CHAPTER 3

Configuring Security Solutions

This chapter describes the security solutions for wireless LANs. It contains the following sections:

Cisco Unified Wireless Network Solution Security

The Cisco Unified Wireless Network Solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 access point security components into a simple policy manager that customizes system-wide security policies on a per wireless LAN basis. It provides simple, unified, and systematic security management tools.

One of the challenges to wireless LAN deployment in the enterprise is wired equivalent privacy (WEP) encryption, which is a weak standalone encryption method. A more recent problem is the availability of low-cost access points that can be connected to the enterprise network and used to mount man-in-the-middle and denial of service attacks. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in wireless LAN security.

This section contains the following topics:

Layer 1 Solutions

The Cisco Unified Wireless Network Solution operating system security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the operator-set timer expires. The operating system can also disable SSID broadcasts on a per wireless LAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, the network administrator can also implement industry-standard security solutions such as 802.1X dynamic keys with Extensible Authentication Protocol (EAP) or Wi-Fi Protected Access (WPA) dynamic keys. The Cisco Unified Wireless Network Solution WPA implementation includes Advanced Encryption Standard (AES), Temporal Key Integrity Protocol + message integrity code checksum (TKIP + Michael MIC) dynamic keys, or static WEP keys. Disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between controllers and access points are secured by passing data through Lightweight Access Point Protocol (LWAPP) tunnels.

Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions such as Virtual Private Networks (VPNs).

The Cisco Unified Wireless Network Solution supports local and RADIUS media access control (MAC) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses. The Cisco Unified Wireless Network Solution also supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Single Point of Configuration Policy Manager Solutions

When the Cisco Unified Wireless Network Solution is equipped with Cisco NCS, you can configure system-wide security policies on a per wireless LAN basis. small office, home office (SOHO) access points force you to individually configure security policies on each access point or use a third-party appliance to configure security policies across multiple access points. Because the Cisco Unified Wireless Network Solution security policies can be applied across the whole system from NCS, errors can be eliminated, and the overall effort is greatly reduced.

Rogue Access Point Solutions

This section describes security solutions for rogue access points and includes the following topics:

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 "Tagging and Containing Rogue Access Points" section on page 3-3 section.

Tagging and Containing Rogue Access Points

When the Cisco Unified Wireless Network Solution is monitored using NCS, 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).

Securing Your Network Against Rogue Access Points

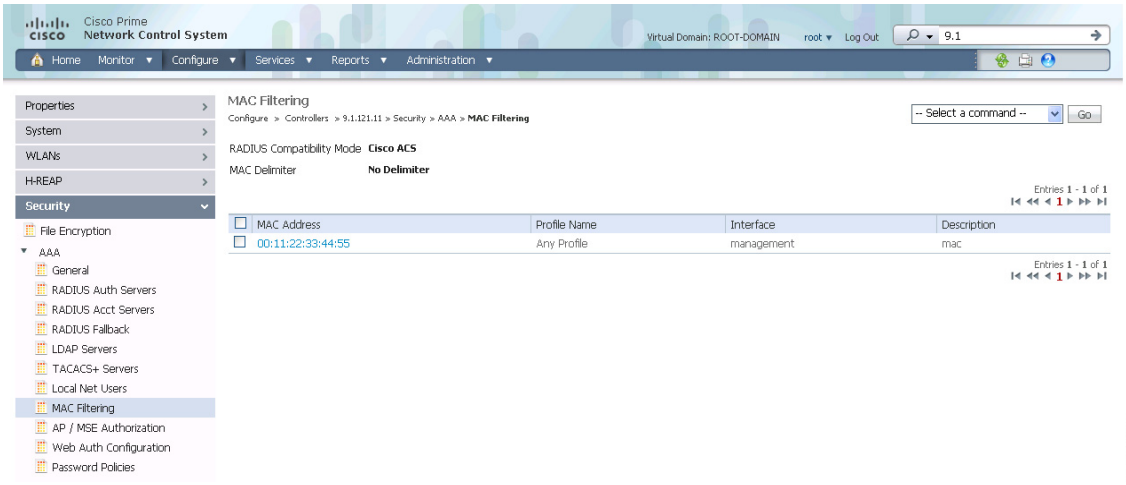
You can secure your network against any rogue access points and disallow access point attacks for those access points not defined in the MAC filter list. To set up MAC filtering, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Click the IP address for which you want to enter MAC filters.

Step 3 Choose **Security > AAA> MAC Filtering** from the left sidebar menu. The MAC Filtering page appears (see Figure 3-1).

Figure 3-1 MAC Filtering Page



The RADIUS compatibility mode, MAC delimiter, MAC address, profile name, interface, and description appears.

Step 4 If you want to set the same configuration across multiple devices, you can choose **Add MAC Filter** from the Select a command drop-down list, and click **Go**. If a template exists, you can apply it. If you need to create a template, you can click the URL to get redirected to the template creation page.

Note The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.

Step 5 To make changes to the profile name, interface, or description, click a specific MAC address in the MAC Address column.

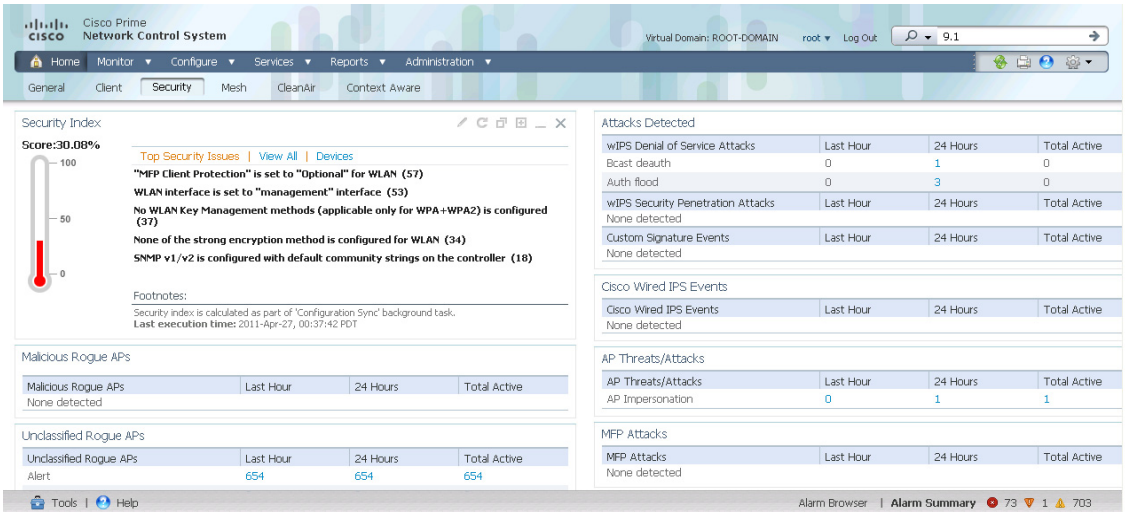
Interpreting the Security Dashboard

Because unauthorized rogue access points are inexpensive and readily available, employees sometimes plug them into existing LANs and build ad hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security because they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having the enterprise security breached.

Rather than having a person with a scanner manually detect rogue access points, the Cisco Unified Wireless Network Solution automatically collects information on rogue access points detected by its managed access points (by MAC and IP address) and allows the system operator to locate, tag, and contain them. It can also be used to discourage rogue access point clients by sending them deauthenticate and disassociate messages from one to four access points.

For a summary of existing events and the security state of the network, click the **Security** dashboard from the NCS home page. Figure 3-2 shows the security dashboard and different dashlets.

Figure 3-2 Security Dashboard



This section describes the Security dashboard, dashlets and contains the following topics:

- Security Index, page 3-5
- Malicious Rogue Access Points, page 3-6
- Adhoc Rogues, page 3-6
- CleanAir Security, page 3-7
- Unclassified Rogue Access Points, page 3-7
- Friendly Rogue Access Points, page 3-8
- Access Point Threats or Attacks, page 3-8
- MFP Attacks, page 3-9
- Attacks Detected, page 3-9

You can customize the order of information you want in the Security dashboard to display. You can move the dashlets to change the order. Use the Edit Dashelt option to customize the information displayed in the dashlet. You can change the dashlet title, enable refresh, and set the refresh time interval using the Edit Dashlet options.

