Configuring Cisco Intrusion Detection System

- Information About Cisco Intrusion Detection System, page 1
- Configuring IDS Sensors (GUI), page 2
- Viewing Shunned Clients (GUI), page 2
- Configuring IDS Sensors (CLI), page 3
- Viewing Shunned Clients (CLI), page 4

Information About Cisco Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. 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 potential attacks:

- IDS sensors
- IDS signatures

You can configure IDS sensors to detect various types of IP-level attacks in your network. When the sensors identify an attack, they can 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 controller can query the sensor to get the list of shunned clients.

Shunned Clients

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client. The shun entry is distributed to all controllers within the same mobility group. If the client to be shunned is currently joined to a controller in this mobility group, the anchor controller adds this client to the dynamic exclusion list, and the foreign controller removes the client. The next time that the client tries to connect to a controller, the anchor controller rejects the handoff and informs the foreign controller that the client is being excluded.
Configuring IDS Sensors (GUI)

Step 1 Choose Security > Advanced > CIDS > Sensors to open the CIDS Sensors List page.
Note If you want to delete an existing sensor, hover your cursor over the blue drop-down arrow for that sensor and choose Remove.

Step 2 Click New to add a new IDS sensor to the list. The CIDS Sensor Add page is displayed.

Step 3 From the Index drop-down list, choose a number (between 1 and 5) to determine the sequence in which the controller consults the IDS sensors. For example, if you choose 1, the controller consults this IDS sensor first. Cisco WLC supports up to five IDS sensors.

Step 4 In the Server Address text box, enter the IP address of your IDS server.

Step 5 In the Port text box, enter the number of the HTTPS port through which the controller has to communicate with the IDS sensor. We recommend that you set this parameter to 443 because the sensor uses this value to communicate by default. The default value is 443 and the range is 1 to 65535.

Step 6 In the Username text box, enter the name that the controller uses to authenticate to the IDS sensor. This username must be configured on the IDS sensor and have at least a read-only privilege.

Step 7 In the Password and Confirm Password text boxes, enter the password that the controller uses to authenticate to the IDS sensor.

Step 8 In the Query Interval text box, enter the time (in seconds) for how often the controller should query the IDS server for IDS events. The default is 60 seconds and the range is 10 to 3600 seconds.

Step 9 Check the State check box to register the controller with this IDS sensor or uncheck this check box to disable registration. The default value is disabled.

Step 10 Enter a 40-hexadecimal-character security key in the Fingerprint text box. This key is used to verify the validity of the sensor and is used to prevent security attacks.
Note Make sure you include colons that appear between every two bytes within the key. For example, enter AA:BB:CC:DD.

Step 11 Click Apply. Your new IDS sensor appears in the list of sensors on the CIDS Sensors List page.

Step 12 Click Save Configuration.

Viewing Shunned Clients (GUI)

Step 1 Choose Security > Advanced > CIDS > Shunned Clients to open the CIDS Shun List page. This page shows the IP address and MAC address of each shunned client, the length of time that the client’s data packets should be blocked by the controller as requested by the IDS sensor, and the IP address of the IDS sensor that discovered the client.
Step 2  Click **Re-sync** to purge and reset the list as desired.

**Note**  The controller does not take any action on shun entries when the corresponding timers have expired. The shun entry timers are maintained only for the display purpose. The shun entries are cleaned up whenever the controller polls the IPS server. If the CIDS IPS server is not reachable, the shun entries are not removed even if they are timed out on the controller. The shun entries are cleaned up only when the CIDS IPS server is operational again and the controller polls the CIDS IPS server.

---

### Configuring IDS Sensors (CLI)

**Step 1**  Add an IDS sensor by entering this command:

```
config wps cids-sensor add index ids_ip_address username password
```

The index parameter determines the sequence in which the controller consults the IDS sensors. The controller supports up to five IDS sensors. Enter a number (between 1 and 5) to determine the priority of this sensor. For example, if you enter 1, the controller consults this IDS sensor first.

**Note**  The username must be configured on the IDS sensor and have at least a read-only privilege.

**Step 2**  (Optional) Specify the number of the HTTPS port through which the controller is to communicate with the IDS sensor by entering this command:

```
config wps cids-sensor port index port
```

For the port-number parameter, you can enter a value between 1 and 65535. The default value is 443. This step is optional because we recommend that you use the default value of 443. The sensor uses this value to communicate by default.

**Step 3**  Specify how often the controller should query the IDS server for IDS events by entering this command:

```
config wps cids-sensor interval index interval
```

For the interval parameter, you can enter a value between 10 and 3600 seconds. The default value is 60 seconds.

**Step 4**  Enter a 40-hexadecimal-character security key used to verify the validity of the sensor by entering this command:

```
config wps cids-sensor fingerprint index sha1 fingerprint
```

You can get the value of the fingerprint by entering `show tls fingerprint` on the sensor's console.

**Note**  Make sure to include the colons that appear between every two bytes within the key (for example, AA:BB:CC:DD).

**Step 5**  Enable or disable this controller’s registration with an IDS sensor by entering this command:

```
config wps cids-sensor {enable | disable} index
```

**Step 6**  Enable or disable protection from DoS attacks by entering this command:

```
config wps cids-sensor {enable | disable}
```

The default value is disabled.

**Note**  A potential attacker can use specially crafted packets to mislead the IDS into treating a legitimate client as an attacker. It causes the controller to wrongly disconnect this legitimate client and launches a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

**Step 7**  Save your settings by entering this command:

```
save config
```

**Step 8**  See the IDS sensor configuration by entering one of these commands:
Step 9  The second command provides more information than the first.

Step 10 See the auto-immune configuration setting by entering this command:
show wps summary

Information similar to the following appears:

Auto-Immune
Auto-Immune......................... Disabled

Client Exclusion Policy
Excessive 802.11-association failures........ Enabled
Excessive 802.11-authentication failures....... Enabled
Excessive 802.1x-authentication............... Enabled
IP-theft.................................. Enabled
Excessive Web authentication failure.......... Enabled

Signature Policy
Signature Processing......................... Enabled

Step 11 Obtain debug information regarding IDS sensor configuration by entering this command:
debug wps cids enable

Note  If you ever want to delete or change the configuration of a sensor, you must first disable it by entering the config
wps cids-sensor disable index command. To delete the sensor, enter the config wps cids-sensor delete index
command.

Viewing Shunned Clients (CLI)

Step 1  View the list of clients to be shunned by entering this command:
show wps shun-list

Step 2  Force the controller to synchronize with other controllers in the mobility group for the shun list by entering this command:
config wps shun-list re-sync

Note  The controller does not take any action on shun entries when the corresponding timers have expired. The shun
entry timers are maintained only for the display purpose. The shun entries are cleaned up whenever the controller polls the IPS server. If the CIDS IPS server is not reachable, the shun entries are not removed even if they are timed out on the controller. The shun entries are cleaned up only when the CIDS IPS server is operational again and the controller polls the CIDS IPS server.