Wireless LAN Controller and IPS Integration Guide

Document ID: 71231

Contents

Introduction

The Cisco Unified Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) is part of the Cisco Self−Defending Network and is the first integrated wired and wireless security solution in the industry. The Cisco Unified IDS/IPS takes a comprehensive approach to security at the wireless edge, wired edge, WAN edge, and through the data center. When an associated client sends malicious traffic through the Cisco Unified Wireless Network, a Cisco wired IDS device detects the attack and sends shun requests to Cisco Wireless LAN Controllers (WLCs), which then disassociate the client device.

The Cisco IPS is an inline, network−based solution, designed to accurately identify, classify, and stop malicious traffic, including worms, spyware / adware, network viruses, and application abuse, before they affect business continuity.

With the utilization of Cisco IPS Sensor software version 5, the Cisco IPS solution combines inline prevention services with innovative technologies to improve accuracy. The result is total confidence in the provided protection of your IPS solution, without the fear of legitimate traffic being dropped. The Cisco IPS solution also offers comprehensive protection of your network through its unique ability to collaborate with other network security resources and provides a proactive approach to the protection of your network.

The Cisco IPS solution helps users stop more threats with greater confidence through the use of these features:

- **Accurate inline prevention technologies** Provides unparalleled confidence to take preventive action against a broader range of threats without the risk of dropping legitimate traffic. These unique technologies offer intelligent, automated, contextual analysis of your data and help ensure that you receive the most out of your intrusion prevention solution.
- **Multi−vector threat identification** Protects your network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7.
- **Unique network collaboration** Enhances scalability and resiliency through network collaboration, including efficient traffic capture techniques, load−balancing capabilities, and visibility into encrypted traffic.
- **Comprehensive deployment solutions** Provides solutions for all environments, from small and medium−sized businesses (SMBs) and branch office locations to large enterprise and service provider installations.
- **Powerful management, event correlation, and support services** Enables a complete solution, including configuration, management, data correlation, and advanced support services. In particular the Cisco Security Monitoring, Analysis, and Response System (MARS) identifies, isolates, and recommends precision removal of offending elements, for a network wide intrusion prevention solution. And the Cisco Incident Control System prevents new worm and virus outbreaks by enabling the network to rapidly adapt and provide a distributed response.

When combined, these elements provide a comprehensive inline prevention solution and give you the confidence to detect and stop the broadest range of malicious traffic before it affects business continuity. The Cisco Self−Defending Network initiative calls for integrated and built−in security for network solutions. Current Lightweight Access Point Protocol (LWAPP)−based WLAN systems only supports basic IDS features due to the fact that it is essentially a Layer 2 system and it has limited line−processing power. Cisco releases new code in a timely manner to include new enhanced features into the new codes. Release 4.0 has the latest features that include the integration of an LWAPP−based WLAN system with the Cisco IDS/IPS product line. In this release, the goal is to allow the Cisco IDS/IPS system to instruct the WLCs to block certain clients from access to wireless networks when an attack is detected anywhere from Layer 3 through Layer 7 that involves the client in consideration.

Prerequisites

Requirements

Ensure that you meet these minimum requirements:

- WLC firmware version 4.x and later
- Knowledge on how to configure Cisco IPS and the Cisco WLC is desirable.

Components Used

Cisco WLC

These controllers are included with software release 4.0 for IDS modifications:

- Cisco 2000 Series WLC
- Cisco 2100 Series WLC
- Cisco 4400 Series WLC
- Cisco Wireless Services Module (WiSM)
- Cisco Catalyst 3750G Series Unified Access Switch
- Cisco Wireless LAN Controller Module (WLCM)

Access Points

- Cisco Aironet 1100 AG Series Lightweight Access Points
- Cisco Aironet 1200 AG Series Lightweight Access Points
- Cisco Aironet 1300 Series Lightweight Access Points
- Cisco Aironet 1000 Series Lightweight Access Points

Management

- Cisco Wireless Control System (WCS)
- Cisco 4200 Series Sensor
- Cisco IDS Management − Cisco IDS Device Manager (IDM)

Cisco Unified IDS/IPS Platforms

- Cisco IPS 4200 Series Sensors with Cisco IPS Sensor Software 5.x or later.
- SSM10 and SSM20 for the Cisco ASA 5500 Series Adaptive Security Appliances with Cisco IPS Sensor Software 5.x
- Cisco ASA 5500 Series Adaptive Security Appliances with Cisco IPS Sensor Software 5.x
- Cisco IDS Network Module (NM−CIDS) with Cisco IPS Sensor Software 5.x
- Cisco Catalyst 6500 Series Intrusion Detection System Module 2 (IDSM−2) with Cisco IPS Sensor Software 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

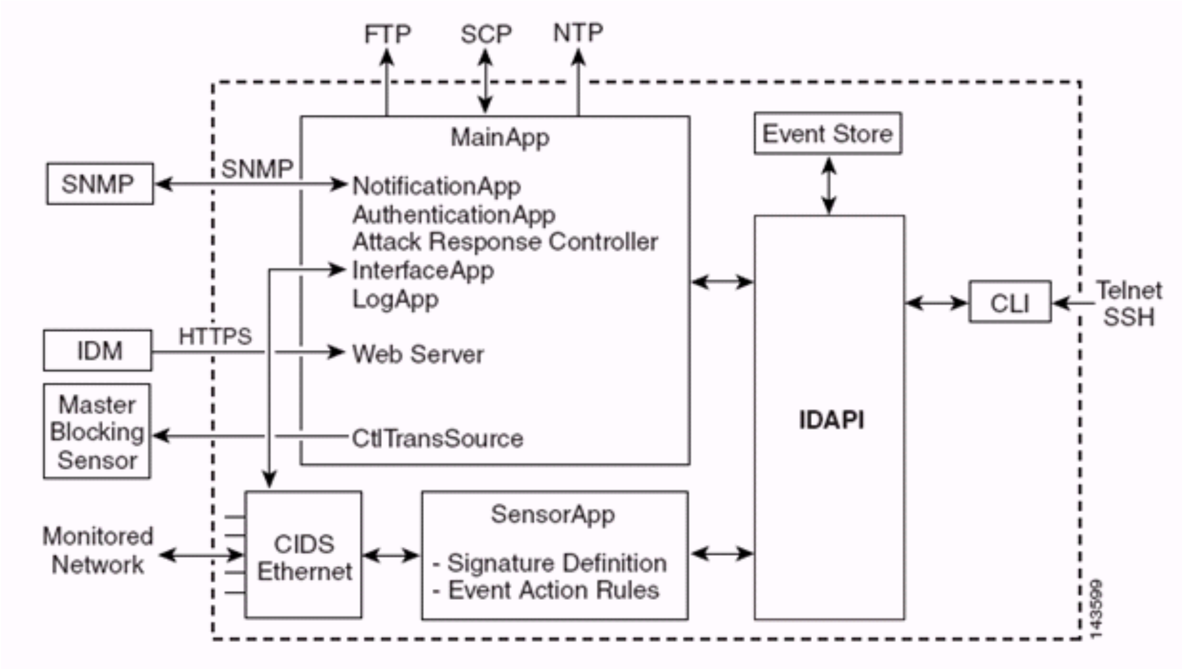
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Cisco IDS Overview

The major components of the Cisco IDS (Version 5.0) are:

- **Sensor App** Performs packet capture and analysis.
- **Event Storage Management and Actions Module** Provides storage of policy violations.
- **Imaging, Install and Startup Module** Loads, initializes, and starts all the system software.
- **User Interfaces and UI Support Module** Provides an embedded CLI and the IDM.
- **Sensor OS** Host operating system (based on Linux).



The Sensor Application (IPS software) consists of:

- **Main App** Initializes the system, starts and stops other applications, configures the OS and is responsible for upgrades. It contains these components:
    - ♦ **Control Transaction Server** Allows the Sensors to send control transactions which are used to enable the Attack Response Controller (formerly known as Network Access Controller) Master Blocking Sensor capability.
    - ♦ **Event Store** An indexed store used to store IPS events (errors, status and alert system messages) that is accessible through the CLI, IDM, Adaptive Security Device Manager (ASDM), or Remote Data Exchange Protocol (RDEP).
- **Interface App** Handles bypass and physical settings and defines paired interfaces. Physical settings consist of speed, duplex, and administrative states.
- **Log App** Writes the log messages of the application to the log file and the error messages to the Event Store.
- **Attack Response Controller (ARC) (formerly known as Network Access Controller)** Manages remote network devices (firewalls, routers, and switches) to provide blocking capabilities when an alert event has occurred. ARC creates and applies access control lists (ACLs) on the controlled network device or uses the **shun** command (firewalls).
- **Notification App** Sends SNMP traps when triggered by an alert, status, and error events. The Notification App uses a public domain SNMP agent in order to this. The SNMP GETs provide information about the health of a Sensor.
    - ♦ **Web Server (HTTP RDEP2 server)** Provides a web user interface. It also provides a means to communicate with other IPS devices through RDEP2 using several servlets to provide IPS services.
    - ♦ **Authentication App** Verifies that users are authorized to perform CLI, IDM, ASDM, or RDEP actions.
- **Sensor App (Analysis Engine)** Performs packet capture and analysis.
- **CLI** The interface that is run when users successfully log in to the Sensor through Telnet or SSH. All accounts created through the CLI use the CLI as their shell (except the service account − only one service account is allowed). Allowed CLI commands depend on the privilege of the user.

