Configuring wIPS and Profiles

This chapter describes how to configure wIPS profiles and those items that must be configured in conjunction to operate wIPS.

This chapter contains the following sections:

Configuring wIPS and Profiles

This chapter describes how to configure wIPS profiles and those items that must be configured in conjunction to operate wIPS.

This chapter contains the following sections:

Guidelines and Limitations

- The Mobility Services Engine can only be configured from one Prime Infrastructure.
- If your wIPS deployment consists of a controller, access point, and MSE, you must set the controller and MSE to UTC timezone.
- A controller is associated to a single configuration profile. All wIPS mode access points connected to that controller share the same wIPS configuration.

Prerequisites

Before you can configure wIPS profiles you must do the following:

1. Install a Mobility Services Engine (if one is not already operating in the network). See the *Cisco 3350 Mobility Services Engine Getting Started Guide* or *Cisco 3310 Mobility Services Engine Getting Started Guide*
2. Add the Mobility Services Engine to the Prime Infrastructure (if not already added).
3. Configure access points to operate in wIPS monitor mode or Local wIPS mode.

4 Configure wIPS profiles.

Information About wIPS Configuration and Profile Management

Configuration of wIPS profiles follows a chained hierarchy starting with the Prime Infrastructure, which is used for profile viewing and modification. The actual profiles are stored within the wIPS service running on the MSE.

From the wIPS service on the Mobility Services Engine, profiles are propagated to specific controllers, which in turn communicate this profile transparently to wIPS mode access points associated to that respective controller.

When a configuration change to a wIPS profile is made at the Prime Infrastructure and applied to a set of Mobility Services Engines and controllers, the following occurs:

1 The configuration profile is modified on the Prime Infrastructure and version information is updated.

2 An XML-based profile is pushed to the wIPS engine running on the Mobility Services Engine. This update occurs over the SOAP/XML protocol.

3 The wIPS engine on the Mobility Services Engine updates each controller associated with that profile by pushing out the configuration profile over NMSP.

4 The controller receives the updated wIPS profile, stores it into NVRAM (replacing any previous revision of the profile) and propagates the updated profile to its associated wIPS access points using CAPWAP control messages.

5 A wIPS mode access point receives the updated profile from the controller and applies the modifications to its wIPS software engine.

This section contains the following topics:

Guidelines and Limitations

• Only Cisco Aironet 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3600, 3502E and 3502I Series Access Points support wIPS monitor mode.

Configuring Access Points for wIPS Monitor Mode

To configure an access point to operate in wIPS monitor mode, follow these steps:

Step 1 Choose **Configure > Access Points**.

Step 2 Click the **802.11a** or **802.11b/g** radio link.

Figure 1: Configure > Access Points > Radio

Step 3 In the Access Point page, unselect the **Admin Status** check box to disable the radio.

Figure 2: Access Points > Radio

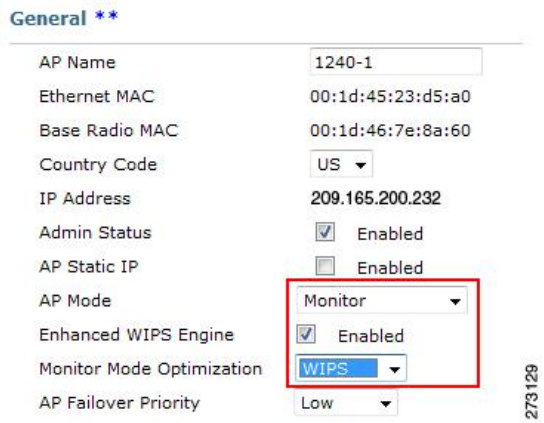
Step 4 Click **Save**.

Note Repeat these steps for each radio on an access point that is to be configured for wIPS monitor mode.

Step 5 Once the radios are disabled, choose **Configure** > **Access Points** and then click the name of the access point of the radio you just disabled.

Step 6 In the access point dialog box, choose **Monitor** from the AP Mode drop-down list.

Figure 3: Configure > Access Points > Access Point Detail



Step 7 Select the **Enabled** check box for the Enhanced WIPS Engine.

