about the alarm.
- Help—Displays the latest information about the alarm.
- Event History—Click to access the Monitoring Events page.
- Annotations—Lists existing notes for this alarm.

Select a Command

Select one or more alarms by selecting their respective check boxes, choosing one of the following commands, and clicking **Go**.

- Assign to me—Assigns the selected alarm to the current user.
- Unassign—Unassigns the selected alarm.

- Delete—Deletes the selected alarm.
- Clear—Clears the selected alarm.
- Acknowledge—You can acknowledge the alarm to prevent it from showing up in the Alarm Summary page. The alarm remains in the NCS and you can search for all Acknowledged alarms using the alarm search functionality.
- Unacknowledge—You can choose to unacknowledge an already acknowledged alarm.
- Email Notification—Takes you to the All Alarms > Email Notification page to view and configure e-mail notifications.
- Detecting APs—View the Cisco Aironet 1000 Series lightweight access points that are currently detecting the rogue ad hoc. See the "Detecting Access Points on a Network" section on page B-6 for more information.
- Map (High Resolution)—Click to display a high-resolution map of the rogue ad hoc location.
- Rogue Clients—Click to view a list of rogue clients associated with this rogue ad hoc. The Rogue Clients page displays the Client MAC Address, when it was last heard, its current status, its controller, and the rogue ad hoc.
- Set State to 'Alert'—Choose this command to tag the rogue ad hoc as the lowest threat, continue monitoring the rogue ad hoc, and to turn off Containment.
- Set State to 'Internal'—Choose this command to tag the rogue ad hoc as internal, add it to the Known Rogue APs list, and to turn off Containment.
- Set State to 'External'—Choose this command to tag the rogue access point as external, add it to the Known Rogue APs list, and to turn off Containment.
- 1 AP Containment—Targets the rogue ad hoc for containment by one access point. (Lowest containment level.)
- 2 AP Containment—Targets the rogue ad hoc for containment by two Cisco Aironet 1000 Series lightweight access points.
- 3 AP Containment—Targets the rogue ad hoc for containment by three Cisco Aironet 1000 Series lightweight access points.
- 4 AP Containment—Targets the rogue ad hoc for containment by four Cisco Aironet 1000 Series lightweight access points. (Highest containment level.)

Monitoring Events

Click a Rogues alarm square in the Alarm Monitor, click a list item under Rogue MAC Addresses, from the Select a command drop-down list, choose **Event History**, and click **Go** to access this page.

Choose **Monitor > Alarms** and then choose **New Search** from the left sidebar menu. Choose **Severity > All Severities and Alarm Category > Rogue AP**, and click **Go** to access the Monitor Alarms > *failure object* page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list, choose **Event History**, and click **Go** to access this page.

This page enables you to review information about rogue alarm events. Events list the sequence of occurrences for an element(s) over a period of time.

Click the title of each column to reorder the listings:

- Severity—Color-coded display of the severity of the event.
- Rogue MAC Address—Click a list item to display information about the entry.

- Vendor—Name of rogue access point manufacturer.
- Type—AP or AD-HOC.
- On Network—Whether or not the rogue access point is on the same subnet as the associated port.
- On 802.11a—Whether or not the rogue access point is broadcasting on the 802.11a band.
- On 802.11b—Whether or not the rogue access point is broadcasting on the 802.11b/802.11g band.
- Date/Time—Date and time of the alarm.
- Classification Type—Malicious, Friendly, or Unclassified.
- State—State of the alarm, such as Alert and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio.

Monitoring Rogue Clients

Choose **Monitor > Alarms** and then choose **New Search** from the left sidebar menu. Choose **Severity > All Severities and Alarm Category > Rogue AP**, and click **Go** to access the Monitor Alarms > *failure object* page. Click an item under the Rogue MAC Address to display the Monitor Alarms > Rogue AP Details page. From the Select a command drop-down list, choose **Rogue Clients** to access this page.

This page enables you to view information about clients that have associated with the rogue access point.

- Client MAC Address—Media Access Control address of the rogue access point client.
- Last Heard—The last time a Cisco access point detected the rogue access point client.
- Status—Status of the rogue access point client.

Configuring Controllers

This section contains the following topics:

Configuring Rogue Policies

This page enables you to set up policies for rogue access points.

To access the Rogue Policies page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Rogue Policies**.

- Rogue Location Discovery Protocol—Enabled, Disabled.
- Rogue APs
  - Expiration Timeout for Rogue AP Entries (seconds)—1 - 3600 seconds (1200 default).
- Rogue Clients
  - Validate rogue clients against AAA (check box)—Enabled, Disabled.

  - Detect and report ad hoc networks (check box)—Enabled, Disabled command buttons.
- Save—Saves the changes made to the client exclusion policies and returns to the previous page.
- Audit—Compares the NCS values with those used on the controller.

Configuring Rogue AP Rules

This page enables you to view and edit current rogue AP rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > Rogue AP Rules**. The Rogue AP Rules page displays the rogue AP rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Select a rogue AP rule to view or edit its details. See the "Configuring Rogue AP Rules" section on page B-13 for more information.