All IPS applications communicate with each other through a common Application Program Interface (API) called IDAPI. Remote applications (other Sensors, management applications, and third−party software) communicate with Sensors through RDEP2 and Security Device Event Exchange (SDEE) protocols.

It must be noted that the Sensor has these disk partitions:

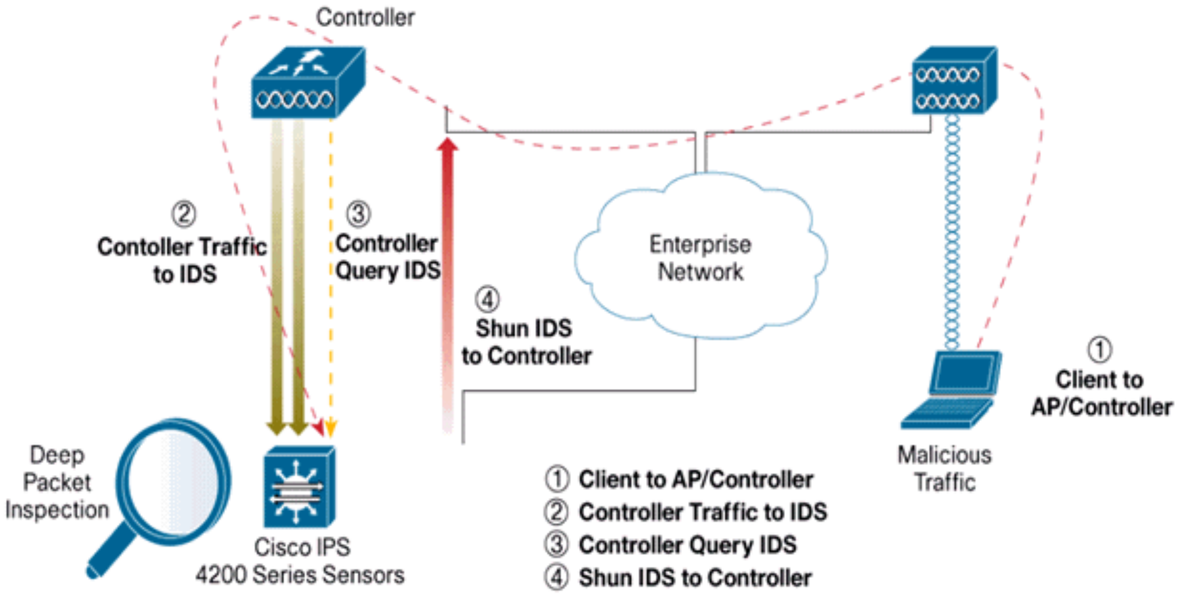
- **Application Partition** Contains the full IPS system image.
- **Maintenance Partition** A special purpose IPS image used to re−image the application partition of the IDSM−2. A re−image of the maintenance partition results in lost configuration settings.
- **Recovery Partition** A special purpose image used for recovery of the Sensor. Booting into the recovery partition enables users to completely re−image the application partition. Network settings are preserved, but all other configurations are lost.

Cisco IDS and WLC Integration Overview

Version 5.0 of the Cisco IDS introduces the ability to configure deny actions when policy violations (signatures) are detected. Based on user configuration at the IDS/IPS system, a shun request can be sent to a firewall, router, or WLC in order to block the packets from a particular IP address.

With the Cisco Unified Wireless Network Software Release 4.0 for Cisco Wireless Controllers, a shun request needs to be sent to a WLC in order to trigger the client blacklisting or exclusion behavior available on a controller. The interface the controller uses to get the shun request is the command and control interface on the Cisco IDS.

- The controller allows up to five IDS Sensors to be configured on a given controller.
- Each configured IDS Sensor is identified by its IP address or qualified network name and authorization credentials.
- Each IDS Sensor can be configured on a controller with a unique query rate in seconds.



IDS Shunning

The controller queries the Sensor at the configured query rate in order to retrieve all the shun events. A given shun request is distributed throughout the entire mobility group of the controller that retrieves the request from the IDS Sensor. Each shun request for a client IP address is in effect for the specified timeout seconds value. If the timeout value indicates an infinite time, then the shun event ends only if the shun entry is removed on the IDS. The shunned client status is maintained on each controller in the mobility group even if any or all of the controllers are reset.

Note: The decision to shun a client is always made by the IDS Sensor. The controller does not detect Layer 3 attacks. It is a far more complicated process to determine that the client is launching a malicious attack at Layer 3. The client is authenticated at Layer 2 which is good enough for the controller to grant Layer 2 access.

Note: For example, if a client gets a previous offending (shunned) IP address assigned, it is up to the Sensor timeout to unblock the Layer 2 access for this new client. Even if the controller gives access at Layer 2, the client traffic might be blocked at routers in Layer 3 anyway, because the Sensor also informs routers of the shun event.

Assume that a client has IP address A. Now, when the controller polls the IDS for shun events, the IDS sends the shun request to the controller with IP address A as the target IP address. Now, the controller black lists this client A. On the controller, clients are disabled based on a MAC address.

Now, assume that the client changes its IP address from A to B. During the next poll, the controller gets a list of shunned clients based on IP address. This time again, IP address A is still in the shunned list. But since the client has changed its IP address from A to B (which is not in the shunned list of IP addresses), this client with a new IP address of B is released once the timeout of black listed clients is reached on the controller. Now, the controller starts to allow this client with new the IP address of B (but the client MAC address remains the same).

Therefore, although a client remains disabled for the duration of the controller exclusion time and is re−excluded if it re−acquires its previous DHCP address, that client is no longer disabled if the IP address of the client that is shunned changes. For example, if the client connects to the same network and the DHCP lease timeout is not expired.

Controllers only support connection to the IDS for client shunning requests that use the management port on the controller. The controller connects to the IDS for packet inspection via the applicable VLAN interfaces that carry wireless client traffic.

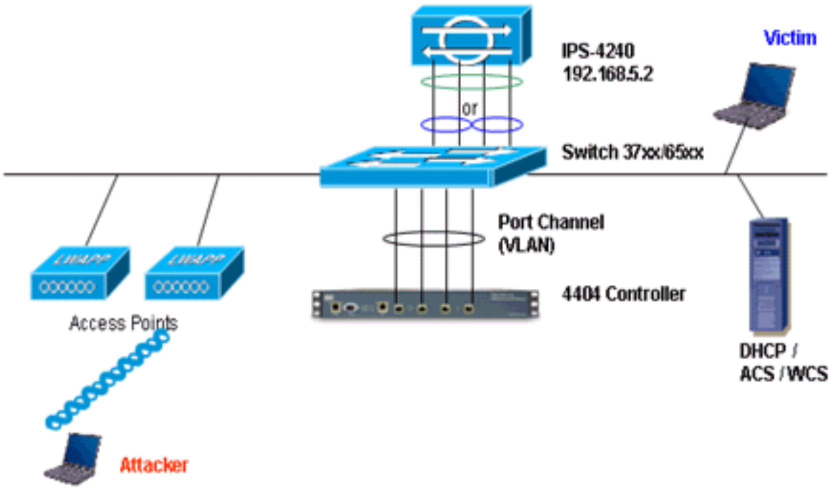
On the controller, the Disable Clients page shows each client that has been disabled via an IDS Sensor request. The CLI **show** command also displays a list of blacklisted clients.

On the WCS, the excluded clients are displayed under the Security sub tab.

Here are the steps to follow in order to complete the integration of Cisco IPS Sensors and Cisco WLCs.

1. Install and connect the IDS appliance on the same switch where the wireless controller resides.
2. Mirror (SPAN) the WLC ports that carry the wireless client traffic to the IDS appliance.
3. The IDS appliance receives a copy of every packet and inspects traffic at Layer 3 through 7.
4. The IDS appliance offers a downloadable signature file, which can also be customized.
5. The IDS appliance generates the alarm with an event action of shun when an attack signature is detected.
6. The WLC polls the IDS for alarms.
7. When an alarm with the IP address of a wireless client, which is associated to the WLC, is detected, it puts the client into the exclusion list.
8. A trap is generated by the WLC and WCS is notified.
9. The user is removed from the exclusion list after the specified time period.

Network Architecture Design



The Cisco WLC is connected to the gigabit interfaces on the Catalyst 6500. Create a port−channel for the gigabit interfaces and enable Link Aggregation (LAG) on the WLC.

```
(Cisco Controller) >show interface summary

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr
-------------------------------- ---- -------- --------------- ------- ------
ap−manager                       LAG  untagged 10.10.99.3      Static  Yes
management                       LAG  untagged 10.10.99.2      Static  No
service−port                     N/A  N/A      192.168.1.1     Static  No
virtual                          N/A  N/A      1.1.1.1         Static  No
vlan101                          LAG  101      10.10.101.5     Dynamic No
```

The controller is connected to interface gigabit 5/1 and gigabit 5/2 on the Catalyst 6500.

```
cat6506#show run interface gigabit 5/1
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel−group 99 mode on
end

cat6506#show run interface gigabit 5/2
Building configuration...

Current configuration : 183 bytes
!
interface GigabitEthernet5/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
 channel−group 99 mode on
end
```

```
cat6506#show run interface port−channel 99
Building configuration...

Current configuration : 153 bytes
!
interface Port−channel99
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 99
 switchport mode trunk
 no ip address
end
```

The sensing interfaces of the IPS Sensor can operate individually in **Promiscuous mode** or you can pair them to create inline interfaces for **Inline Sensing mode**.