Step 8 From the Monitor Mode Optimization drop-down list, choose **WIPS**.

Step 9 Click **Save**.

Step 10 Click **OK** when prompted to reboot the access point.

Step 11 To reenable the access point radio, choose **Configure > Access Points**.

Step 12 Click the appropriate access point radio.

Figure 4: Configure > Access Points > Radio

Step 13 In the Radio Detail page, select the Admin Status **Enabled** check box.

Step 14 Click **Save**.

Repeat this procedure for each access point and each respective radio configured for wIPS monitor mode.

Configuring wIPS Profiles

By default, the Mobility Services Engine and corresponding wIPS access points inherit the default wIPS profile from the Prime Infrastructure. This profile comes pre-tuned with a majority of attack alarms enabled by default and monitors attacks against access points within the same RFGroup as the wIPS access points. In

this manner, the system comes pre-setup to monitor attacks against a deployment model that utilizes an integrated solution in which both the WLAN infrastructure and wIPS access points are intermixed on the same controller.

Note Some of the configuration steps that follow are marked as Overlay-Only and are only to be undertaken when deploying the wIPS solution to monitor an existing WLAN Infrastructure such as an autonomous or completely separate controller-based WLAN.

To configure wIPS profiles, follow these steps:

Step 1 Choose **Configure** > **wIPS Profiles**.
The wIPS Profiles page appears.

Step 2 From the Select a command drop-down list, choose **Add Profile**, and click **Go**.

Figure 5: wIPS Profiles > Profile List

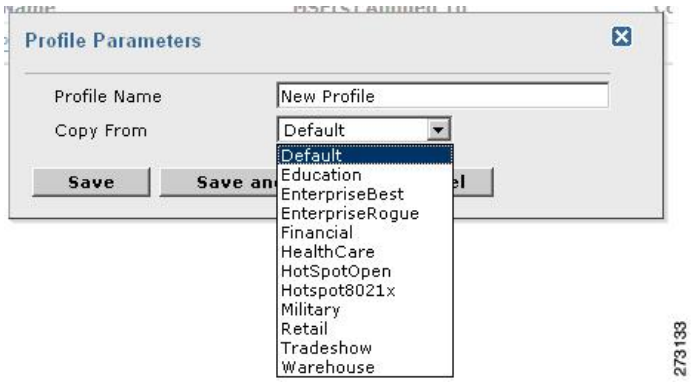
Step 3 `Selecting a Profile Template`
In the Profile Parameters dialog box, choose a profile template from the Copy From drop-down list.

Note The wIPS comes with a pre-defined set of profile templates from which you can choose or use as a basis for their own custom profiles. Each profile is tailored to either a specific business or application as are the specific alarms enabled on that profile.

Note You cannot edit the default profile.

Note Ensure that the NMSP session is active to push the profile to the controller.

Figure 6: Profile Parameters Dialog Box



Step 4 After selecting a profile and entering a profile name, click **Save and Edit**. Fore more information, see the wIPS Profiles, on page 11 section.

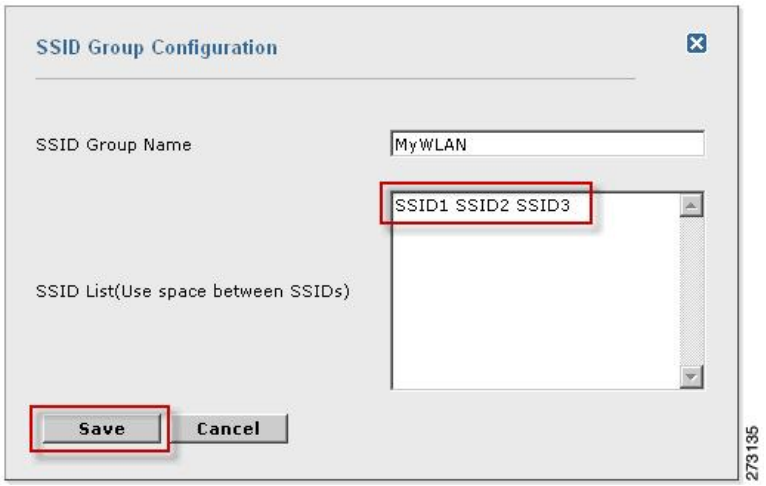
Step 5 **`Configure the SSIDs to Monitor`**
(Optional) Configure SSIDs in the SSID Group List page. By default, the system monitors attacks launched against the local Wireless LAN Infrastructure (as defined by APs which have the same RF Group name). If the system should also be required to monitor attacks against another network, such as when deployed in an overlay deployment model, the SSID groups feature must be utilized.

