CHAPTER 3

Configuring Security Solutions

This chapter describes security solutions for wireless LANs. It contains these 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.

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 WCS, 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 WCS, errors can be eliminated, and the overall effort is greatly reduced.

Rogue Access Point Solutions

This section describes security solutions for rogue access points.

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.

Tagging and Containing Rogue Access Points

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

Rogue Management

WCS rogue management includes rogue access points and rogue adhocs. You can click the **Security** tab from the WCS Home window to see the most recent rogue adhocs.

Most Recent Rogue Adhocs

The Most Recent Rogue Adhocs section displays the rogue adhoc MAC address, SSID, state, and date and time of initial detection.

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

Step 1 Click the **MAC Address** of a specific rogue adhoc to view its associated alarm details.

Step 2 To modify the alarm, choose one of the following commands from the Select a command drop-down menu and click **GO**.

- Assign to me—Assigns the selected alarm to the current user.
- Unassign—Unassigns the selected alarm.
- Delete—Deletes the selected alarm.
- Clear—Clears the selected alarm.
- Acknowledge—Allows you to designate the alarm as acknowledged.

  Note If you mark the alarm as acknowledged, it does not show in the Alarm Summary window.

- Unacknowledge—Changes the acknowledged alarm back to unacknowledged.
- Event History—Enables you to view events for the rogue adhoc alarm.

  Note Event History for this adhoc can also be accessed from the Most Recent Rogue Adhocs details page.

- Detecting APs—Enables you to view the access points that are currently detecting the rogue adhoc.
- Map (High Resolution)—Displays the current calculated rogue adhoc location on the Maps > *Building Name* > *Floor Name* page.
- Rogue Clients—Enables you to view the clients associated with this rogue adhoc.

- Set State to ‘Unknown - Alert’—Tags the rogue adhoc as the lowest threat, continues to monitor the rogue adhoc, and turns off containment.
- Set State to ‘Known - Internal’—Tags the rogue adhoc as internal, adds it to the known rogue adhoc list, and turns off containment.
- Set State to ‘Known - External’—Tags the rogue adhoc as external, adds it to the known rogue adhoc list, and turns off containment.
- 1 AP Containment through 4 AP Containment—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send deauthenticate and disassociate messages to the client devices that are associated to the rogue unit.

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

Follow these steps to convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 LWAPP transport mode using the WCS user interface.

Note IOS-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 WCS user interface. Then follow these steps to change the LWAPP transport mode from Layer 3 to Layer 2:

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

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

c. In the sidebar, click **System > General** to display the *IP Address* > General page.

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

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

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

Step 3 Follow these steps to restart your Cisco Unified Wireless Network Solution:

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 > Devices > Controllers** to navigate to the Controllers > Search Results page.

b. Click the desired controller's IP address 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 WCS

When a WCS server and a WCS 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 WCS server and a WCS 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 Authorization**.

Step 4 The AP Policies portion of the window 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 menu 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 Auth Entry** from the Select a command drop-down menu and click **GO**.

Step 6 From the drop-down menu, choose a template to apply to this controller and click **Apply**. To create a new template for access point authorization, click the **click here** to get redirected to the template creation page. Refer to the "Configuring an Access Point or LBS Authorization" section on page 11-39 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. WCS software release 4.1 and later supports both infrastructure and client MFP while WCS software release 4.0 supports only infrastructure MFP.

- **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. Refer to the "Configuring WLAN Templates" section on page 11-9.

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 protection 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.

Follow these steps to view IDS sensors.

Step 1 Choose **Configure > Controllers**.