In Promiscuous mode, packets do not flow through the Sensor. The Sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating in Promiscuous mode is that the Sensor does not affect the packet flow with the forwarded traffic.

Note: The architecture diagram is just an example setup of WLC and IPS integrated architecture. The example configuration shown here explains the IDS sensing interface acting in Promiscuous mode. The architecture diagram shows the sensing interfaces being paired together to act in Inline Pair mode. Refer to Inline Mode for more information about Inline Interface mode.

In this configuration, it is assumed that the sensing interface acts in Promiscuous mode. The monitoring interface of the Cisco IDS Sensor is connected to the gigabit interface 5/3 on the Catalyst 6500. Create a monitor session on the Catalyst 6500 where the port−channel interface is the source of the packets and the destination is the gigabit interface where the monitoring interface of the Cisco IPS Sensor is connected. This replicates all ingress and egress traffic from the controller wired interfaces to the IDS for Layer 3 through Layer 7 inspection.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3

cat6506#show monitor session 5
Session 5
−−−−−−−−−
Type                   : Local Session
Source Ports           :
    Both               : Po99
Destination Ports      : Gi5/3
cat6506#
```

Configure the Cisco IDS Sensor

The initial configuration of the Cisco IDS Sensor is done from the console port or by connecting a monitor and keyboard to the Sensor.

1. Log in to the appliance:

    a. Connect a console port to the Sensor.
    b. Connect a monitor and a keyboard to the Sensor.
2. Type your username and password at the login prompt.

Note: The default username and password are both cisco. You are prompted to change them the first time you log in to the appliance. You must first enter the UNIX password, which is cisco. Then you must enter the new password twice.

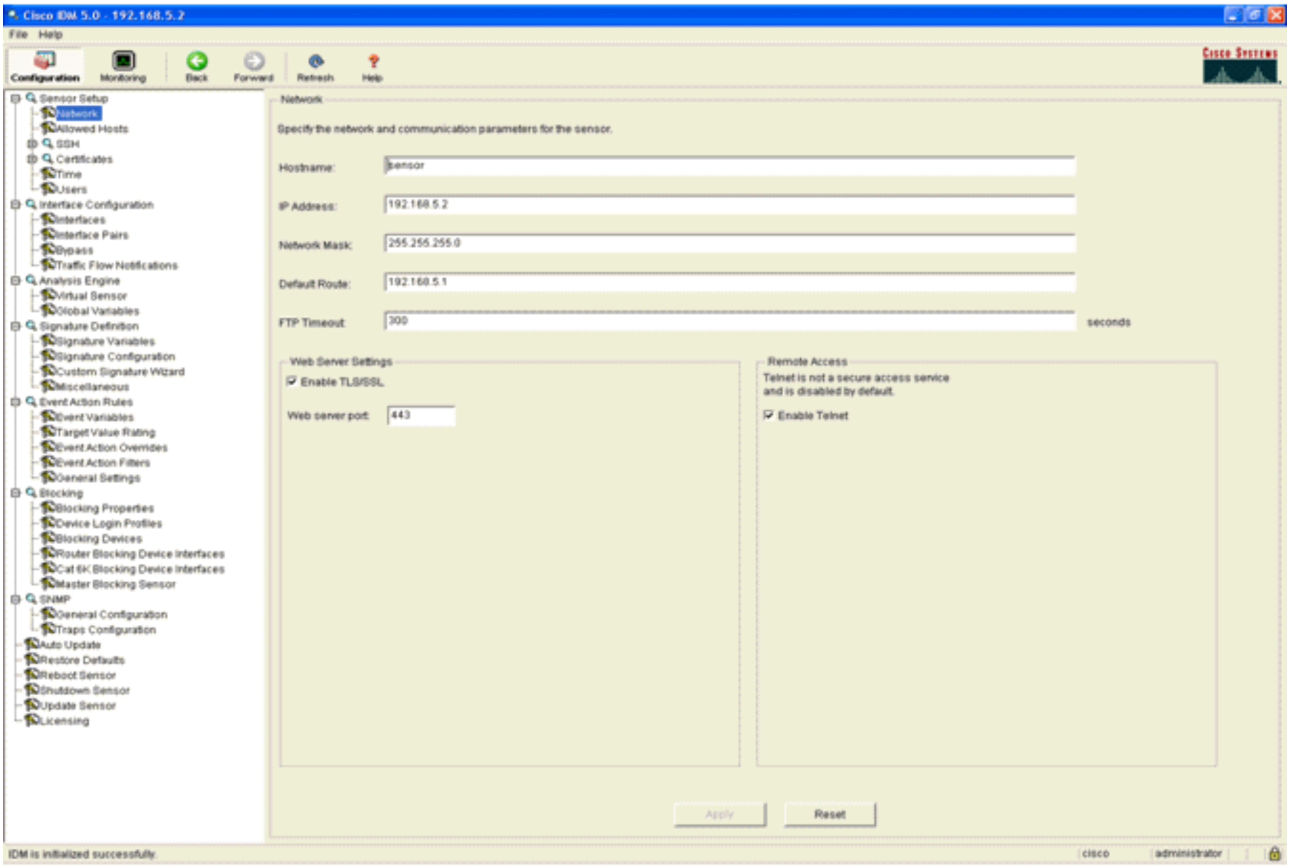
```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws.
By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may
be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending
email to export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet
           (registered customers only)

to obtain a new license or install a license.
```

3. Configure the IP address, subnet mask and access list on the Sensor.

   Note: This is the command and control interface on the IDS used to communicate with the controller. This address should be routable to the controller management interface. The sensing interfaces do not require addressing. The access list should include the controller(s) management interface address, as well as allowable addresses for management of the IDS.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes:?[yes]: yes
sensor(config)#exit
sensor#
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.6/1.0 ms
sensor#
```

4. You can now configure the IPS Sensor from the GUI. Point the browser to the management IP address of the Sensor. This image displays a sample where the Sensor is configured with 192.168.5.2..



Network

Specify the network and communication parameters for the sensor.

Hostname: sensor

IP Address: 192.168.5.2

Network Mask: 255.255.255.0

Default Route: 192.168.5.1

FTP Timeout: 300 seconds

Web Server Settings

☑ Enable TLS/SSL

Web server port: 443

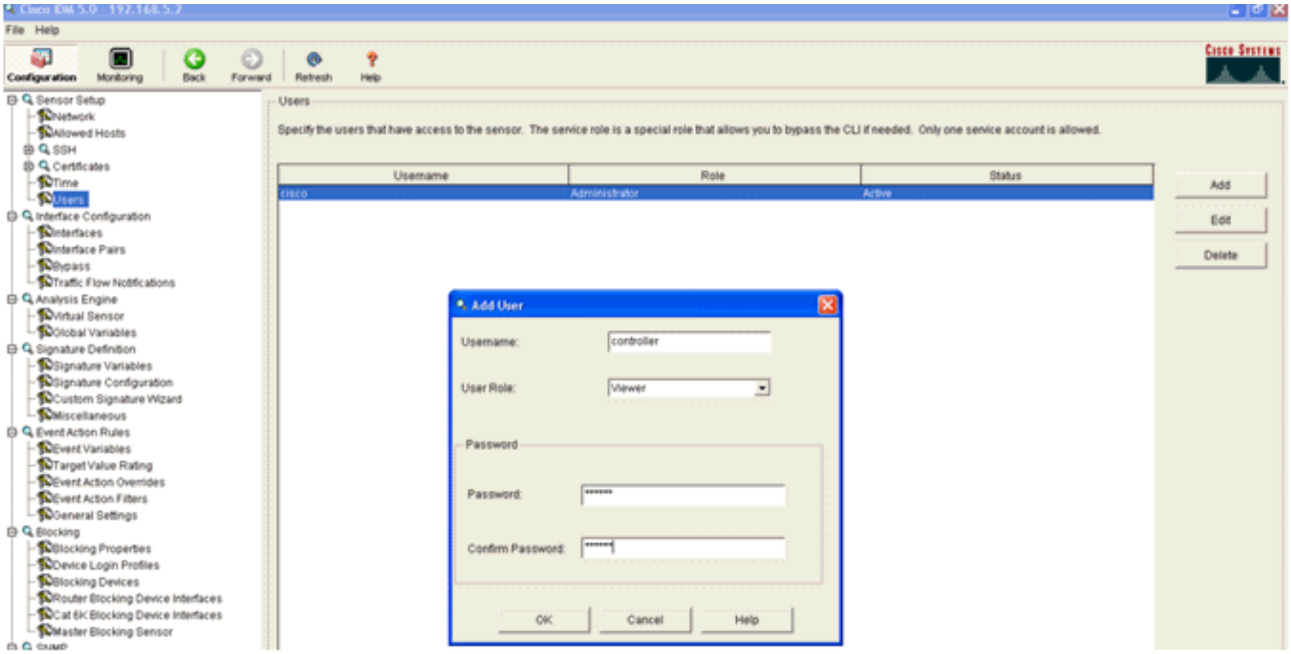
Remote Access

Telnet is not a secure access service and is disabled by default.