Note If this step is not required, simply click **Next**.

Figure 7: SSID Groups Summary Pane

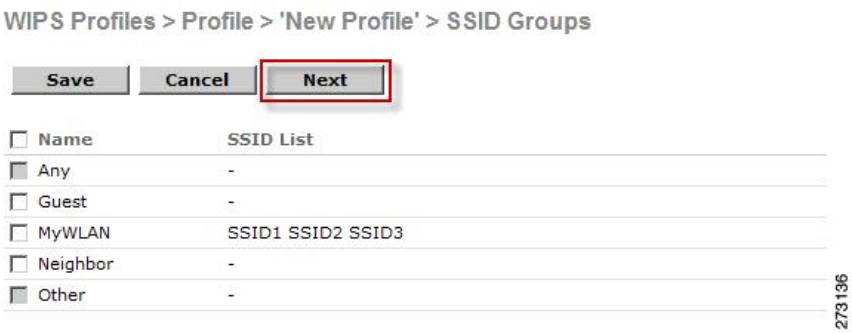
1. Select the **MyWLAN** check box and choose **Edit Group** from the drop-down list, then click **Go**.
2. Enter SSIDs to Monitor. This step is required if the system to be utilized to monitor attacks against a different WLAN infrastructure which is typical of an overlay deployment model.
3. Enter the SSID name (separate multiple entries by a single space), and click **Save**.

Figure 8: SSID Group Configuration Dialog Box



The SSID Groups page appears confirming that the SSIDs are added successfully. For more information, see the Configuring wIPS SSID Group List, on page 14 section.

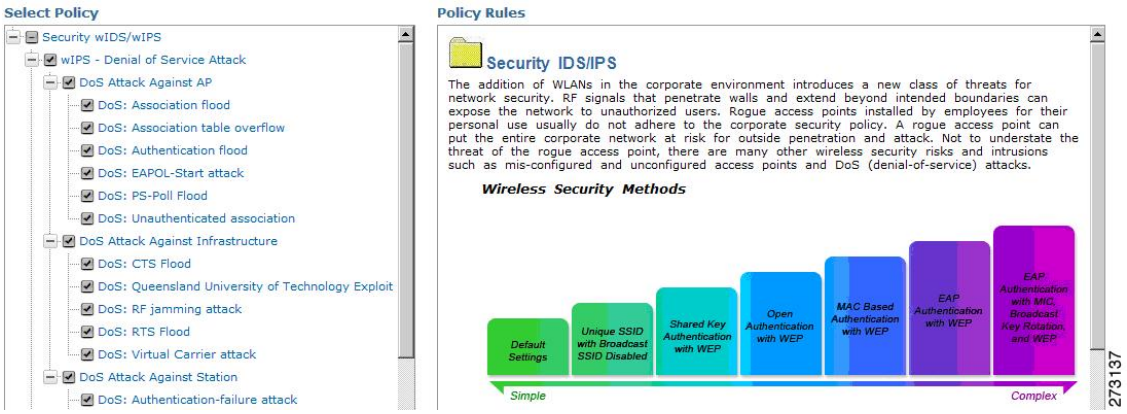
Figure 9: New Profile > SSID Groups Page



4 Click **Next**.

The Select Policy and Policy Rules summary panes appear.

Figure 10: Next > Select Policy Summary Pane



Step 6 **`Editing the Profile`**

To enable or disable attacks to be detected and reported, select the check box next to the specific attack type in question in the Select Policy pane.

Step 7 To edit the profile, click the name of the attack type (such as DoS: Association flood).