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

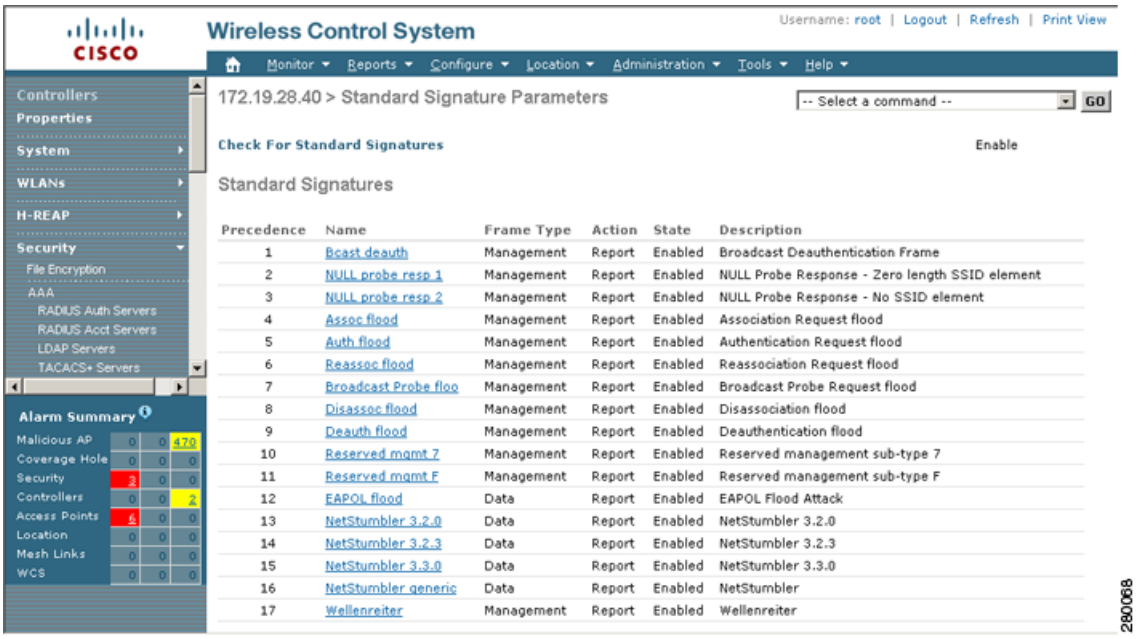
Step 3 From the left sidebar menu, choose **Security > IDS Sensor Lists**. The IDS Sensor window appears. This page lists all of the IDS sensors that have been configured for this controller.

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 3-1).

Figure 3-1 Standard Signature Window



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 WCS.

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.

- 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.
- 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:

Table 3-1 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)

Follow these instructions to configure signatures:

Uploading IDS Signatures

Follow these steps to upload IDS signatures from the controller.

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 3-12.

Step 2 Make sure you have a Trivial File Transfer Protocol (TFTP) server available 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.
- 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 WCS because WCS's built-in TFTP server and third-party TFTP server use the same communication port.

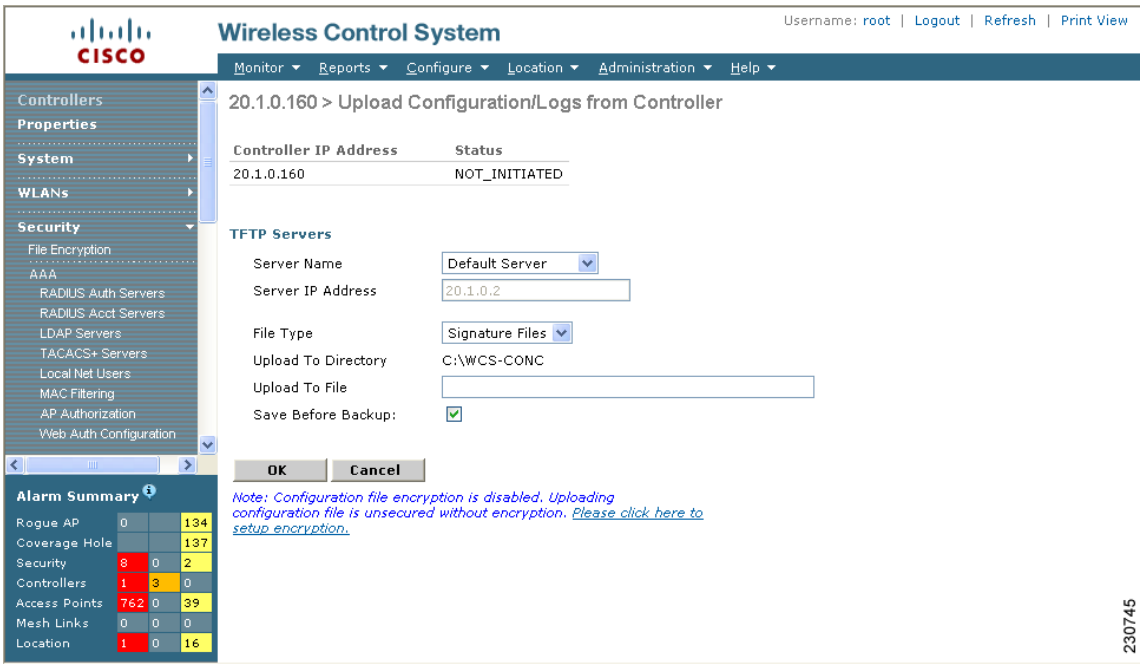
Step 3 Choose **Configure > Controllers**.