Security Index

The Security Index dashlet indicates the security of the NCS managed network, and it is calculated as part of daily background tasks. It is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weighting can vary from 0 to 100 where 0 signifies the least secured and 100 is the maximum secured. The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within NCS itself. The Security Index of the NCS managed network is equal to the lowest scoring controller plus the lowest scoring Location Service/Mobility Service Engine.

The security thermometer color range is represented as follows:

- Above or equal to 80 - Green
- Below 80 but greater than or equal to 60 - Yellow
- Below 60 - Red

Note Guest WLANs are excluded from the WLANs. A WLAN that has web authentication or web passthrough enabled is identified as a guest WLAN.

The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.

Note The configurations stored in NCS may not be the latest with the ones in the controllers unless the Refresh from Controller command is run from NCS. You can run Security Index calculations from the Configuration Sync task to get the latest configuration data from all the controllers. See the "Performing a Configuration Sync" section on page 15-22 for steps on enabling the security index.

Malicious Rogue Access Points

This dashlet provides information on rogue access points that are classified as *Malicious*. Table 3-1 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note Malicious access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

Table 3-1 Malicious Rogue AP Details

Parameter	Description
Alert	Indicates the number of rogues in an alert state. **Note** An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending. **Note** Contained Pending indicates that the containment action is delayed due to unavailable resources.

Adhoc Rogues

The Adhoc Rogues dashlet displays the rogues that have occurred in the last hour, last 24 hours, and the total active. Table 3-2 describes the various parameters. If you click the number in any of these columns, a page with further information appears.

Note The Adhoc Rogue state displays as *Alert* when first scanned by the controller or as *Pending* when operating system identification is underway.

Table 3-2 Ad hoc Rogues

Parameter	Description
Alert	Indicates the number of ad hoc rogues in an alert state. **Note** An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Contained	Indicates the number of contained rogues.
Threat	Indicates the number of threat rogues.
Contained Pending	Indicates the number of contained rogues pending. **Note** Contained pending indicates that the containment action is delayed due to unavailable resources.

CleanAir Security

This dashlet provides information on CleanAir security and provides information about the security-risk devices active during the last hour, 24 hours, and Total Active security-risk devices on the wireless network.

The following information is displayed:

- Severity
- Failure Source
- Owner
- Date/Time
- Message
- Acknowledged

To learn more about the security-risk interferers, see the "Monitoring CleanAir Security Alarms" section on page 5-137.

Unclassified Rogue Access Points

Table 3-3 describes the unclassified rogue access point parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

Table 3-3 Unclassified Rogue Access Points

Parameter	Description
Alert	Number of unclassified rogues in alert state. Rogue access point radios appear as *Alert* when first scanned by the controller or as *Pending* when operating system identification is underway.
Contained	Number of contained unclassified rogues.
Contained Pending	Number of contained unclassified rogues pending.

Friendly Rogue Access Points

This dashlet provides information on rogue access points that are classified as *friendly*. Table 3-4 describes the various parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Note Friendly rogue access points are known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Table 3-4 Friendly Rogue AP Details

Parameter	Description
Alert	Indicates the number of rogues in an alert state. **Note** An access point is moved to Alert if it is not on the neighbor list or part of the user-configured Friendly AP list.
Internal	Indicates the number of internal access points. **Note** Internal indicates that the detected access point is inside the network and has been manually configured as Friendly - Internal.
External	Indicates the number of external access points. **Note** External indicates that the detected access point is outside of the network and has been manually configured as Friendly - External.

Access Point Threats or Attacks

Table 3-5 describes the AP Threats or Attacks parameters. For each of these parameters, a value is provided for last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Table 3-5 AP Threats/Attacks

Parameter	Description
Fake Attacks	Number of fake attacks
AP Missing	Number of missing access points
AP Impersonation	Number of access point impersonations
AP Invalid SSID	Number of invalid access point SSIDs
AP Invalid Preamble	Number of invalid access point preambles
AP Invalid Encryption	Number of invalid access point encryption
AP Invalid Radio Policy	Number of invalid access point radio policies
Denial of Service (NAV related)	Number of Denial of Service (NAV related) request
AP Detected Duplicate IP	Number of detected duplicate access point IPs

MFP Attacks

A value is provided for Infrastructure and client MFP attacks in the last hour, last 24 hours, and total active. If you click an underlined number in any of the time period categories, a page with further information appears.

Attacks Detected

A value is provided for wIPS Denial of Service and wIPS Security Penetration attacks and custom signature attacks for the past hour, past 24 hours, and total active. If you click an underline number in any of the time period categories, a page with further information appears.

Recent Rogue AP Alarms

A value is provided for the five most recent rogue alarms. Click the number in parentheses to access the Alarms page. Then click an item under MAC address to view alarm details.

Recent Adhoc Rogue Alarm

Displays the five most recent ad hoc rogue alarms. Click the number in parentheses to access the Alarms page. Click an item under MAC address to view ad hoc details.

Most Recent Security Alarms

Displays the five most recent security alarms. Click the number in parentheses to access the Alarms page.

Rogue Access Points, Ad hoc Events, and Clients

This section describes security solutions for rogue devices. A rogue device is an unknown access point or client that is detected by managed access points in your network.

Controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network.

Note NCS consolidates all of the controllers' rogue access point data.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

This section contains the following topics:

- Classifying Rogue Access Points, page 3-10
- Rogue Access Point Classification Types, page 3-11
- Adhoc Rogue, page 3-13

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

Note NCS consolidates all of the controllers' rogue access point data.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only.

Note Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

Note The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies that the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.

2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state. Table 3-6 shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 3-6 Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Rogue Access Point Classification Types

Rogue access points classification types include:

- Malicious—Detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification. See the "Malicious Rogue Access Points" section on page 3-6 for more information.

- Friendly—Known, acknowledged, or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained. See the "Friendly Rogue APs" section on page 3-12 for more information. For more information on configuring friendly access point rules, see the "Configuring a Friendly Access Point Template" section on page 11-82.
- Unclassified—Rogue access point that are not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list. See the "Unclassified Rogue APs" section on page 3-13 for more information.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of the NCS home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points. See the "Monitoring Rogue Access Points" section on page 5-86 for more information.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

The Security dashboard of the NCS home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points. See the "Monitoring Rogue Access Points" section on page 5-86 for more information.

Unclassified Rogue APs

An unclassified rogue access point refers to a rogue access point that is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the NCS home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information. See the "Monitoring Rogue Access Points" section on page 5-86.

Adhoc Rogue

If the MAC address of a mobile client operating in a adhoc network is not in the authorized MAC address list, then it is identified as an adhoc rogue.

Rogue Access Point Location, Tagging, and Containment

When the Cisco Unified Wireless Network Solution is monitored using NCS, 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 the 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.

This section contains the following topics:

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 details 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 2-33 for more information about the search feature.
- In the NCS home page, click the **Security** dashboard. This page 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 dashlet.

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

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

Step 4 Click **Go**.

Click a list item to display data about that item:

- AP Name
- Radio
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- 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.

Viewing Rogue Access Points by Controller

Use the Detecting Access Points feature to view information about the rogue access points by controller.

To access the Rogue AP Alarms details 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 2-33 for more information about the search feature.
- In the NCS home page, click the **Security** dashboard. This page 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 dashlet.

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

Step 3 From the Select a command drop-down list, choose **View AP Details by Controller**.

Step 4 Click **Go**.

Click a list item to display data about that item:

- Controller IP Address
- Detecting AP Name
- Radio
- Detecting AP Location
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- RSSI—Received signal strength indicator in dBm.
- Classification—Indicates if the rogue AP classification.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Rogue Access Point Classification Types" section on page 3-11 for additional information.
- On Network—Whether it belongs to this network "Yes" or "No".
- Containment Level—Indicates the containment level of the rogue access point or Unassigned (not contained).

- Last Updated Time

Working with Alarms

You can view, assign, and clear alarms and events on access points and mobility services engine using Cisco NCS.

Details on how to have email notifications of alarms sent to you is also described. This section contains the following topics:

Assigning and Unassigning Alarms

To assign and unassign an alarm to yourself, follow these steps:

Step 1 Perform an advanced search for access point alarms. See the "Using the Search Feature" section on page 2-33 for more information.

Step 2 Select the alarms that you want to assign to yourself by selecting their corresponding check boxes.