Configuring Controller Templates

This section contains the following topics:

Configuring Rogue Policies

This page enables you to configure the rogue policy template (for access points and clients) applied to the controller.

To view current templates and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue Policies**.

To create a new rogue policy template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue Policies**.

Step 3 From the Select a command drop-down list, choose **Add Template**.

Step 4 Click **Go**.

Note To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue Policies**, and click a template name in the Template Name column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Select the **Rogue Location Discovery Protocol** check box to enable it. Rogue Location Discovery Protocol (RLDP) determines whether or not the rogue is connected to the enterprise wired network.

Note With RLDP, the controller instructs a managed access point to associate with the rogue access point and send a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

Step 6 Set the expiration timeout (in seconds) for rogue access point entries.

Step 7 Select the **Validate rogue clients against AAA** check box to enable the AAA validation of rogue clients.

Step 8 Select the **Detect and report Adhoc networks** check box to enable detection and reporting of rogue clients participating in ad hoc networking.

Step 9 Click any of these buttons:

- ***Save***—Click to save the current template.
- **Apply to Controllers**—Click to apply the current template to controllers. In the Apply to Controllers page, select the applicable controllers, and click **OK**.
- **Delete**—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- **Cancel**—Click to cancel the current template creation or changes to the current template.

Configuring Rogue AP Rules

Rogue AP rules allow you to define rules to automatically classify rogue access points. The NCS applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps, based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Note Rogue AP rules also help reduce false alarms.

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configure > Controller Templates > Security > Rogue AP Rules**.

Note Rogue classes include the following types:
Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.

Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.
Unclassified Rogue—A detected access point that does not match the Malicious or Friendly rules.

To create a new classification rule template for rogue access points, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue AP Rules**.

Step 3 From the Select a command drop-down list, choose **Add Classification Rule**.

Step 4 Click **Go**.

Note To make modifications to an existing Rogue AP Rules template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rules** and click a template name in the Template Name column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Complete the following fields:

- General:
  - Rule Name—Enter a name for the rule in the text box.
  - Rule Type—Choose **Malicious** or **Friendly** from the drop-down list.

Note Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category.
Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

  - Match Type—Choose **Match All Conditions** or **Match Any Condition** from the drop-down list.
- Malicious Rogue Classification Rule
  - Open Authentication—Select the check box to enable Open Authentication.
  - Match Managed AP SSID—Select the check box to enable thematching of managed AP SSID rule condition.

Note Managed SSID are the SSIDs configured for the WLAN and is known to the system.

  - Match User Configured SSID—Select the check box to enable the matching of user configured SSID rule condition.

Note User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

  - Minimum RSSI—Select the check box to enable the Minimum RSSI threshold limit.

Note Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

- Time Duration—Select the check box to enable the Time Duration limit.

Note Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

- Minimum Number Rogue Clients—Select the check box to enable the Minimum Number Rogue Clients limit.

Note Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

Step 6 Click any of the following buttons:

- **Save**—Click to save the current template.
- **Apply to Controllers**—Click to apply the current template to controllers. In the Apply to Controllers page, select the applicable controllers and click **OK**.
- **Delete**—Click to delete the current template. If the template is currently applied to controllers, click **OK** to confirm that you want to remove the template from the selected controllers to which it is applied.
- **Cancel**—Click to cancel the current template creation or changes to the current template.

Configuring Rogue AP Rule Groups

The Rogue AP Rule Group template allows you to combine more than one rogue AP rule to apply to controllers.

To view current Rogue AP Rule Group templates, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups**.

To create a new Rogue AP Rule Groups template, follow these steps:

Step 1 Choose **Configure > Controller Templates**.

Step 2 From the left sidebar menu, choose **Security > Rogue AP Rule Groups**.

Step 3 From the Select a command drop-down list, choose **Add Rogue Rule Group**.

Step 4 Click **Go**.

Note To make modifications to an existing rogue policy template or to apply a current template to controllers, choose **Configure > Controller Templates > Security > Rogue AP Rule Groups** and click a template name in the Template Name column. Make the necessary changes to the template and click **Save** or **Apply to Controllers**.

Step 5 Enter the following parameters:

- General
  - Rule Group Name—Enter a name for the rule group in the text box.

Step 6 To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.

Note Rogue AP rules can be added from the Rogue AP Rules group box. See the "Configuring Rogue AP Rules" section on page B-13 for more information.

Step 7 To remove a Rogue AP rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.

Step 8 Use the Move Up/Move Down buttons to specify the order in which the rules apply. Highlight the desired rule, and click **Move Up** or **Move Down** to move it higher or lower in the current list.

Step 9 Click **Save** to confirm the Rogue AP rule list.

Step 10 Click **Cancel** to close the page without making any changes to the current list.

Note To view and edit the rules applied to a controller, choose **Configure > Controller**, and click the controller name to open the controller.