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 menu, choose **Upload Signature Files from Controller**. Figure 3-2 shows the window that appears.

Figure 3-2 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 menu.

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 on an IP address.

Step 3 Choose **System > Commands**.

Step 4 From the Upload/Download Commands drop-down menu, 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 WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS server's TFTP directory, and the download web page now automatically populates the filename.

Step 11 Click **OK**.

Enabling or Disabling IDS Signatures

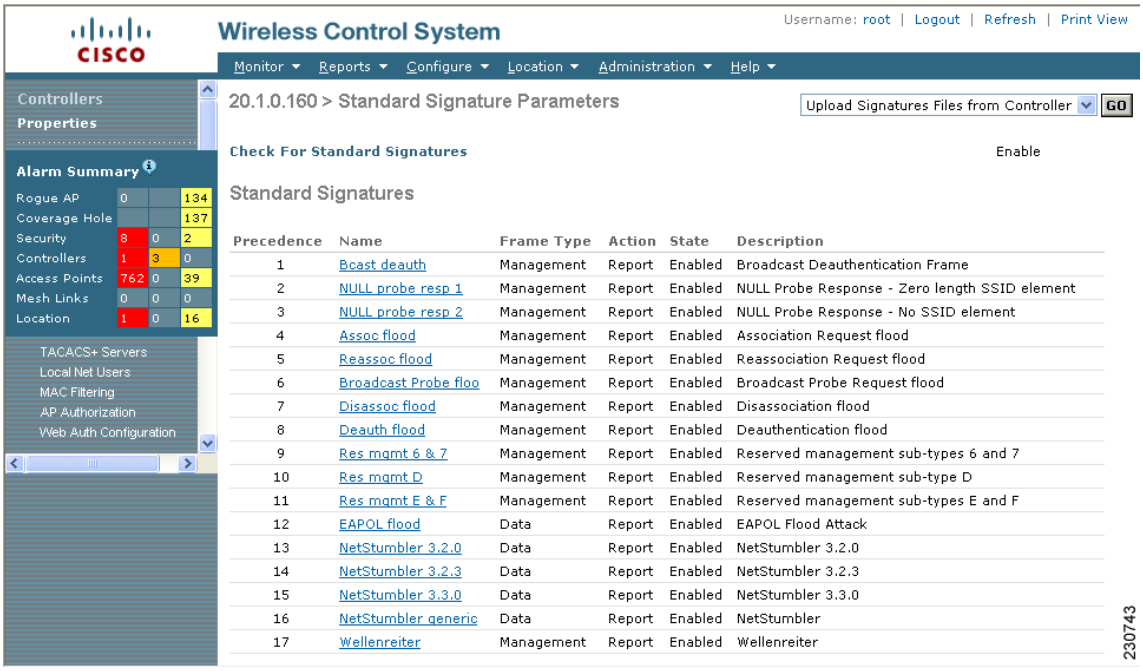
Follow these steps to enable or disable IDS signature.

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 3-3 shows a sample of the screen that appears.

Figure 3-3 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 3-4 shows a sample of a detailed signature screen.

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

- 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.