Note To unassign an alarm assigned to you, unselect the box next to the appropriate alarm. You cannot unassign alarms assigned to others.

Step 3 From the Select a command drop-down list, choose **Assign to Me** (or **Unassign**), and click **Go**.

If you choose **Assign to Me**, your username appears in the Owner column. If you choose **Unassign**, the username column becomes empty.

Deleting and Clearing Alarms

To delete or clear an alarm from a mobility services engine, follow these steps:

Step 1 In the Monitor > Alarms page, select the alarms that you want to delete or clear by selecting their corresponding check boxes.

Note If you delete an alarm, Cisco NCS removes it from its database. If you clear an alarm, it remains in the Cisco NCS database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

Step 2 From the Select a command drop-down list, choose **Delete** or **Clear**, and click **Go**.

Note To set up cleanup of old alarms and cleared alarms, choose **Administration > Settings > Alarms**.

Acknowledging Alarms

You may want certain alarms to be removed from the Alarms List. For example, if you are continuously receiving an interference alarm from a certain access point on the 802.11g interface, you may want to stop that access point from being counted as an active alarm on the page or any alarms list. In this scenario, you can find the alarm for the 802.11g interface in the Alarms list, select the check box, and choose **Acknowledge** from the Select a command drop-down list.

Now if the access point generates a new violation on the same interface, NCS will not create a new alarm, and the page shows no new alarms. However, if the interference violation is created on another interface, such as 802.11a, a new alarm is created.

Any alarms, once acknowledged, will not show up on either the page or any alarm list page. Also, no emails are generated for these alarms after you have marked them as acknowledged. By default, acknowledged alarms are not included for any search criteria. To change this default, choose **Administration > Settings > Alarms** page and disable the Hide Acknowledged Alarms preference.

Note When you acknowledge an alarm, a warning displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Use the Administration > User Preferences page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. NCS automatically deletes cleared alerts that are more than seven days old so your results can only show activity for the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which NCS has already generated an alarm.

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. NCS generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for rogue access point events using the Advanced Search feature of NCS. See the "Using the Search Feature" section on page 2-33 for more information.
- In the Rogue AP Alarms details page, choose **Event History** from the Select a command drop-down list.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the "Viewing Rogue AP Event Details" section on page 3-18 for more information.
- Vendor—Rogue access point vendor name or Unknown.

- Classification Type—Malicious, Friendly, or Unclassified. See the "Rogue Access Point Classification Types" section on page 3-11 for more information.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Rogue Access Point Classification Types" section on page 3-11 for additional information.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Rogue AP Event Details

To view rogue access point event details, follow these steps:

Step 1 In the Rogue AP Events list page, click the **Rogue MAC Address** link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Classification Type—Malicious, Friendly, or Unclassified. See the "Rogue Access Point Classification Types" section on page 3-11 for more information.
- State—Indicates the state of the alarm. Possible states vary depending on the classification type of rogue access point. See the "Rogue Access Point Classification Types" section on page 3-11 for additional information.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—The method by which the event was generated (such as Controller).
- Device IP Address
- Severity—Indicates the severity of the alarm.

- Message—Provides details of the current event.

Monitoring Adhoc Rogue Events

The Events page enables you to review information about adhoc rogue events. NCS generates an event when an adhoc rogue is detected or if you make manual changes to an adhoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all adhoc rogue events.

To access the Rogue AP Events list page, follow these steps:

Step 1 Do one of the following:

- Perform a search for adhoc rogues events using the Advanced Search feature of NCS. See the "Using the Search Feature" section on page 2-33 for more information.
- In the Adhoc Rogue Alarms details page, choose **Event History** from the Select a command drop-down list.

Step 2 The Rogue AP Events list page displays the following event information.

- Severity—Indicates the severity of the alarm.
- Rogue MAC Address—Click the rogue MAC address to view the Rogue AP Event Details page. See the "Viewing Adhoc Rogue Event Details" section on page 3-19 for more information.
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Date/Time—The date and time that the event was generated.
- State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

Viewing Adhoc Rogue Event Details

To view rogue access point event details, follow these steps:

Step 1 In the Rogue AP Events list page, click the **Rogue MAC Address** link.

Step 2 The Rogue AP Events Details page displays the following information:

- Rogue MAC Address
- Vendor—Rogue access point vendor name or Unknown.
- On Network—Indicates how the rogue detection occurred.

  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- State—Indicates the state of the alarm. Possible states for adhoc rogues include Threat, Alert, Internal, External, Contained, Contained Pending, and Removed.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Channel Number—The channel on which the rogue access point is broadcasting.
- Containment Level—Indicates the containment level of the rogue access point or Unassigned.
- Radio Type—Lists all radio types applicable to this rogue access point.
- Created—The date and time that the event was generated.
- Generated By—The method by which the event was generated (such as Controller).
- Device IP Address
- Severity—Indicates the severity of the alarm.
- Message—Provides details of the current event.

Security Overview

NCS provides a foundation that allows IT managers to design, control, secure, and monitor enterprise wireless networks from a centralized location.

NCS provides the following tools for managing and enforcing wireless security configurations and policies within the Cisco wireless network infrastructure:

- Network security policy creation and enforcement, such as user authentication, encryption, and access control
- Wireless infrastructure security configuration
- Rogue detection, location, and containment
- Wireless intrusion prevention system (wIPS)
- Wireless IPS signature tuning and management
- Management Frame Protection (MFP)
- Collaboration with Cisco wired Network IPS for monitoring and mitigating unauthorized or malicious wireless user activity
- Comprehensive security event management and reporting

Security Vulnerability Assessment

In Cisco Unified Wireless Network Version 5.1, an automated security vulnerability assessment is available to facilitate analysis of an enterprise's overall wireless security posture, as well as to provide WLAN operators with real-time benchmarking of their security services configurations against industry best practices. The automated security vulnerability assessment provides:

- Proactive vulnerability monitoring of the entire wireless network

- Comprehensive information on security vulnerabilities that could lead to loss of data, network intrusion, or malicious attack
- Reduction in the time and expertise required to analyze and remedy weaknesses in wireless security posture

The automated wireless vulnerability assessment audits the security posture of the entire wireless network for vulnerabilities. These vulnerabilities can result in:

- Unauthorized management access or using management protocols to compromise or adversely impact the network
- Unauthorized network access, data leakage, man-in-the-middle, or replay attacks
- Compromised or adverse impacts to the network through manipulation of network protocols and services, for example through denial of service (DoS) attacks

The Cisco NCS automatically scans the entire network and compares settings against Cisco recommended and industry best practices for wireless security configurations. The automated wireless security assessment functions within NCS scan wireless LAN controllers, access points, and network management interfaces for vulnerabilities in configuration settings, encryption, user authentication, infrastructure authentication network management, and access control.

Status of the wireless network security is graphically displayed to provide wireless network administrators with an easy-to-read dashboard of security events. The NCS displays the vulnerability assessment results through a Security Index on the NCS security dashboard. The Security Index summarizes the network security posture with a composite security score and prioritized summary of vulnerabilities. See the "Security Index" section on page 3-21" for more information.

Administrators can drill down to the Security Index Detailed Report if an event in the Security Summary warrants further investigation. The Security Index Detailed Report provides in-depth analysis of the vulnerabilities across the network. It also identifies optimal security settings and recommends changes that will remedy the vulnerabilities. Any changes the administrator makes are reflected in an updated Security Index score. See the "Security Index Detailed Report" section on page 3-22" for more information.

Security Index

The Security Index gives an indication of the security of the NCS managed network. The security index is calculated by assigning weight to the various security configurations and displaying it in visual form. The combined weightages can vary from 0 to 100, where 0 signifies least secured and 100 maximum secured.

The weighting comes from the lowest scoring controller and the lowest scoring Location Server/Mobility Service Engine related security configurations that are maintained within NCS itself. For example, the security index of the NCS managed network is equal to the lowest scoring controller plus the lowest scoring Location Server/Mobility Service Engine.

The following color scheme applies for the security index:

- Above or equal to 80—Green
- Below 80 but above or equal to 60—Yellow
- Below 60—Red

Note Guest WLANs are excluded from the WLANs. A WLAN which has web authentication or web passthrough enabled is identified as a guest WLAN.