The configuration pane for that attack type appears in the right pane above the policy rule description.

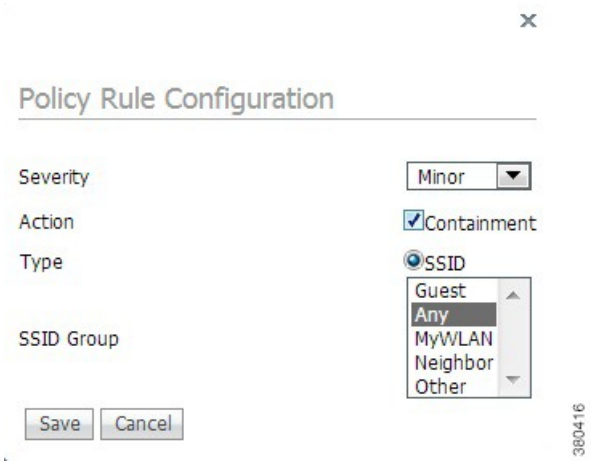
Figure 11: Policy Rules Pane

Step 8 **`Editing the Policy Rules`**.

To modify a policy rule, select the check box next to the policy rule in the Policy Rules page, and click **Edit**.

The Policy Rule Configuration dialog box appears. Configure the following in the **Policy Rule Configuration** dialog box:

Figure 12: Policy Rule Configuration Dialog Box



a) Choose the severity of the alarm to be modified from the **Severity** drop-down list. The possible options are **Minor**, **Major**, **Critical**, and **Warning**.
b) Select the **Containment** check box to enable the auto containment action.
Note The following security penetration attacks can be configured for Rogue AP containment in Release 7.5:

- Soft AP or Host AP Detected
- Airsnarf Attack Detected
- Honeypot AP Detected
- Hotspotter Tool Detected
- Karma Tool Detected
- Device Broadcast XSS SSID

c) Select the **Forensic** check box if you want to capture packets for this alarm.
d) Modify the number of active associations, if desired. (This value varies by alarm type).
e) Select the type of WLAN infrastructure (SSID or Device Group) that the system monitors for attacks from the **SSID Group** drop-down list.

- If you select SSID, continue with Step 9.
- If you select Device Group, continue with Step 10.

Note Device Group (Type) and Internal are the defaults. Internal indicates all access points within the same RF Group. Selecting SSID as the type, allows you to monitor a separate network, which is typical of an overlay deployment.

Step 9 `Add Policy Rules (Optional)`
(Optional), For overlay deployments only, to add a policy rule for an SSID, do the following:

1 To add a policy rule, click **Add**.

Figure 13: Adding a Policy Rule

2 In the **Policy Rule Configuration** dialog box, choose **MyWLAN** from the SSID Group list.

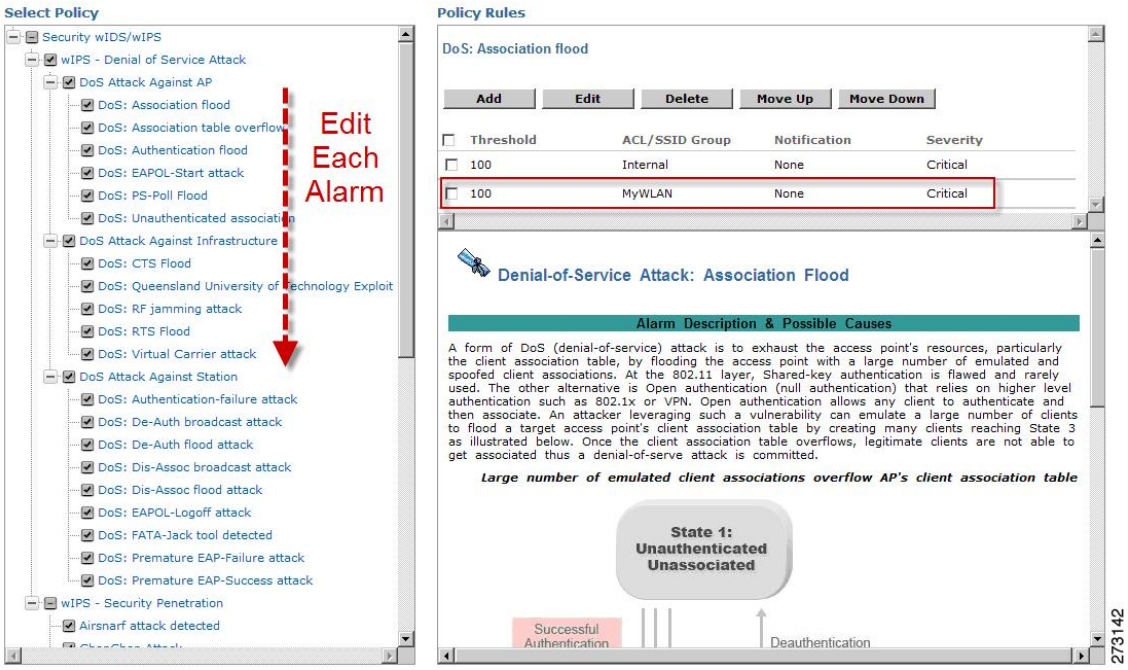
Note SSID is already selected as the type.