☑ Enable Telnet

IDM is initialized successfully. cisco administrator

5. Add a user that the WLC uses to access the IPS Sensor events.



Users

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
cisco	Administrator	Active

Add User

Username: controller

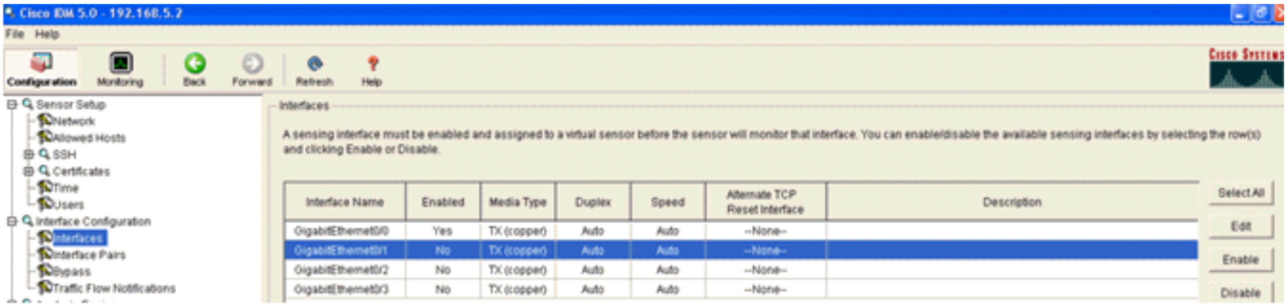
User Role: Viewer

Password

Password: *******

Confirm Password: *******

6. Enable the monitoring interfaces.

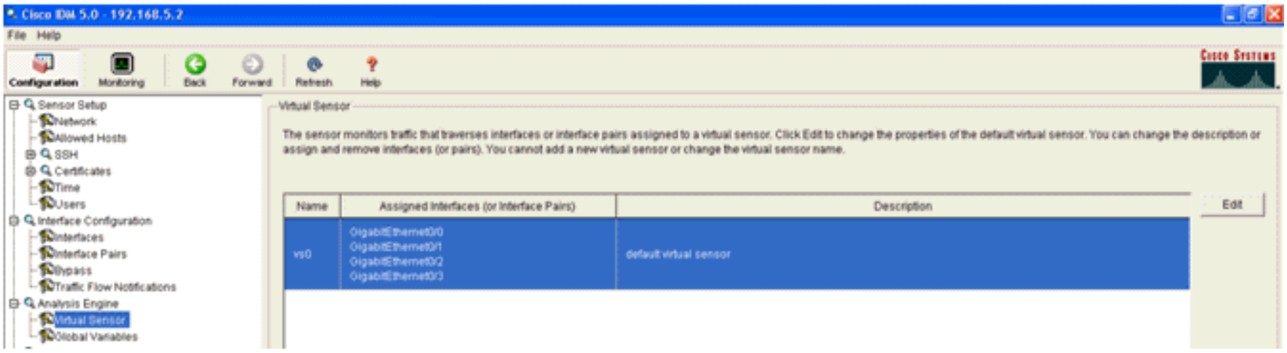


Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Media Type	Duplex	Speed	Alternate TCP Reset Interface	Description
GigabitEthernet0/0	Yes	TX (copper)	Auto	Auto	--None--	
GigabitEthernet0/1	No	TX (copper)	Auto	Auto	--None--	
GigabitEthernet0/2	No	TX (copper)	Auto	Auto	--None--	
GigabitEthernet0/3	No	TX (copper)	Auto	Auto	--None--	

The monitoring interfaces must be added to the Analysis Engine, as this window shows:

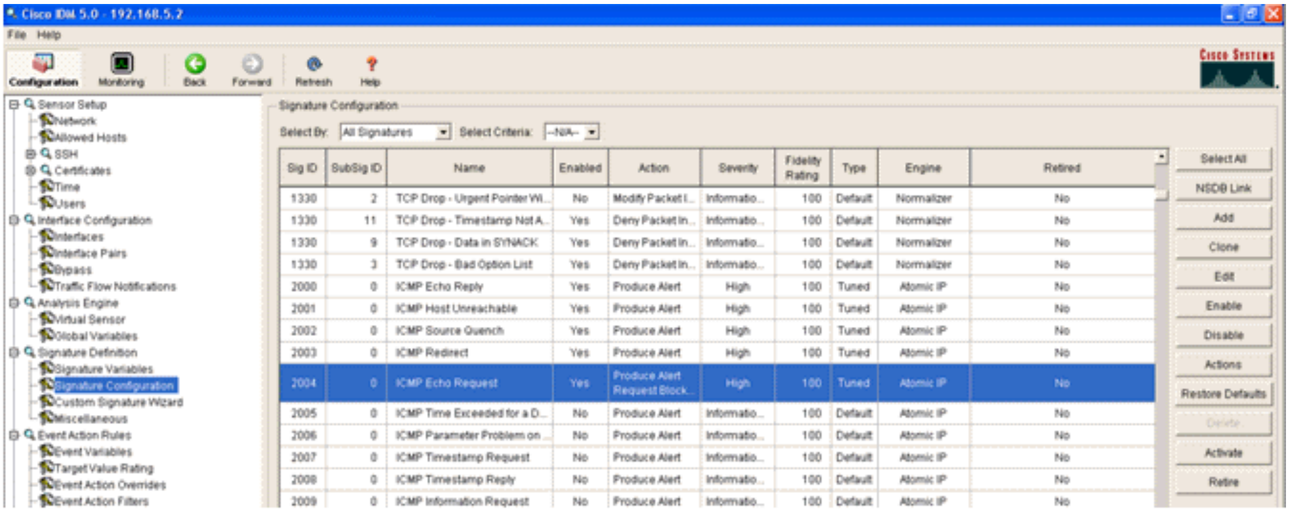


Virtual Sensor

The sensor monitors traffic that traverses interfaces or interface pairs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the description or assign and remove interfaces (or pairs). You cannot add a new virtual sensor or change the virtual sensor name.

Name	Assigned Interfaces (or Interface Pairs)	Description
vs0	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	default virtual sensor

7. Select the 2004 signature (ICMP Echo Request) in order to perform a quick setup verification.

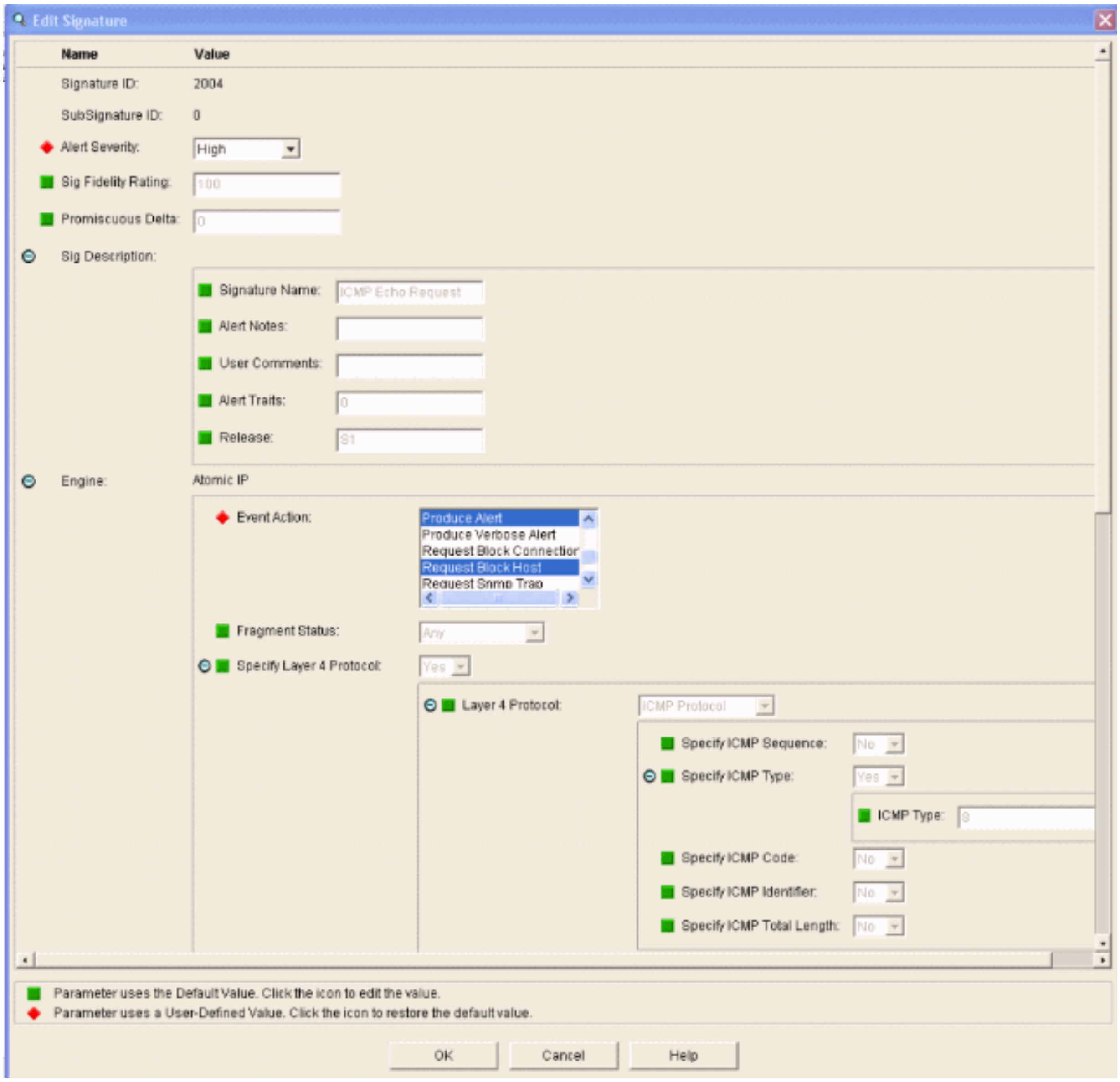


Signature Configuration

Select By: All Signatures Select Criteria: --N/A--

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired
1330	2	TCP Drop - Urgent Pointer Wi...	No	Modify Packet I...	Informatio...	100	Default	Normalizer	No
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2004	0	ICMP Echo Request	Yes	Produce Alert Request Block...	High	100	Tuned	Atomic IP	No
2005	0	ICMP Time Exceeded for a D...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2006	0	ICMP Parameter Problem on ...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2009	0	ICMP Information Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No

The signature should be enabled, Alert Severity set to **High** and Event Action set to **Produce Alert** and **Request Block Host** for this verification step to be completed.