The security index of the latest release is the benchmark for the required security configurations. For example, if AES encryption was not present in an earlier version of code, the index is reduced by the number associated with the AES encryption security configuration. Likewise, if new security configurations are introduced, the weighting would be altered.

The configurations stored in NCS may not be up-to-date with the ones in the controllers unless the Refresh from Controller command is run from NCS. You can run Security Index calculations from the Configuration Sync task to get the latest config data from all the controllers.

Top Security Issues

The Top Security Issues section displays the five top security issues. The View All and Devices links sort relevant columns and show a report of security issues occurring across all controllers. Click **View All** to open the Security Index Detailed Report. Click **Devices** to view the Security Index Controller Report.

- Security Index Detailed Report, page 3-22
- Security Index Controller Report, page 3-22
- Potential Security Issues, page 3-23

Security Index Detailed Report

The Security Index Detailed Report displays all security issues found across all controllers, location servers, and mobility service engines. It details problems found in a particular security configuration retrieved from the device. If a particular issue has been acknowledged (just like alarms), it is ignored when the next Configuration Sync task runs (if Security Index Calculation is enabled).

In some cases when an issue is acknowledged and it is ignored the next time the Configuration Sync task runs, the final security index score does not change. Some possible reasons for this may include:

- The acknowledged issue is on a controller which is not directly affecting the security index score (for instance, it is not the controller with the lowest score).
- The acknowledged issue is on a WLAN that is not directly affecting the security index score. Only the lowest scoring WLAN of the lowest scoring controller affects the security index score.

When SSH and Telnet are enabled on a controller and are both flagged as issues, the Telnet issue has a higher precedence than SSH. Even if SSH is acknowledged on the controller with the lowest score, no change would occur for the security index.

From the Select a command drop-down list, choose **Show All** to view all security issues (both acknowledged and unacknowledged). Choose **Show Unacknowledged** to only view unacknowledged security issues. This is the default view when View All is selected from the Security Summary page. Choose **Show Acknowledged** to only view acknowledged security issues.

Note In order for an user to Acknowledge or Unacknowledge security issues, the user has to have “Ack and Unack Security Index Issues permission enabled".

Security Index Controller Report

This page shows the security violation report as a summary for each controller. By row, each controller shows the number of security issues that occurred on that controller and provides a link to all security issues.

If you click the number in the Security Issues Count column, the Security Index Detailed Report appears.

Potential Security Issues

Table 3-7 and Table 3-8 describe the potential security issues.

Table 3-7 Potential Security Issues

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has a weak authentication method.	Weak authentication method for a WLAN which can be broken by using tools available online if WLAN packets are sniffed.	Use the most secured authentication method and one that is WPA+WPA2.
WLAN SSID on the controller has a weak authentication method (CKIP) configured.	Weak authentication method for a WLAN.	Use the most secured authentication method and one that is WPA+WPA2.
WLAN SSID on the controller has no user authentication configured.	No authentication method is a clear security risk for a WLAN.	Configure strong authentication methods such as WPA+WPA2.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with MMH) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 40 bits with MMH and Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has a weak encryption method (CKIP WEP 104 bits with MMH and Key Permutation) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 40 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 128 bits) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (TKIP) configured.	Weak encryption method for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has no encryption configured.	No encryption method is a clear security risk for a WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has a weak encryption method (WEP 104 bits) configured.	Weak encryption method for WLAN.	Configure strong authentication and encryption methods such as WPA+WPA2 with AES.
WLAN SSID on the controller has no key management methods configured (applicable only for WPA+WPA2).	A key management method enhances the security of keys; without one, WLAN is less secure.	Configure at least one key management methods such as CCKM.
WLAN SSID on the controller has MFP Client Protection set to “Optional”.	With MFP Client Protection set to optional for a WLAN, authenticated clients may not be shielded from spoofed frames.	Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.
WLAN SSID on the controller has MFP Client Protection set to “Disabled”.	With MFP Client Protection set to disabled for a WLAN, authenticated clients may not be shielded from spoofed frames.	Set MFP Client Protection to “Required” to protect against clients connecting to a rogue access point.
WLAN SSID interface is set to “management” on the controller.	As recommended from SAFE, user traffic should be separated from management traffic.	WLAN interface should not be set to “management” on the controller.
Interface set to one which is VLAN for a WLAN.	As recommended from SAFE, user traffic should be separated from VLAN traffic.	WLAN needs its interface to be set to one which is neither management nor one which has a VLAN.
WLAN SSID on the controller has “Client Exclusion” disabled.	With Client Exclusion policies disabled, an attacker is able to continuously try to access the WLAN network.	Enable “Client Exclusion” to secure against malicious WLAN client behavior.
WLAN SSID on the controller has “Broadcast SSID” enabled.		Disable “Broadcast SSID” to secure your wireless network.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
WLAN SSID on the controller has "MAC Filtering" disabled.		Enable "MAC Filtering" to secure your wireless network.
Protection Type is set to "AP Authentication" on the controller.	When AP Authentication is set, an access point checks beacon/probe response frames in neighboring access points to see if they contain an authenticated information element (IE) that matches that of the RF group. This provides some security but does not cover all management frames and is open to alteration by rogue access points.	Set Protection Type to "Management Frame Protection (MFP)" on the controller.
Protection Type is set to "None" of the controller.	No security for 802.11 management messages passed between access points and clients.	Set Protection Type to "Management Frame Protection (MFP)" on the controller.
Radio type is configured to detect rogues only on DCA channels.	Rogue detection, if done only on a subset of country/all channels, is less secure than one that is done on country/all channels.	Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.
Radio type is configured to detect rogues on neither country channels nor DCA channels.	Rogue detection, if not configured on country nor DCA channels, is less secure than when done on country/all channels.	Configure radio types 802.11a/n and 802.11b/g/n to detect rogues on country channels or all channels.
The rogue policy to detect and report adhoc networks is disabled on the controller.	With detection and reporting of adhoc networks turned off, adhoc rogues go undetected.	Enable the rogue policy to detect and report adhoc networks
"Check for all Standard and Custom Signatures" is disabled on the controller.	If check for all Standard and Custom Signatures is disabled, various types of attacks in incoming 802.11 packets would go undetected. various types of attacks in incoming 802.11 packets would go undetected.	Check for all Standard and Custom Signatures needs to be turned on to identify various types of attacks in incoming 802.11 packets.
Some of the Standard Signatures are disabled on the controller.	If only some of the Standard Signatures are disabled,	Enable all Standard Signatures on the controller.
The "Excessive 802.11 Association Failures" Client Exclusion Policy is disabled on the controller.	Excessive failed association attempts can consume system resources and launch potential a denial of service attack to the infrastructure.	Enable the "Excessive 802.11 Association Failures" Client Exclusion Policy on the controller.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
The "Excessive 802.11 Authentication Failures" Client Exclusion Policy is disabled on the controller.	Excessive failed authentication attempts can consume system resources and launch potential Denial of Service attack to the infrastructure.	Enable the "Excessive 802.11 Authentication Failures" Client Exclusion Policy on the controller.
The "Excessive 802.1X Authentication Failures" Client Exclusion Policy is disabled on the controller.	Excessive 802.1X failed authentication attempts can consume system resources and launch potential denial of service attack to the infrastructure.	Excessive 802.1X Authentication Failures Client Exclusion Policy must be enabled to prevent denial of service attack to the infrastructure.
The "Excessive 802.11 Web Authentication Failures" Client Exclusion Policy is disabled on the controller.	If Excessive 802.11 Web failed web authentication attempts can consume system resources and launch potential Denial of Service attack to the infrastructure.	Enable the "Excessive 802.11 Web Authentication Failures" Client Exclusion Policy on the controller.
The "IP Theft or IP Reuse" Client Exclusion Policy is disabled on the controller.	If IP Theft or Reuse Client Exclusion Policy is disabled, then an attacker masquerading as another client would not be disallowed.	Enable the "IP Theft or IP Reuse" Client Exclusion Policy on the controller.
No CIDS Sensor configured on the controller.	If no enabled IDS Sensor is configured, then IP-level attacks would not be detected.	Configure at least one CIDS Sensor on the controller.
Controller is configured with default community strings for SNMP v1/v2.	If SNMP V1 or V2 with default Community is configured then it is open to easy attacks since default communities are well known.	Use SNMPv3 with Auth and Privacy Types.
Controller is configured with non-default community strings for SNMP v1/v2.	SNMP V1 or V2 with non-default Community is slightly more secure than default Community but still less secure than SNMP V3.	Use SNMPv3 with Auth and Privacy types.
SNMPv3 is configured with a default user on the controller.	Using a default user makes SNMP V3 connections less secure.	Use a non-default username for SNMPv3 with Auth and Privacy Types.
SNMPv3 is configured with either no Auth or Privacy Type on the controller.	SNMP V3 with either Auth or Privacy Type set to none reduces the security of SNMP V3 connection.	Use SNMPv3 with Auth and Privacy Types to secure your wireless network.
HTTP (Web Mode enabled but Secure Web Mode disabled) is enabled on the controller.	HTTP is less secure than HTTPS.	Enable HTTPS (both Web Mode and Secure Web Mode) on the controller.