3 Click **Save** after all changes are complete.

4 Modify each policy rule. Continue with Step 10 when all modifications are complete.

Note When you configure a system to monitor another WLAN infrastructure by SSID, changes must be made for each and every policy rule to monitor. You must create a policy rule under each separate alarm which defines the system to monitor attacks against the SSID Group created earlier.

Figure 14: Edit Policy Rules for SSID Monitoring

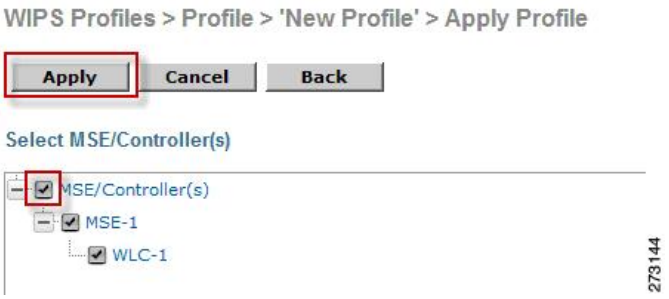


Step 10 In the Profile Configuration dialog box, click **Save** to save the Profile (SSID or Device Group). Click **Next**.

Figure 15: Profile Configuration Dialog box

Step 11 Select the MSE/Controller combinations to apply the profile to and then click **Apply**.

Figure 16: Apply Profile Dialog Box



wIPS Profiles

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles.

Tip To learn more about Cisco Adaptive wIPS features and functionality, go to http://www.cisco.com/en/US/products/ps9817/index.html

To access the wIPS profile list for the Prime Infrastructure, choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List. If the Profile List is not currently displayed, choose **Profile List** from the wIPS Profiles left sidebar menu.

The Profile List provides the following information for each profile:

- Profile Name—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

Note When you hover your mouse cursor over the profile name, the Profile ID and version appear.

- MSE(s) Applied To—Indicates the number of Mobility Services Engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

This section contains the following topics:

- Adding a Profile
- Deleting a Profile
- Applying a Current Profile

The profile editor allows you to create new or modify current profiles. See the Profile Configuration Using the Profile Editor for more information.

Adding a Profile

A new wIPS profile can be created using the default or a pre-configured profile.

Tip Tip To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we add more overview and technical presentations to enhance your learning.

To add a wIPS profile, follow these steps:

Step 1 Select **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.

Step 2 From the Select a command drop-down list, choose **Add Profile**.

Step 3 Click **Go**.

Step 4 Type a profile name in the Profile Name text box of the Profile Parameters page.

Step 5 Select the applicable pre-defined profile, or choose **Default** from the drop-down list. Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow

- Warehouse

Step 6 Select one of the following:

- Save—Saves the profiles to the Prime Infrastructure database with no changes and no Mobility Services Engine or controller assignments. The profile appears in the profile list.
- Save and Edit—Saves the profile and allows you to edit the profile.
- Cancel—Closes the Profile Parameters page without creating a profile.