Name	Value
Signature ID:	2004
SubSignature ID:	0
🟥 Alert Severity:	High
🟩 Sig Fidelity Rating:	100
🟩 Promiscuous Delta:	0
Sig Description:	
🟩 Signature Name:	ICMP Echo Request
🟩 Alert Notes:	
🟩 User Comments:	
🟩 Alert Traits:	0
🟩 Release:	S1
Engine:	Atomic IP
🟥 Event Action:	Produce Alert Produce Verbose Alert Request Block Connection Request Block Host Request Snmp Trap
🟩 Fragment Status:	Any
🟩 Specify Layer 4 Protocol:	Yes
🟩 Layer 4 Protocol:	ICMP Protocol
🟩 Specify ICMP Sequence:	No
🟩 Specify ICMP Type:	Yes
🟩 ICMP Type:	8
🟩 Specify ICMP Code:	No
🟩 Specify ICMP Identifier:	No
🟩 Specify ICMP Total Length:	No

🟩 Parameter uses the Default Value. Click the icon to edit the value.

🟥 Parameter uses a User-Defined Value. Click the icon to restore the default value.

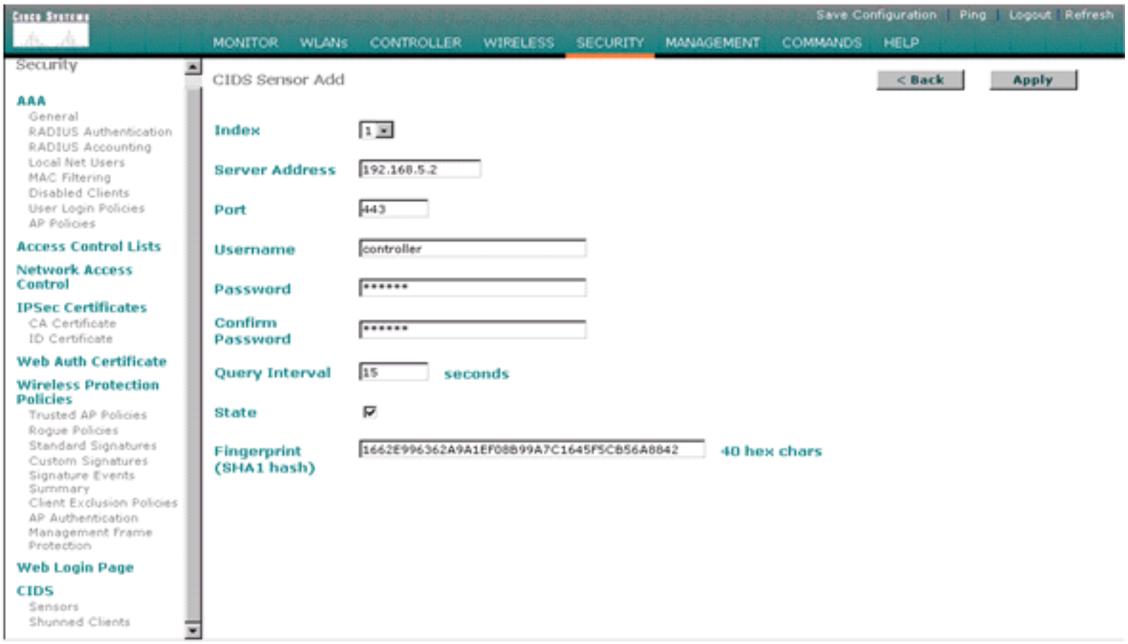
Configure the WLC

Complete these steps in order to configure the WLC:

1. Once the IPS appliance is configured and ready to be added in the controller, choose **Security** > **CIDS** > **Sensors** > **New**.
2. Add the IP address, TCP port number, username and password you previously created.

   In order to obtain the fingerprint from the IPS Sensor, execute this command in the IPS Sensor and add the SHA1 fingerprint on the WLC (without the colon). This is used to secure the controller−to−IDS polling communication.

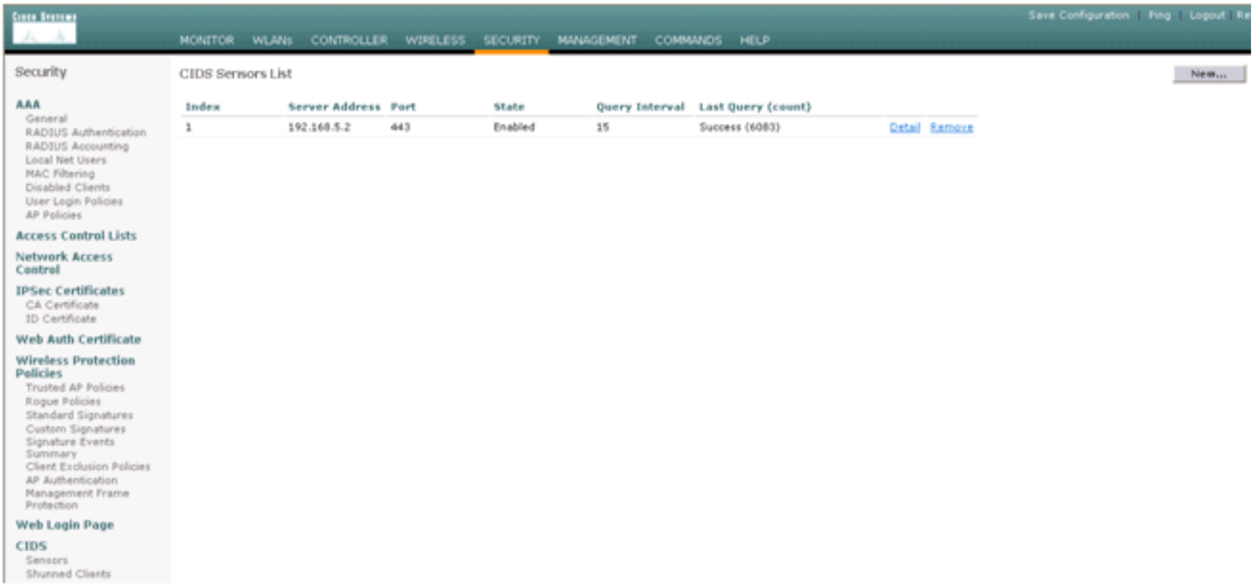
   ```
   sensor#show tls fingerprint
   MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
   SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
   ```



CIDS Sensor Add

Index	1
Server Address	192.168.5.2
Port	443
Username	controller
Password	******
Confirm Password	******
Query Interval	15 seconds
State	☑
Fingerprint (SHA1 hash)	1662E996362A9A1EF08B99A7C1645F5CB56A8842 40 hex chars

3. Check the status of the connection between the IPS Sensor and the WLC.

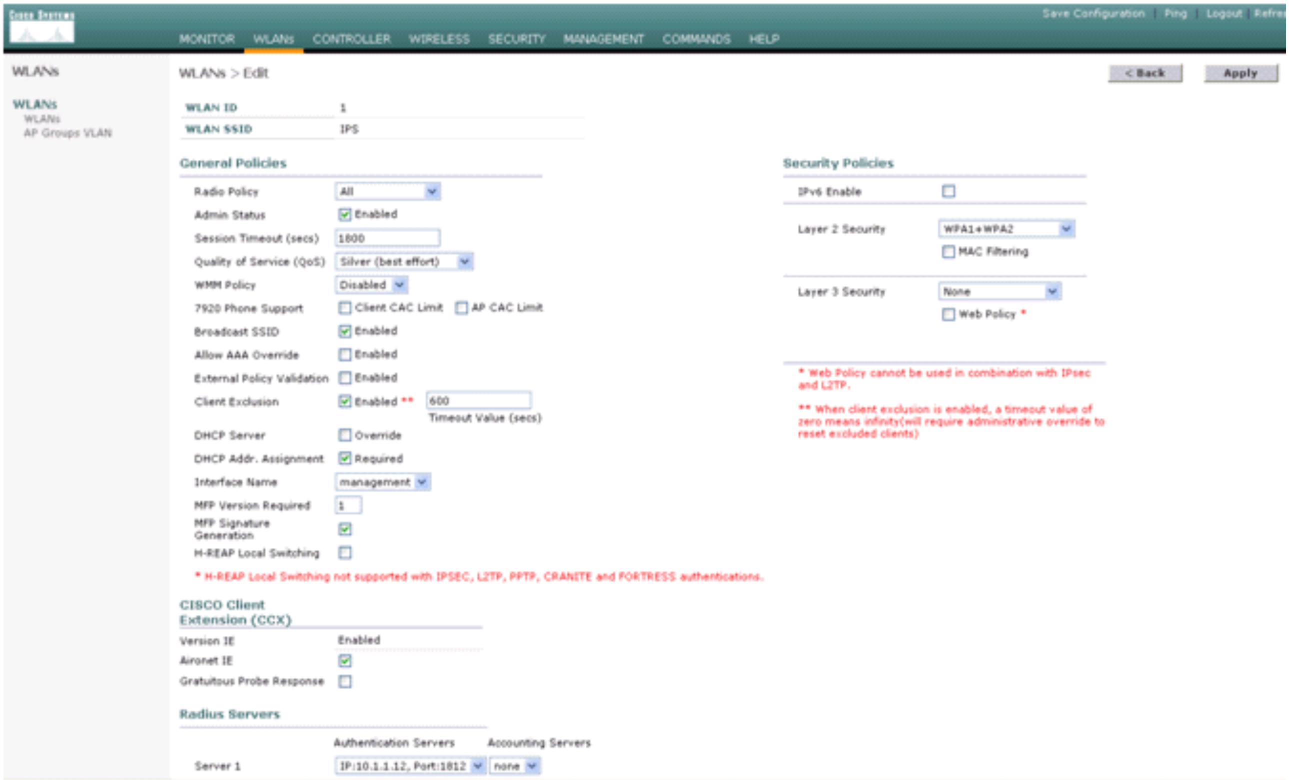


CIDS Sensors List

Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Success (6083)	Detail Remove

4. Once you establish the connectivity with the Cisco IPS Sensor, make sure the WLAN configuration is correct and that you enable **Client Exclusion**.