Table 3-7 Potential Security Issues (continued)

Controller Security Issue	Why is this an Issue?	What is the Solution?
Telnet is enabled on the controller.	If telnet is enabled, then the controller is at risk of being hacked into.	Disable telnet on the controller.
SSH is disabled and timeout value is set to zero on the controller.	If SSH is enabled and timeout is zero then the controller has risk of being hacked into.	Enable SSH with non-zero timeout value on the controller.
Telnet is enabled on the AP.	If telnet is enabled, then the access point is at risk of being hacked into.	Disable Telnet on all access points.
SSH is enabled on the AP.		Disable SSH on all the access points.
At least one of the APs is configured with default username or password.	If default password is configured, then access points are more susceptible to connections from outside the network.	Configure a non-default username and strong password for all access points associated to the controller.

Table 3-8 Potential Security Issues

Location Server/ Mobility Server Engine Security Issue	Why is this an Issue?	What is the Solution?
HTTP is enabled on the location server.	HTTP is less secure than HTTPS.	Enable HTTPS on the location server.
A location server user has a default password configured.	If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.	Configure a strong password for the location server users.
HTTP is enabled on the mobility services engine.	HTTP is less secure than HTTPS.	Enable HTTPS on the mobility services engine.
A mobility services engine user has default password configured.	If default password is configured, then Location Server/ Mobility Server Engine is more susceptible to connections from outside the network.	Configure a strong password for the users on the mobility services engine.
wIPS Service is not enabled on the mobility services engine.	Your network is vulnerable to advanced security threats.	Deploy wIPS Service to protect your network from advanced security threats.

Switch Port Tracing

Currently, NCS provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in an CAPWAP Rogue AP Report message. With this method, NCS would simply gather the information received from the controllers; but with software release 5.1, you can incorporate switch port tracing of Wired Rogue Access Point Switch Ports. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in the NCS log and only for rogue access points, not rogue clients.

Note Rogue Client connected to the Rogue Access point information is used to track the switch port to which the Rogue Access point is connected in the network.

Note If you try to set tracing for a friendly or deleted rogue, a warning message appears.

Note For Switch Port Tracing to successfully trace the switch ports using SNMP v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group.

Establishing Switch Port Tracing

To establish switch port tracing, follow these steps:

Step 1 In the NCS home page, click the **Security** dashboard.

Step 2 In the Rogue APs and Adhoc Rogues section, click the number URL which specifies the number of rogues in the last hour, last 24 hours, or total active.

Step 3 Choose for which rogue you are setting switch port tracking by clicking the URL in the MAC Address column. The Alarms > Rogue AP details page opens.

Step 4 From the Select a command drop-down list, choose **Trace Switch Port**. The Trace Switch Port page opens, and NCS runs a switch port trace.

When one or more searchable MAC addresses are available, the NCS uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the switch port of a rogue.

Integrated Security Solutions

The Cisco Unified Wireless Network Solution also provides these integrated security solutions:

- Cisco Unified Wireless Network Solution operating system security is built around a robust 802.1X authorization, authentication, and accounting (AAA) engine, which enables operators to rapidly configure and enforce a variety of security policies across the Cisco Unified Wireless Network Solution.
- The controllers and access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Operating system security policies are assigned to individual wireless LANs, and access points simultaneously broadcast all (up to 16) configured wireless LANs. These policies can eliminate the need for additional access points, which can increase interference and degrade system throughput.
- Operating system security uses the RRM function to continually monitor the air space for interference and security breaches and notify the operator when they are detected.
- Operating system security works with industry-standard AAA servers, making system integration simple and easy.
- The Cisco intrusion detection system/intrusion protection system (CIDS/IPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected.
- The operating system security solution offers comprehensive Layer 2 and Layer 3 encryption algorithms, which typically require a large amount of processing power. Rather than assigning the encryption tasks to yet another server, the controller can be equipped with a VPN/enhanced security module that provides extra hardware required for the most demanding security configurations.

Using NCS to Convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 Mode

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 LWAPP transport mode using the NCS user interface, follow these steps:

Note Cisco-based lightweight access points do not support Layer 2 LWAPP mode. These access points can only be run with Layer 3.

Note This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

Note You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Log into the NCS user interface. Then follow these steps to change the LWAPP transport mode from Layer 3 to Layer 2:

a. Choose **Configure > Controllers** to navigate to the All Controllers page.

b. Click the desired IP address of a controller to display the *IP Address* > Controller Properties page.

c. From the left sidebar menu, click **System > General** to display the *IP Address* > General page.

d. Change LWAPP transport mode to **Layer2,** and click **Save**.

e. If NCS displays the following message, click **OK**:

```
Please reboot the system for the LWAPP Mode change to take effect.
```

Step 3 To restart your Cisco Unified Wireless Network Solution, follow these steps:

a. Return to the *IP Address* > Controller Properties page.

b. Click **System > Commands** to display the *IP Address* > Controller Commands page.

c. Under Administrative Commands, choose **Save Config To Flash**, and click **Go** to save the changed configuration to the controller.

d. Click **OK** to continue.

e. Under Administrative Commands, choose **Reboot**, and click **Go** to reboot the controller.

f. Click **OK** to confirm the save and reboot.

Step 4 After the controller reboots, follow these steps to verify that the LWAPP transport mode is now Layer 2:

a. Click **Monitor > Controllers** to navigate to the Controllers > Search Results page.

b. Click the desired IP address of a controller to display the Controllers > *IP Address* > Summary page.

c. Under General, verify that the current LWAPP transport mode is Layer2.

You have completed the LWAPP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

Configuring a Firewall for NCS

When an NCS server and an NCS user interface are on different sides of a firewall, they cannot communicate unless the following ports on the firewall are open to two-way traffic:

- 80 (for initial http)
- 69 (tftp)
- 162 (trap port)
- 443 (https)

Open these ports to configure your firewall to allow communications between a NCS server and a NCS user interface.

Access Point Authorization

You can view a list of authorized access points along with the type of certificate that an access point uses for authorization.

Step 1 Choose **Configure > Controllers**.

Step 2 Click one of the URLs in the IP address column.

Step 3 From the left sidebar menu, choose **Security > AP/MSE Authorization**.

Step 4 The AP Policies portion of the page indicates whether the authorization of access points is enabled or disabled. It also indicates whether the acceptance of self-signed certificates (SSC APs) is enabled or disabled. Normally, access points can be authorized either by AAA or certificates. (SSC is only available for 4400 and 200 controllers.)

To change these values, choose **Edit AP Policies** from the Select a command drop-down list, and click **Go**.

Step 5 The AP Authorization List portion shows the radio MAC address of the access point, certificate type, and key hash. To add a different authorization entry, choose **Add AP/MSE Auth Entry** from the Select a command drop-down list, and click **Go**.

Step 6 From the drop-down list, choose a template to apply to this controller, and click **Apply**. To create a new template for access point authorization, click the **click here** link to get redirected to the template creation page. See the "Configuring an Access Point or MSE Authorization Template" section on page 11-59 for steps on creating a new template.

Management Frame Protection (MFP)

Management Frame Protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support.

- Infrastructure MFP—Protects management frames by detecting adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting network performance by attacking the QoS and radio measurement frames. It also provides a quick and effective means to detect and report phishing incidents.

  Specifically, infrastructure MFP protects 802.11 session management functions by adding message integrity check information elements (MIC IEs) to the management frame emitted by access points (and not those emitted by clients), which are then validated by other access points in the network. Infrastructure MFP is passive. It can detect and report intrusions but has no means to stop them.