Deleting a Profile

To delete a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.
Step 2 Select the check box of the wIPS profile(s) you want to delete.
Step 3 From the Select a command drop-down list, choose **Delete Profile**.
Step 4 Click **Go**.
Step 5 Click **OK** to confirm the deletion.

Note If the profile is already applied to a controller, it cannot be deleted.

Applying a Current Profile

Tip Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html. Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To apply a wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**. The page defaults to the wIPS Profiles > Profile List.
Step 2 Select the check box of the wIPS profile(s) you want to apply.
Step 3 From the Select a command drop-down list, choose **Apply Profile**.
Step 4 Click **Go**.
Step 5 Select the Mobility Services Engine(s) and controller(s) to which the profile is applied.

Note If the new assignment is different than the current assignment, you are prompted to save the profile with a different name

Step 6 When the applicable Mobility Services Engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected Mobility Services Engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

Configuring wIPS SSID Group List

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. You must know the SSID to join an 802.11 network. SSIDs can be associated with a wIPS profile as a group using the SSID group list feature.

An SSID group can be added to a profile by importing it from the Global SSID Group List page (Configure > wIPS Profiles > SSID Group List) or by adding one directly from the SSID Groups page.

This section contains the following topics:

- Global SSID Group List
- SSID Groups

Tip Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.htmlHere you will also find learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

Global SSID Group List

The SSID Group List page allows you to add or configure global SSID groups that you might later import into an applicable wIPS profile.

Tip Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.htmlHere you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

To access the SSID Group List page, choose **Configure > wIPS Profiles**. From the left sidebar menu, choose **SSID Group List**. The SSID Group List page display current SSID groups and their associated SSIDs.

This section contains the following topics:

- Adding a Group

Adding a Group

To add an SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.
Step 2 From the left sidebar menu, choose **SSID Group List**.
Step 3 From the Select a command drop-down list, choose **Add Group**.
Step 4 Click **Go**.
Step 5 In the SSID configuration page, type an SSID group name in the available text box.
Step 6 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a space.
Step 7 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.
- Cancel—Closes the SSID configuration page without saving the new SSID group.

Note To import the SSID groups to a profile, choose **Configure > wIPS Profile**. Click the profile name for the applicable profile to open the SSID Groups page. From the Select a command drop-down list, choose **Add Groups from Global List**. Select the check box(es) for the SSID group(s) you want to import and click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.
Step 2 From the left sidebar menu, choose **SSID Group List**.
Step 3 Select the check box of the SSID group that you want to edit.
Step 4 From the Select a command drop-down list, choose **Edit Group**.
Step 5 Click **Go**.
Step 6 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.
Step 7 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.
- Cancel—Closes the SSID configuration page without saving the changes.

Deleting a Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.
Step 2 From the left sidebar menu, choose **SSID Group List**.
Step 3 Select the check box of the SSID group(s) that you want to delete.
Step 4 From the Select a command drop-down list, choose **Delete Group**.
Step 5 Click **Go**.
Step 6 Click **OK** to confirm the deletion.

SSID Groups

The SSID Groups page is the first page displayed when you access the profile editor. This page displays SSID groups that are included for the current wIPS profile.

From this page, you can add, import, edit, or delete an SSID group for the current profile.

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html. Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

This section contains the following topics:

- Adding a Group
- Adding Groups from Your Global List
- Editing a Group
- Deleting Group

Adding a Group

To add an SSID Group to the current wIPS profile, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.
Step 2 From the left sidebar menu, choose **Profile List**.
Step 3 Click the profile name of the applicable wIPS profile.
Step 4 From the Select a command drop-down list, choose **Add Group**.
Step 5 Click **Go**.
Step 6 In the SSID configuration page, type an SSID group name in the available text box.
Step 7 Enter the SSIDs in the SSID List text box. Separate multiple SSIDs with a comma.
Step 8 When finished, select one of the following:

- Save—Saves the SSID group and adds it to the SSID Group List.
- Cancel—Closes the SSID configuration page without saving the new SSID group.

Adding Groups from Your Global List

SSID groups can also be added by importing them from your Global SSID Groups list. See the Global SSID Group List for more information on creating a global SSID groups list.