   The default client exclusion timeout value is 60 seconds. Also note that regardless of the client exclusion timer, the client exclusion persists as long as the client block invoked by the IDS remains active. The default block time in the IDS is 30 minutes.



WLANs > Edit

WLAN ID 1
WLAN SSID IPS

General Policies

Radio Policy: All
Admin Status: ☑ Enabled
Session Timeout (secs): 1800
Quality of Service (QoS): Silver (best effort)
WMM Policy: Disabled
7920 Phone Support: □ Client CAC Limit □ AP CAC Limit
Broadcast SSID: ☑ Enabled
Allow AAA Override: □ Enabled
External Policy Validation: □ Enabled
Client Exclusion: ☑ Enabled ** 600 Timeout Value (secs)
DHCP Server: □ Override
DHCP Addr. Assignment: ☑ Required
Interface Name: management
MFP Version Required: 1
MFP Signature Generation: ☑
H-REAP Local Switching: □

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

CISCO Client Extension (CCX)

Version IE: Enabled
Aironet IE: ☑
Gratuitous Probe Response: □

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	IP:10.1.1.12, Port:1812	none

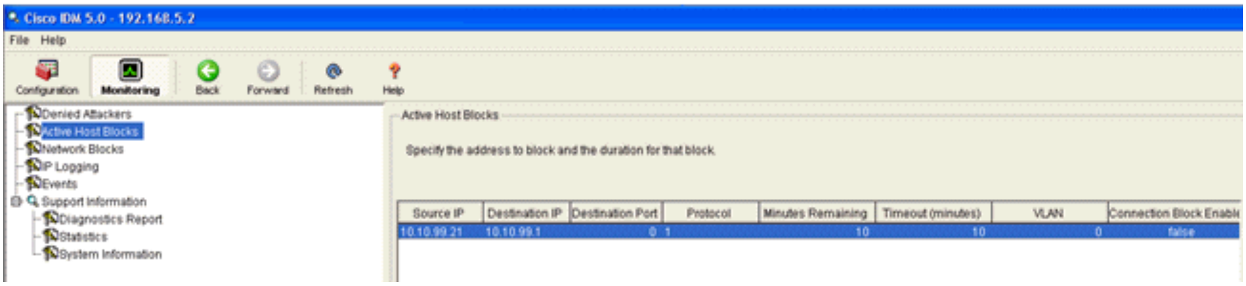
Security Policies

IPv6 Enable: □
Layer 2 Security: WPA1+WPA2
□ MAC Filtering
Layer 3 Security: None
□ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

5. You can trigger an event in the Cisco IPS system either when you do an NMAP Scan to certain devices in the network or when you do a ping to some hosts monitored by the Cisco IPS Sensor. Once an alarm is triggered in the Cisco IPS, go to **Monitoring and Active Host Blocks** in order to check the details about the host.

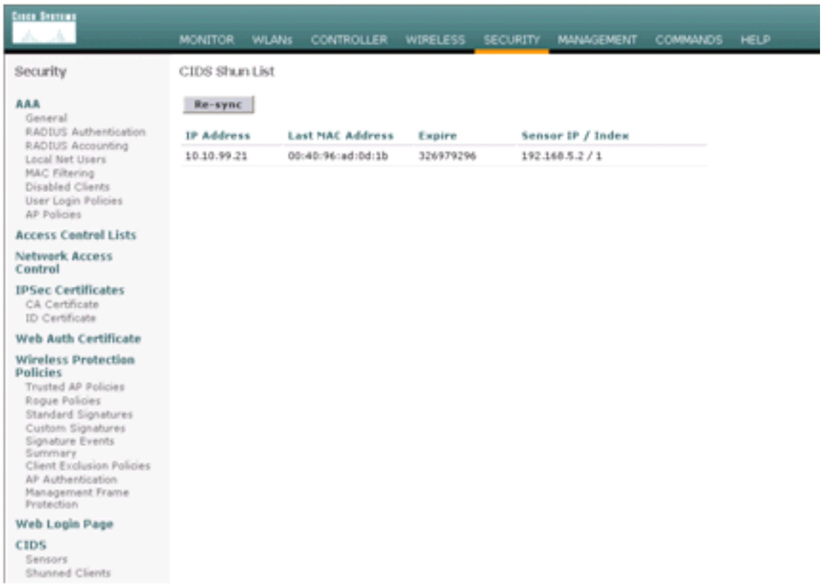


Active Host Blocks

Specify the address to block and the duration for that block.

Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	VLAN	Connection Block Enable
10.10.99.21	10.10.99.1	0	1	10	10	0	false

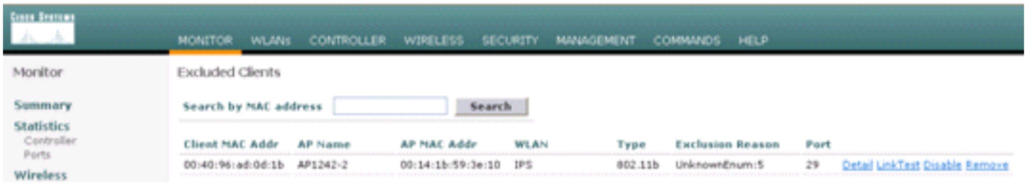
The Shunned Clients list in the controller is now populated with the IP and MAC address of the host.



CIDS Shun List

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.21	00:40:96:ad:0d:1b	326979296	192.168.5.2 / 1

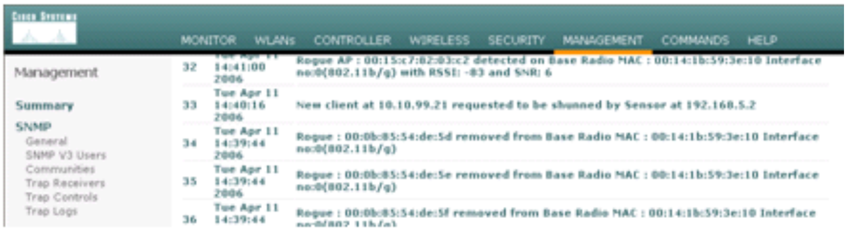
The user is added to the Client Exclusion list.



Excluded Clients

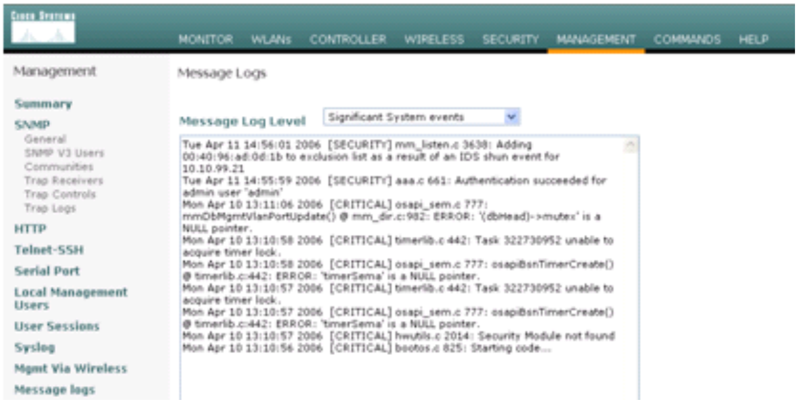
Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:0d:1b	AP1242-2	00:14:1b:59:3e:10	IPS	802.11b	UnknownEnum:5	29	Detail LinkTest Disable Remove

A trap log is generated as a client is added to the shun list.



```
32  14:41:00   Rogue AP : 00:15:c7:82:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface
    2006       no:0(802.11b/g) with RSSI: -83 and SNR: 6
    Tue Apr 11
33  14:40:16   New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2
    2006
    Tue Apr 11
34  14:39:44   Rogue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface
    2006       no:0(802.11b/g)
    Tue Apr 11
35  14:39:44   Rogue : 00:0b:85:54:de:5e removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface
    2006       no:0(802.11b/g)
    Tue Apr 11
36  14:39:44   Rogue : 00:0b:85:54:de:5f removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface
```

A message log is also generated for the event.