- Client MFP—Shields authenticated clients from spoofed frames, preventing many of the common attacks against wireless LANs from becoming effective. Most attacks, such as deauthentication attacks, revert to simply degrading performance by contending with valid clients.

  Specifically, client MFP encrypts management frames sent between access points and Cisco Compatible Extension clients so that both access points and clients can take preventive action by dropping spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect the following types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP is active. It can protect a client-access point session from the most common type of denial of service attack. It protects class 3 management frames by using the same encryption method used for the session's data frames. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.

To use client MFP, clients must support Cisco Compatible Extensions (version 5) MFP and must negotiate WPA2 using either TKIP or AES-CCMP. EAP or PSK may be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points or Layer 2 and Layer 3 fast roaming.

To prevent attacks against broadcast frames, access points supporting Cisco Compatible Extensions (version 5) do not emit any broadcast class 3 management frames (such as disassociation, deauthentication, or action). Compatible extensions clients (version 5) and access points must discard broadcast class 3 management frames.

Client MFP supplements infrastructure MFP rather than replacing it because infrastructure MFP continues to detect and report invalid unicast frames sent to clients that are not client-MFP capable, as well as invalid class 1 and 2 management frames. Infrastructure MFP is applied only to management frames that are not protected by client MFP.

Infrastructure MFP consists of three main components:

- Management frame protection—The access point protects the management frames it transmits by adding a MIC IE to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy.
- Management frame validation—In infrastructure MFP, the access point validates every management frame it receives from other access points in the network. It ensures that the MC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system. In order for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.
- Event reporting—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to the network management system.

Note Client MFP uses the same event reporting mechanisms as infrastructure MFP.

Infrastructure MFP is enabled by default and can be disabled globally. When you upgrade from a previous software release, infrastructure MFP is disabled globally if access point authentication is enabled because the two features are mutually exclusive. After infrastructure MFP is enabled globally, signature generation (adding MICs to outbound frames) can be disabled for selected WLANs, and validation can be disabled for selected access points.

You set MFP in the WLAN template. See the "Configuring WLAN Template" section on page 11-22.

Guidelines for Using MFP

Follow these guidelines for using MFP:

- MFP is supported for use with Cisco Aironet lightweight access points, except for the 1500 series mesh access points.
- Lightweight access points support infrastructure MFP in local and monitor modes and in REAP and hybrid-REAP modes when the access point is connected to a controller. They support client MFP in local, hybrid-REAP, and bridge modes.
- Client MFP is supported for use only with Cisco Compatible Extensions (version 5) clients using WPA2 with TKIP or AES-CCMP.

- Non-Cisco Compatible Extensions (version 5) clients may associate to a WLAN if client MFP is disabled or optional.

Configuring Intrusion Detection Systems (IDS)

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/IPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect IDS attacks:

- IDS sensors (for Layer 3)
- IDS signatures (for Layer 2)

Viewing IDS Sensors

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

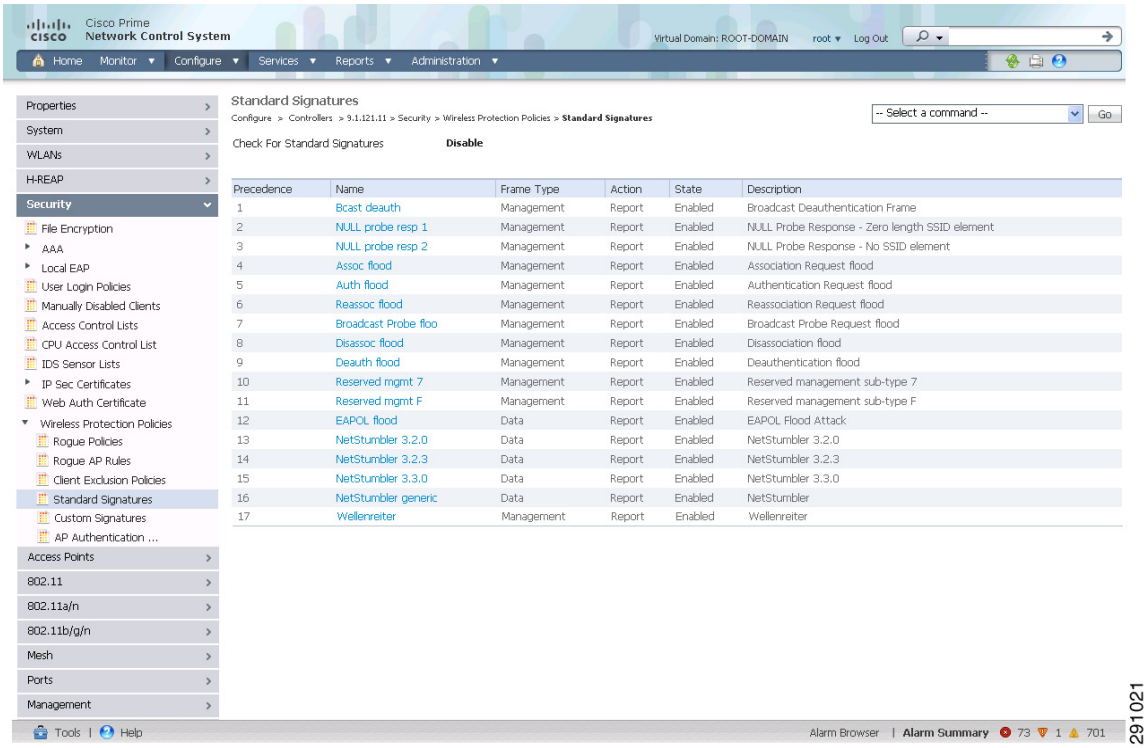
Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**. The IDS Sensor page appears. This page lists all of the IDS sensors that have been configured for this controller.

Configuring IDS Signatures

You can configure *IDS signatures*, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on the controller as shown on the Standard Signatures and Custom Signatures page (see Figure 3-3). To open this page, choose **Configure > Controllers**, select a controller IP address, and then choose **Security > Wireless Protection Policies > Standard Signatures** from the left sidebar menu.

Figure 3-3 Standard Signatures Page



These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures:

- Broadcast deauthentication frame signatures—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.
- NULL probe response signatures—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures include:
  - NULL probe resp 1 (precedence 2)
  - NULL probe resp 2 (precedence 3)
- Management frame flood signatures—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristics of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to NCS.

The management frame flood signatures include:

- Assoc flood (precedence 4)
- Auth flood (precedence 5)
- Reassoc flood (precedence 6)
- Broadcast probe flood (precedence 7)
- Disassoc flood (precedence 8)
- Deauth flood (precedence 9)
- Reserved mgmt 7 (precedence 10)
- Reserved mgmt F (precedence 11)

The reserved management frame signatures 7 and F are reserved for future use.

- EAPOL flood signature—During an EAPOL flood attack, a hacker floods the air with EAPOL frames containing 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.
- NetStumbler signatures—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached). If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version listed in Table 3-9.

Table 3-9 NetStumbler Versions

Version	String
3.2.0	“Flurble gronk bloopit, bnip Frundletrune”
3.2.3	“All your 802.11b are belong to us”
3.3.0	Sends white spaces

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures include:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

- Wellenreiter signature—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.

This section provides the instructions to configure signatures and includes the following topics:

Uploading IDS Signatures

To upload IDS signatures from the controller, follow these steps:

Step 1 Obtain a signature file from Cisco (hereafter called a *standard signature file*). You can also create your own signature file (hereafter called a *custom signature file*) by following the "Downloading IDS Signatures" section on page 3-37.

Step 2 You can configure a TFTP server for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add *IP address of TFTP server*).
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco NCS because built-in TFTP server of NCS and third-party TFTP server use the same communication port.