To import SSID groups into a profile, follow these steps:

Step 1 Select **Configure > wIPS Profile**.
Step 2 Click the profile name for the applicable profile to open the SSID Groups page.
Step 3 From the Select a command drop-down list, choose **Add Groups from Global List**.
Step 4 Select the check box(es) for the SSID group(s) you want to import.
Step 5 Click **Save**.

Editing a Group

To edit a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.
Step 2 From the left sidebar menu, choose **Profile List**.
Step 3 Click the profile name of the applicable wIPS profile.
Step 4 Select the check box of the SSID group that you want to edit.
Step 5 From the Select a command drop-down list, choose **Edit Group**.
Step 6 Click **Go**.
Step 7 In the SSID configuration page, make the necessary changes to the SSID group name or the SSID list.
Step 8 When finished, select one of the following:

- Save—Saves the current changes and closes the SSID configuration page.
- Cancel—Closes the SSID configuration page without saving the changes.

Deleting Group

To delete a current SSID Group, follow these steps:

Step 1 Choose **Configure > wIPS Profiles**.
Step 2 From the left sidebar menu, choose **Profile List**.
Step 3 Click the profile name of the applicable wIPS profile.
Step 4 Select the check box of the SSID group that you want to delete.
Step 5 From the Select a command drop-down list, choose **Delete Group**.
Step 6 Click **Go**.
Step 7 Click **OK** to confirm the deletion.

Profile Configuration Using the Profile Editor

Tip To learn more about Cisco Adaptive wIPS features and functionality, access the following URL: http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html. Here you also find learning modules for a variety of the Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

The profile editor allows you to configure profile details including the following:

- SSID groups—Add, edit, or delete SSID groups.
- Policy inclusion—Determine which policies are included in the profile.
- Policy level settings—Configure settings for each policy such as threshold, severity, notification type, and ACL/SSID groups.
- MSE/controller applications—Select the Mobility Services Engine(s) or controller(s) to which you want to apply the profile.

To configure profile details, follow these steps:

Step 1 Access the profile editor. This can be done in two ways:

- When creating a new profile, click **Save and Edit** in the Profile Parameters page.
- Click the profile name from the Profile List page.

Step 2 From the SSID Groups page, you can edit and delete current groups or add a new group. For more information on adding, editing, or deleting SSID groups, see the Configuring wIPS SSID Group List for more information.

Step 3 When SSID groups have been added or edited as needed, select one of the following:

- Save—Saves the changes made to the SSID groups.
- Cancel—Returns to the profile list with no changes made.
- Next—Proceeds to the Profile Configuration page.

Step 4 From the Profile Configuration page, you can determine which policies are included in the current profile. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. You can enable or disable an entire branch or an individual policy as needed by selecting the check box for the applicable branch or policy.

Note By default, all policies are selected.

Note For detailed information regarding each of the wIPS policies, see the wIPS Policy Alarm Encyclopedia.

Step 5 In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings.
The following options are available for each policy:

- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.

  Note There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.
- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

The following settings can be configured at the policy level:

- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

  Note Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.

  Note Threshold options vary based on the selected policy.

  Note Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

- Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
- Notification—Indicates the type of notification associated with the threshold.
- ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

  Note Only selected groups trigger the policy.

Step 6 When the profile configuration is complete, select one of the following:

- Save—Saves the changes made to the current profile.
- Cancel—Returns to the profile list with no changes made.
- Back—Returns to the SSID Groups page.
- Next—Proceeds to the MSE/Controller(s) page.

Step 7 In the Apply Profile page, select the check box(es) of the Mobility Services Engine and controller(s) to which you want to apply the current profile.

Step 8 When the applicable Mobility Services Engine(s) and controller(s) are selected, choose one of the following:

- Apply—Applies the current profile to the selected Mobility Services Engine/controller(s).
- Cancel—Returns to the profile list with no changes made.

  Note A created profile can also be applied directly from the profile list. From the Profile List page, select the check box of the profile you want to apply and click **Apply Profile** from the Select a command drop-down list. Click **Go** to access the Apply Profile page.