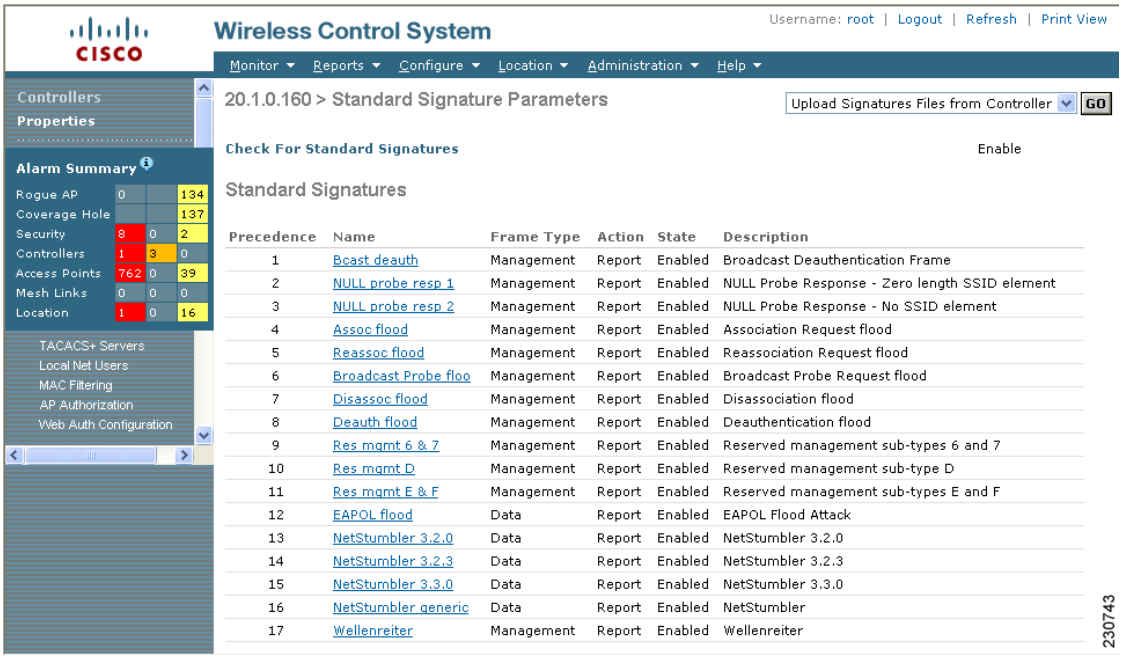
- Interval - Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value is 1 second.
- Enable - Check this to enable this signature to detect security attacks or uncheck it to disable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

Figure 3-4 Standard Signature

Step 5 In the Enable yes or no drop-down menu, 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 3-3) from the Select a command drop-down list and click **GO**. The Global Settings for Standard and Custom Signature window appears (see Figure 3-5).

Figure 3-5 Global Setting for Standard and Custom Signature



Step 7 Check the **Enable Check for All Standard and Custom Signatures** check box. This enables all signatures that were individually selected as enabled in Step 5. If this box remains unchecked, 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**.

Viewing IDS Signature Events

Follow these steps to see the number of attacks detected by the enabled signatures.

Step 1 Choose **Monitor > Events** or **Monitor > Alarms**.

Step 2 From the Event Category drop-down menu on the left sidebar menu, choose **Security** and click **Search**.

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 11-50 to create a template that replaces the Web authentication page provided on the controller.

Step 1 Choose **Configure > Controller.**

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 > Web Auth Configuration**.

Step 4 Choose the appropriate web authentication type from the drop-down menu. 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 3-17.
- 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 field is http://www.company.com, the user is directed to the company home page.

Step 5 Click 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 Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this field is http://www.company.com, the user is directed to the company home page.

Step 9 Click **Save**.

Downloading Customized Web Authentication

Follow these steps if you chose the customized web authentication option in Step 4 of the previous section. 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, the following steps are required:

Step 1 Click on the preview image to download the sample login.html bundle file from the server. See Figure 3-6 for an example of the login.html file. The downloaded bundle is a .TAR file.