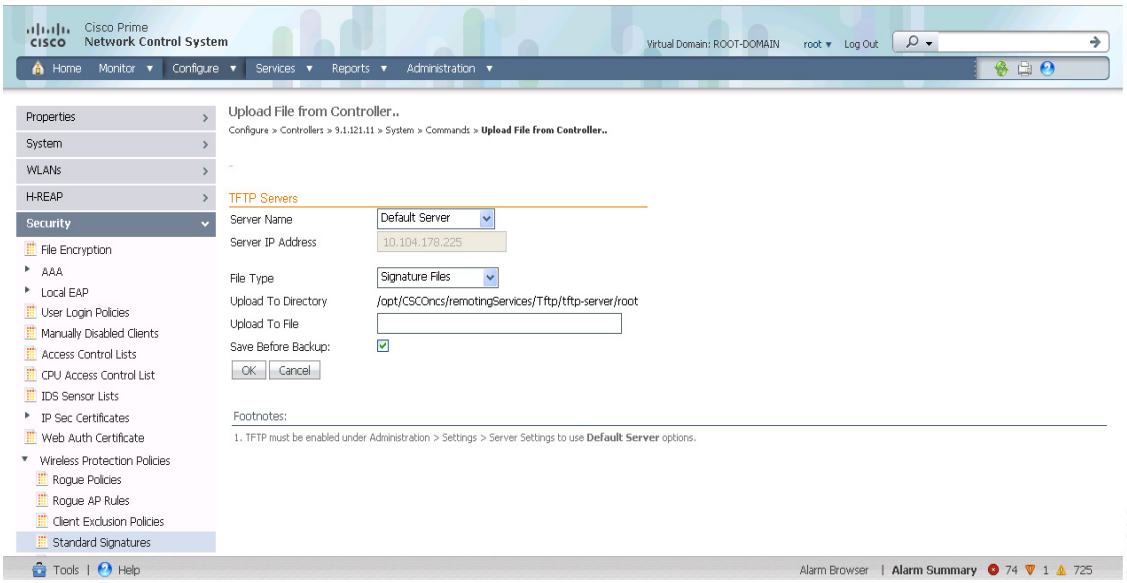
Step 3 Choose **Configure > Controllers**.

Step 4 Choose a controller by clicking on an IP address.

Step 5 From the left sidebar menu, choose **Security** and then **Standard Signatures** or **Custom Signatures**.

Step 6 From the Select a command drop-down list, choose **Upload Signature Files from Controller**. Figure 3-4 shows the page that appears.

Figure 3-4 Uploading Signature File



Step 7 Specify the TFTP server name being used for the transfer.

Step 8 If the TFTP server is new, enter the TFTP IP address at the Server IP Address parameter.

Step 9 Choose **Signature Files** from the File Type drop-down list.

Step 10 The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File parameter (this parameter only shows if the Server Name is the default server). The controller uses this local file name as a base name and then adds *_std.sig* as a suffix for standard signature files and *_custom.sig* as a suffix for custom signature files.

Step 11 Click **OK**.

Downloading IDS Signatures

If the standard signature file is already on the controller but you want to download customized signatures to it, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking an IP address.

Step 3 Choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down list, choose **Download IDS Signatures**, and click **Go**.

Step 5 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 6 Choose **local machine** from the File is Located On parameter. If you know the filename and path relative to the server's root directory, you can also choose TFTP server.

Step 7 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries parameter.

Step 8 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout parameter.

Step 9 The signature files are uploaded to the c:\tftp directory. Specify the local file name in that directory or use the Browse button to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Step 10 If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name will be populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to the built-in TFTP server of NCS. Then the controller retrieves that file. For later operations, the file is already in the NCS server's TFTP directory, and the download web page now automatically populates the filename.

Step 11 Click **OK**.

Enabling or Disabling IDS Signatures

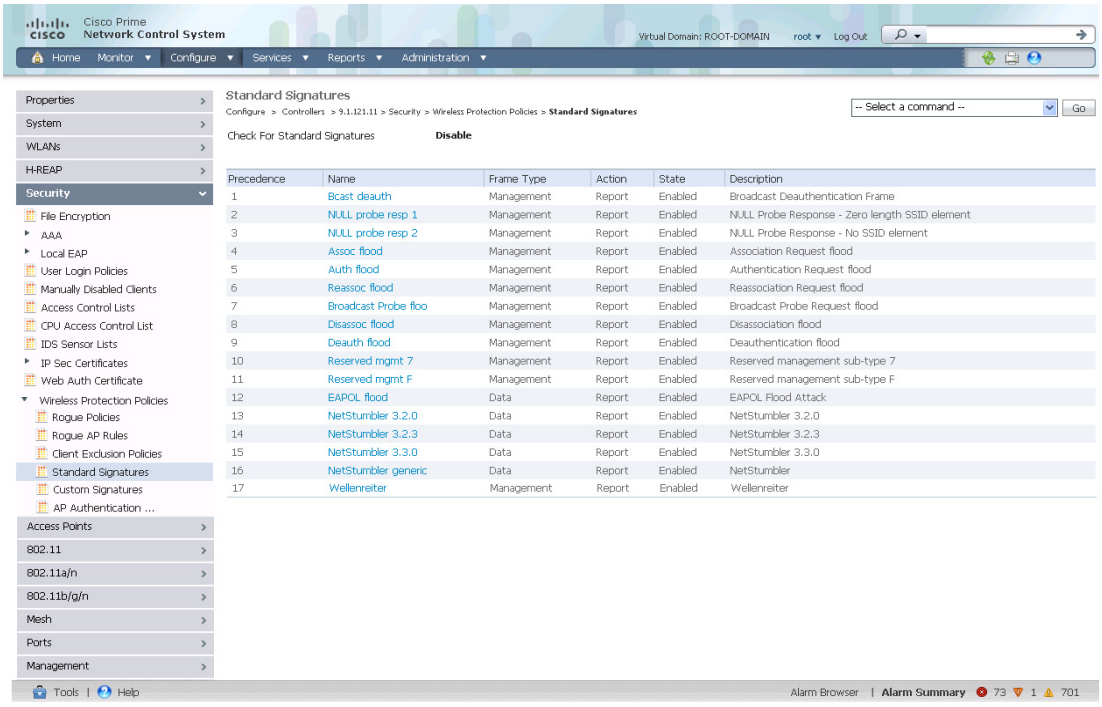
To enable or disable IDS signature, follow these steps:

Step 1 Choose **Configure > Controllers**.

Step 2 Choose a controller by clicking on an IP address.

Step 3 From the left sidebar menu, choose **Security** and then **Standard Signatures** or **Custom Signatures**. Figure 3-5 shows a sample of the page that appears.

Figure 3-5 Checking for Standard Signatures



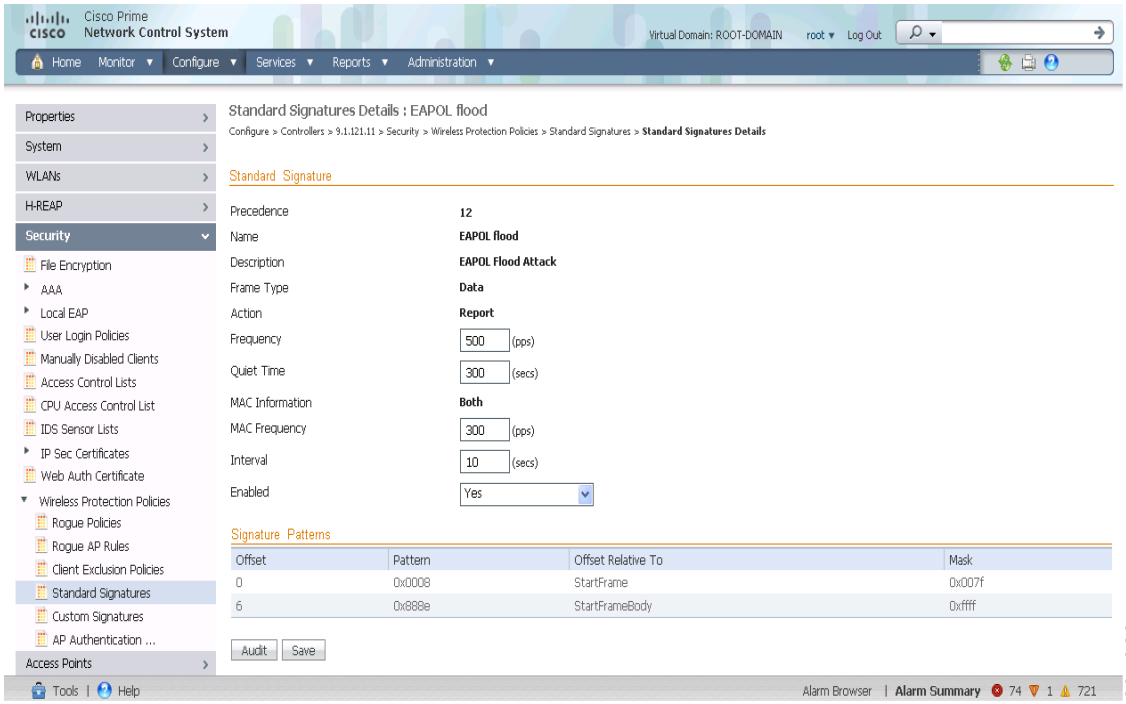
Step 4 To enable or disable an individual signature, click in the **Name** column for the type of attack you want to enable or disable. Figure 3-6 shows a sample of a detailed signature screen.

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following information is displayed either on the signature page or the detailed signature page:

- Precedence - The order, or precedence, in which the controller performs the signature checks.
- Name - The type of attack the signature is trying to detect.
- Description - A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type - Management or data frame type on which the signature is looking for a security attack.
- Action - What the controller is directed to do when the signature detects an attack. One possibility is *None*, where no action is taken, and another is *Report*, to report the detection.
- Frequency - The signature frequency, or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value is 50 packets per interval.
- Quiet Time - The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds, and the default value is 300 seconds.
- MAC Information - Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- MAC Frequency - The signature MAC frequency, or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value is 30 packets per interval.

- Interval - Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value is 1 second.
- Enable - Select this to enable this signature to detect security attacks or unselect it to disable this signature.
- Signature Patterns - The pattern that is being used to detect a security attack.

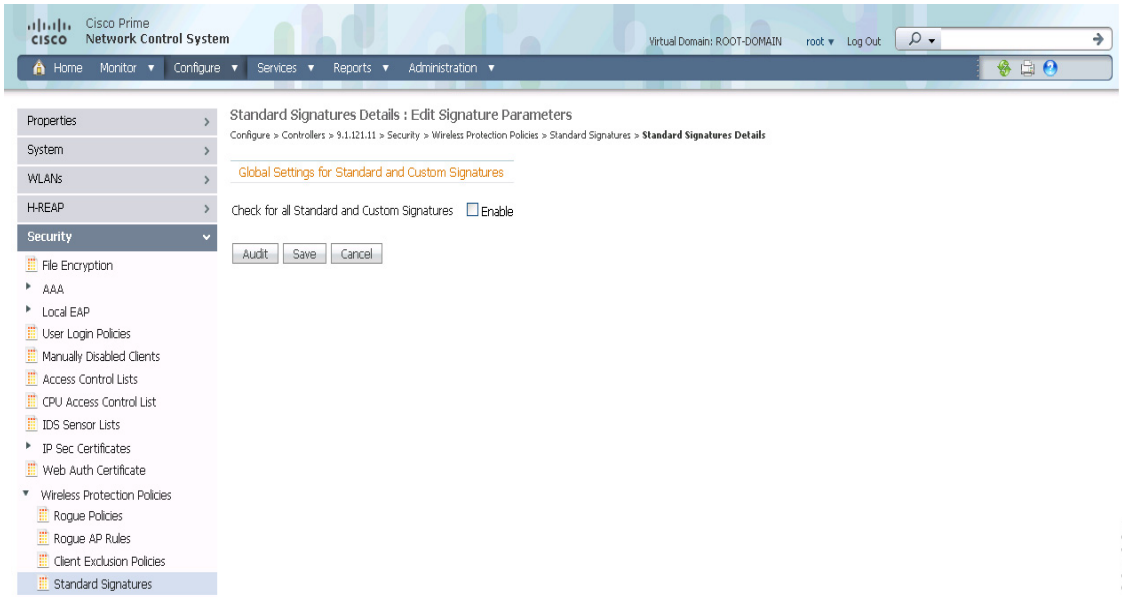
Figure 3-6 Standard Signature



Step 5 From the Enabled yes or no drop-down list, choose **yes**. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. (For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.)

Step 6 To enable all standard and custom signatures currently on the controller, choose **Edit Signature Parameters** (from the screen in Figure 3-5) from the Select a command drop-down list, and choose **Go**. The Edit Signature Parameters page appears (see Figure 3-7).

Figure 3-7 Global Setting for Standard and Custom Signature



Step 7 Select the Check for All Standard and Custom Signatures parameter, **Enable** check box. This enables all signatures that were individually selected as enabled in Step 5. If this check box remains unselected, all files are disabled, even those that were previously enabled in Step 5. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

Step 8 Click **Save**.

Enabling Web Login

With web authentication, guests are automatically redirected to web authentication pages when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts may be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. See the "Configuring a Web Authentication Template" section on page 11-64 to create a template that replaces the Web authentication page provided on the controller.

Step 1 Choose **Configure > Controllers**.

Step 2 Choose the controller on which to enable web authentication by clicking an IP address URL in the IP Address column.

Step 3 From the left sidebar menu, choose **Security > AAA > Web Auth Configuration**.

Step 4 Choose the appropriate web authentication type from the drop-down list. The choices are default internal, customized web authentication, or external.

- If you choose default internal, you can still alter the page title, message, and redirect URL, as well as choose whether the logo appears. Continue to Step 5.

- If you choose customized web authentication, skip to the "Downloading Customized Web Authentication" section on page 3-42.
- If you choose external, you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

Step 5 Select the **Logo Display** check box if you want your company logo to display.

Step 6 Enter the title you want displayed on the Web authentication page.

Step 7 Enter the message you want displayed on the Web authentication page.

Step 8 In the Customer Redirect URL parameter, provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.company.com, the user is directed to the company home page.

Step 9 Click **Save**.

Downloading Customized Web Authentication

You can download a customized Web authentication page to the controller. A customized web page is created to establish a username and password for user web access.

When downloading customized web authentication, these strict guidelines must be followed:

- A username must be provided.
- A password must be provided.
- A redirect URL must be retained as a hidden input item after extracting from the original URL.
- The action URL must be extracted and set from the original URL.
- Scripts to decode the return status code must be included.
- All paths used in the main page should be of relative type.

Before downloading, if you chose the customized web authentication option in Step 4 of the previous section, follow these steps:

Step 1 Click the preview image to download the sample login.html bundle file from the server. See Figure 3-8 for an example of the login.html file. The downloaded bundle is a .TAR file.

Figure 3-8 Login.html

Step 2 Open and edit the login.html file and save it as a .tar or .zip file.

Note You can edit the text of the Submit button with any text or HTML editor to read "Accept terms and conditions and Submit."

Step 3 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco NCS because the built-in TFTP server of NCS and third-party TFTP server use the same communication port.

Step 4 Click **here** in the "After editing the HTML you may click **here** to redirect to the Download Web Auth Page" link to download the .tar or .zip file to the controller(s). The Download Customized Web Auth Bundle to Controller page appears.

Note The IP address of the controller to receive the bundle and the current status are displayed.

Step 5 Choose **local machine** from the File is Located On parameter. If you know the filename and path relative to the server's root directory, you can also choose TFTP server.

Note For a local machine download, either .zip or .tar file options exists, but NCS does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files are specified.

Step 6 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout parameter.

Step 7 The NCS Server Files In parameter specifies where the NCS server files are located. Specify the local file name in that directory or use the Browse button to navigate to it. A "revision" line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

Step 8 If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated. The local machine option initiates a two-step operation. First, the local file is copied from the administrator's workstation to the built-in TFTP server of NCS. Then the controller retrieves that file. For later operations, the file is already in the NCS server's TFTP directory, and the download web page now automatically populates the filename.

Step 9 Click **OK**.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On parameter, and the Server File Name is populated for you.

Step 10 After completing the download, you are directed to the new page and able to authenticate.

Connecting to the Guest WLAN

To connect to the guest central WLAN to complete the web authentication process, follow these steps: See the "Creating Guest User Accounts" section on page 7-10 for more explanation of a guest user account.

Step 1 When you are set for open authentication and are connected, browse to the virtual interface IP address (such as /1.1.1.1/login.html).

Step 2 When the NCS user interface displays the Login page, enter your username and password.

Note All entries are case sensitive.

The lobby ambassador has access to the templates only to add guest users.

Certificate Signing Request (CSR) Generation

To generate a Certificate Signing Request (CSR) for a third-party certificate using NCS, refer to the following document for instructions on uploading the certificate:

http://www.cisco.com/en/US/products/ps6305/products_configuration_example09186a00808a94ca.shtml.