Figure 3-6 Login.html

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

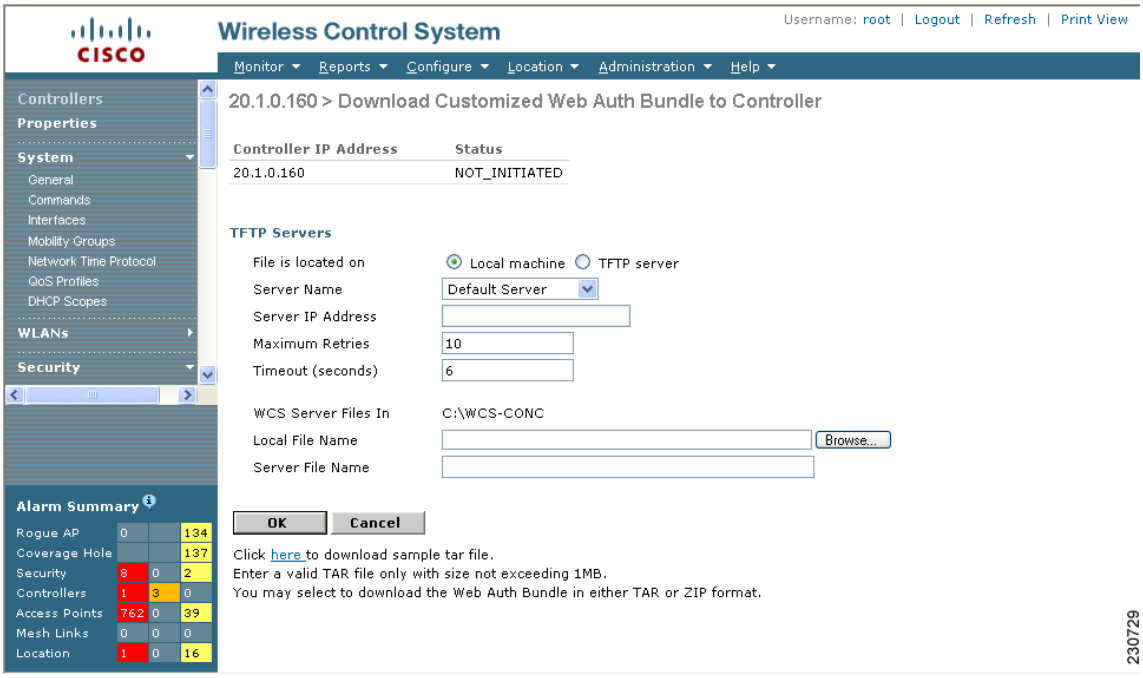
Note You can edit the text of the Submit button with any text or HTML editor to read "Accept terms and conditions and Submit."

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 WCS because WCS's built-in TFTP server 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 window appears (see Figure 3-7).

Figure 3-7 Download Customized Web Auth Bundle to Controller



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 the WCS 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 WCS Server Files In parameter specifies where the WCS 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 WCS's own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in the WCS 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

Follow these steps to connect to the guest central WLAN to complete the web authentication process. See the "Creating Guest User Accounts" section on page 7-11 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 WCS user interface displays the Login window, enter your username and password.

Note All entries are case sensitive.

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

Step 3 Click **Submit** to log into WCS. The WCS user interface is now active and available for use. The Guest Users Templates page is displayed. This page provides a summary of all created Guest User templates.

Note To exit the WCS user interface, close the browser window or click **Logout** in the upper right corner of the page. Exiting a WCS user interface session does not shut down WCS on the server.

Note When a system administrator stops the WCS server during your WCS session, your session ends, and the web browser displays this message: "The page cannot be displayed." Your session does not reassociate to WCS when the server restarts. You must restart the WCS session.

Deleting a Guest User

Follow these steps to delete all clients stations that are logged in and using the guest WLAN and its account's username.

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

Step 2 From the left sidebar menu, choose **Security > Guest Users**.

Step 3 Click the check box before the username you want to delete. WCS gives you a warning message before deletion.

Step 4 From the Select a command drop-down menu, choose **Delete Templates**. The window displays remove results if the deletion was successful.

Note The controller can also send notification when a guest account has expired by invoking a trap. WCS processes this trap and deletes the guest user account from the configuration of that controller.

Certificate Signing Request (CSR) Generation

To generate a Certificate Signing Request (CSR) for a third-party certificate using WCS, refer to the following document for instructions on uploading the certificate: http://www.cisco.com/en/US/products/ps6305/products_configuration_example09186a00808a94ca.shtml.