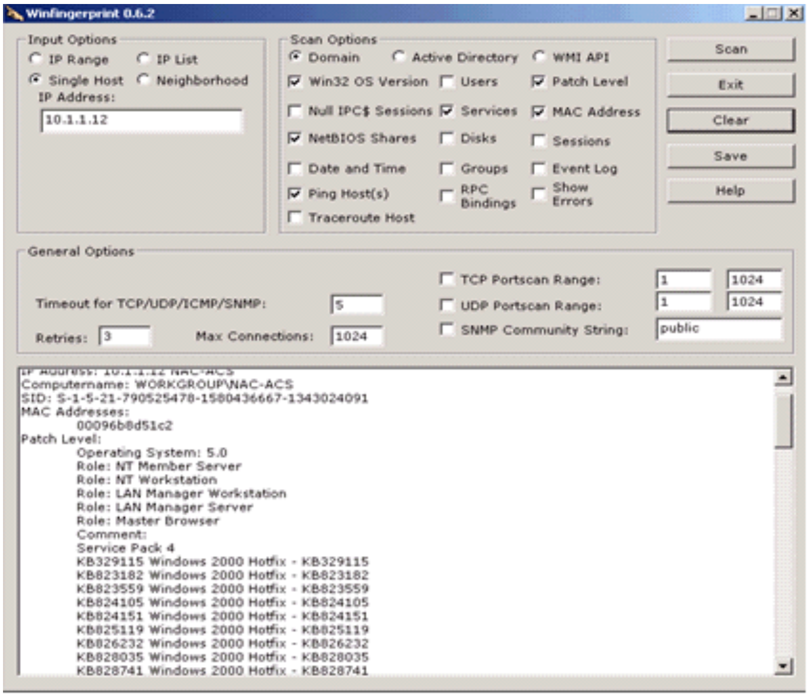


Message Logs

Message Log Level: Significant System events

```
Tue Apr 11 14:56:01 2006  [SECURITY] mm_listen.c 3638: Adding
00:40:96:ad:0d:1b to exclusion list as a result of an IDS shun event for
10.10.99.21
Tue Apr 11 14:55:59 2006  [SECURITY] aaa.c 661: Authentication succeeded for
admin user 'admin'
Mon Apr 10 13:11:06 2006  [CRITICAL] osapi_sem.c 777:
mmDbMgmtVlanPortUpdate() @ mm_dir.c:982: ERROR: '(dbHead)->mutex' is a
NULL pointer.
Mon Apr 10 13:10:58 2006  [CRITICAL] timerlib.c 442: Task 322730952 unable to
acquire timer lock.
Mon Apr 10 13:10:58 2006  [CRITICAL] osapi_sem.c 777: osapiBsnTimerCreate()
@ timerlib.c:442: ERROR: 'timerSema' is a NULL pointer.
Mon Apr 10 13:10:57 2006  [CRITICAL] timerlib.c 442: Task 322730952 unable to
acquire timer lock.
Mon Apr 10 13:10:57 2006  [CRITICAL] osapi_sem.c 777: osapiBsnTimerCreate()
@ timerlib.c:442: ERROR: 'timerSema' is a NULL pointer.
Mon Apr 10 13:10:57 2006  [CRITICAL] hwutils.c 2014: Security Module not found
Mon Apr 10 13:10:56 2006  [CRITICAL] bootos.c 825: Starting code...
```

Some additional events are generated in the Cisco IPS Sensor when an NMAP scan is done on a device it monitors.



IP Address: 10.1.1.12

Timeout for TCP/UDP/ICMP/SNMP: 5

Retries: 3

Max Connections: 1024

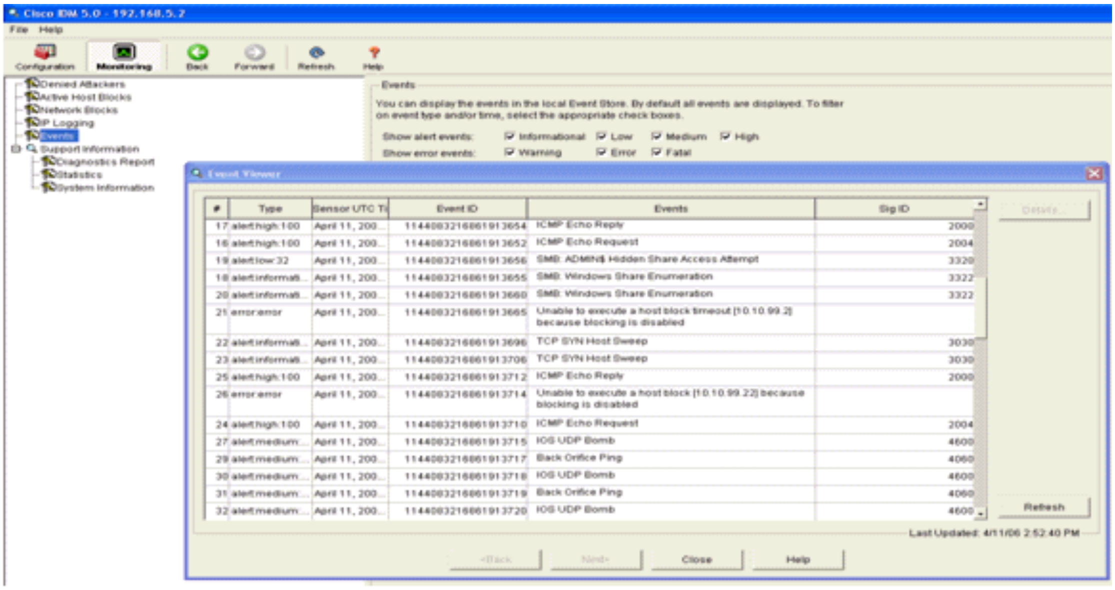
TCP Portscan Range: 1 1024

UDP Portscan Range: 1 1024

SNMP Community String: public

```
IP Address: 10.1.1.12 NAC-ACS
Computername: WORKGROUP\NAC-ACS
SID: S-1-5-21-790525478-1580436667-1343024091
MAC Addresses:
        00096b8d51c2
Patch Level:
        Operating System: 5.0
        Role: NT Member Server
        Role: NT Workstation
        Role: LAN Manager Workstation
        Role: LAN Manager Server
        Role: Master Browser
        Comment:
        Service Pack 4
        KB329115 Windows 2000 Hotfix - KB329115
        KB823182 Windows 2000 Hotfix - KB823182
        KB823559 Windows 2000 Hotfix - KB823559
        KB824105 Windows 2000 Hotfix - KB824105
        KB824151 Windows 2000 Hotfix - KB824151
        KB825119 Windows 2000 Hotfix - KB825119
        KB826232 Windows 2000 Hotfix - KB826232
        KB828035 Windows 2000 Hotfix - KB828035
        KB828741 Windows 2000 Hotfix - KB828741
```

This window shows events generated in the Cisco IPS Sensor.



You can display the events in the local Event Store. By default all events are displayed. To filter on event type and/or time, select the appropriate check boxes.

Show alert events: ☑ Informational ☑ Low ☑ Medium ☑ High

Show error events: ☑ Warning ☑ Error ☑ Fatal

#	Type	Sensor UTC Ti	Event ID	Events	Sig ID
17	alert:high:100	April 11, 200...	1144083216861913654	ICMP Echo Reply	2000
16	alert:high:100	April 11, 200...	1144083216861913652	ICMP Echo Request	2004
19	alert:low:32	April 11, 200...	1144083216861913656	SMB: ADMIN$ Hidden Share Access Attempt	3320
18	alert:informati...	April 11, 200...	1144083216861913655	SMB: Windows Share Enumeration	3322
20	alert:informati...	April 11, 200...	1144083216861913660	SMB: Windows Share Enumeration	3322
21	error:error	April 11, 200...	1144083216861913665	Unable to execute a host block timeout [10.10.99.2] because blocking is disabled	
22	alert:informati...	April 11, 200...	1144083216861913696	TCP SYN Host Sweep	3030
23	alert:informati...	April 11, 200...	1144083216861913706	TCP SYN Host Sweep	3030
25	alert:high:100	April 11, 200...	1144083216861913712	ICMP Echo Reply	2000
26	error:error	April 11, 200...	1144083216861913714	Unable to execute a host block [10.10.99.22] because blocking is disabled	
24	alert:high:100	April 11, 200...	1144083216861913710	ICMP Echo Request	2004
27	alert:medium:...	April 11, 200...	1144083216861913715	IOS UDP Bomb	4600
29	alert:medium:...	April 11, 200...	1144083216861913717	Back Orifice Ping	4060
30	alert:medium:...	April 11, 200...	1144083216861913718	IOS UDP Bomb	4600
31	alert:medium:...	April 11, 200...	1144083216861913719	Back Orifice Ping	4060
32	alert:medium:...	April 11, 200...	1144083216861913720	IOS UDP Bomb	4600

Last Updated: 4/11/06 2:52:40 PM

Cisco IDS Sensor Sample Configuration

This is the output from the setup script from the installation:

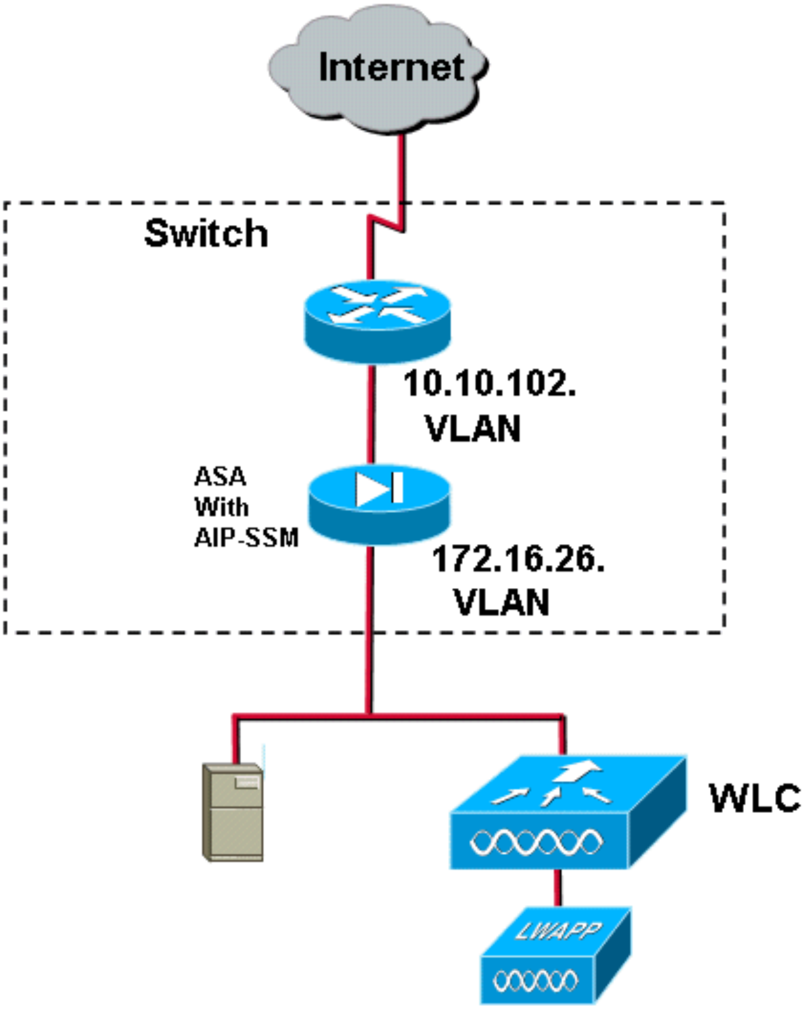
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
```

```
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
exit
signatures 2001 0
alert-severity high
status
enabled true
exit
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
```

```
description default virtual sensor
physical−interface GigabitEthernet0/0
exit
exit
! ------------------------------
service interface
physical−interfaces GigabitEthernet0/0
admin−state enabled
exit
exit
! ------------------------------
service trusted−certificates
exit
sensor#
```

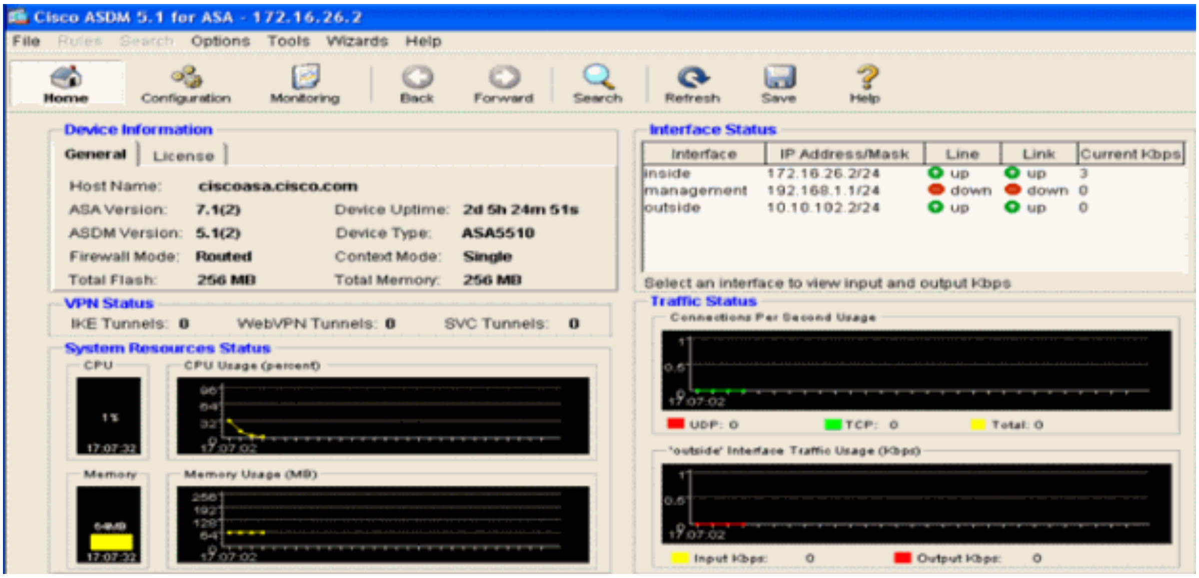
Configure an ASA for IDS

Unlike a traditional Intrusion Detection Sensor, an ASA must always be in the data path. In other words, instead of spanning traffic from a switch port over to a passive sniffing port on the Sensor, the ASA must receive data on one interface, process it internally, and then forward it out another port. For IDS, use the modular policy framework (MPF) in order to copy traffic the ASA receives over to the internal Advanced Inspection and Prevention Security Services Module (AIP−SSM) for inspection.



In this example, the ASA used is already setup and passes traffic. These steps demonstrate how to create a policy that sends data to the AIP−SSM.

1. Log into the ASA using ASDM. Upon successful login, the ASA Main System window appears.



Cisco ASDM 5.1 for ASA - 172.16.26.2

Device Information

General | License

Host Name: ciscoasa.cisco.com

ASA Version: 7.1(2) Device Uptime: 2d 5h 24m 51s

ASDM Version: 5.1(2) Device Type: ASA5510

Firewall Mode: Routed Context Mode: Single

Total Flash: 256 MB Total Memory: 256 MB

VPN Status

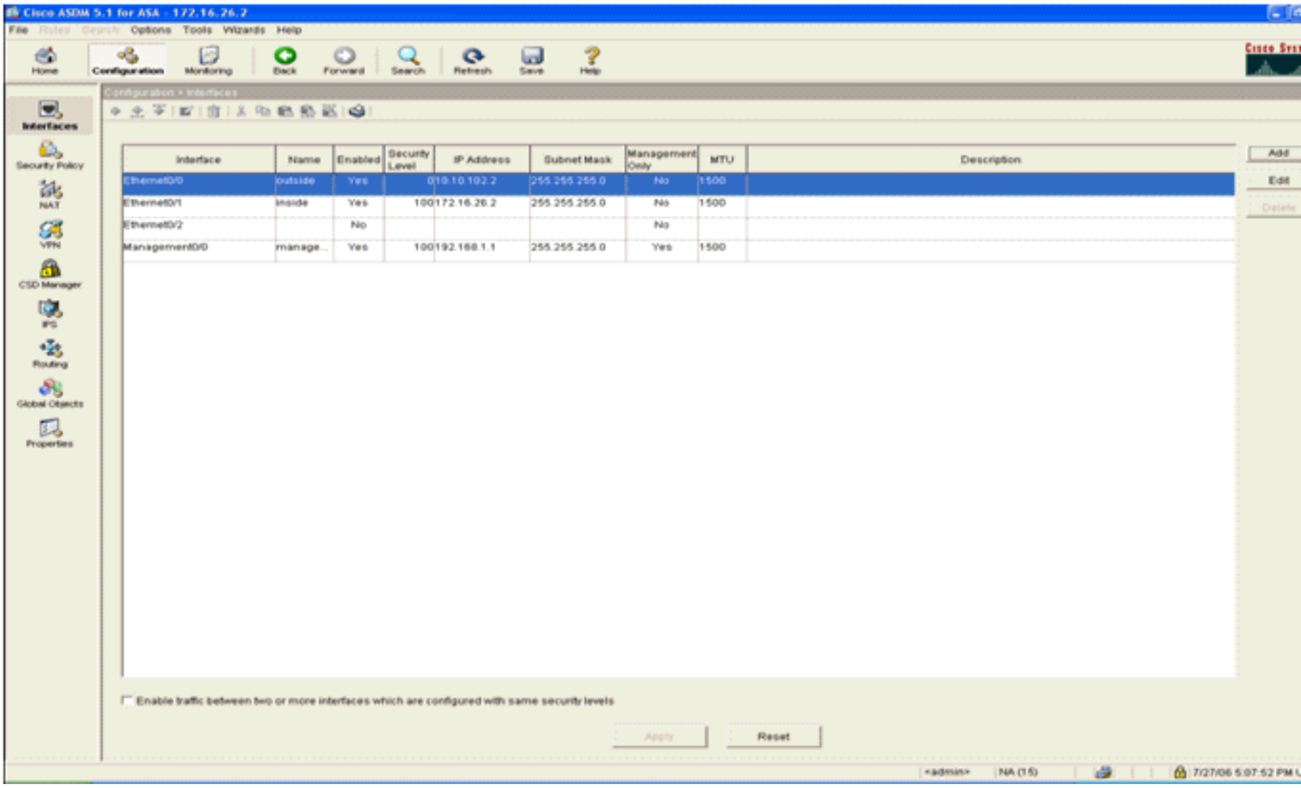
IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0

Interface Status

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.16.26.2/24	up	up	3
management	192.168.1.1/24	down	down	0
outside	10.10.102.2/24	up	up	0

Select an interface to view input and output Kbps

2. Click **Configuration** at the top of the page. The window switches to a view of the ASA interfaces.



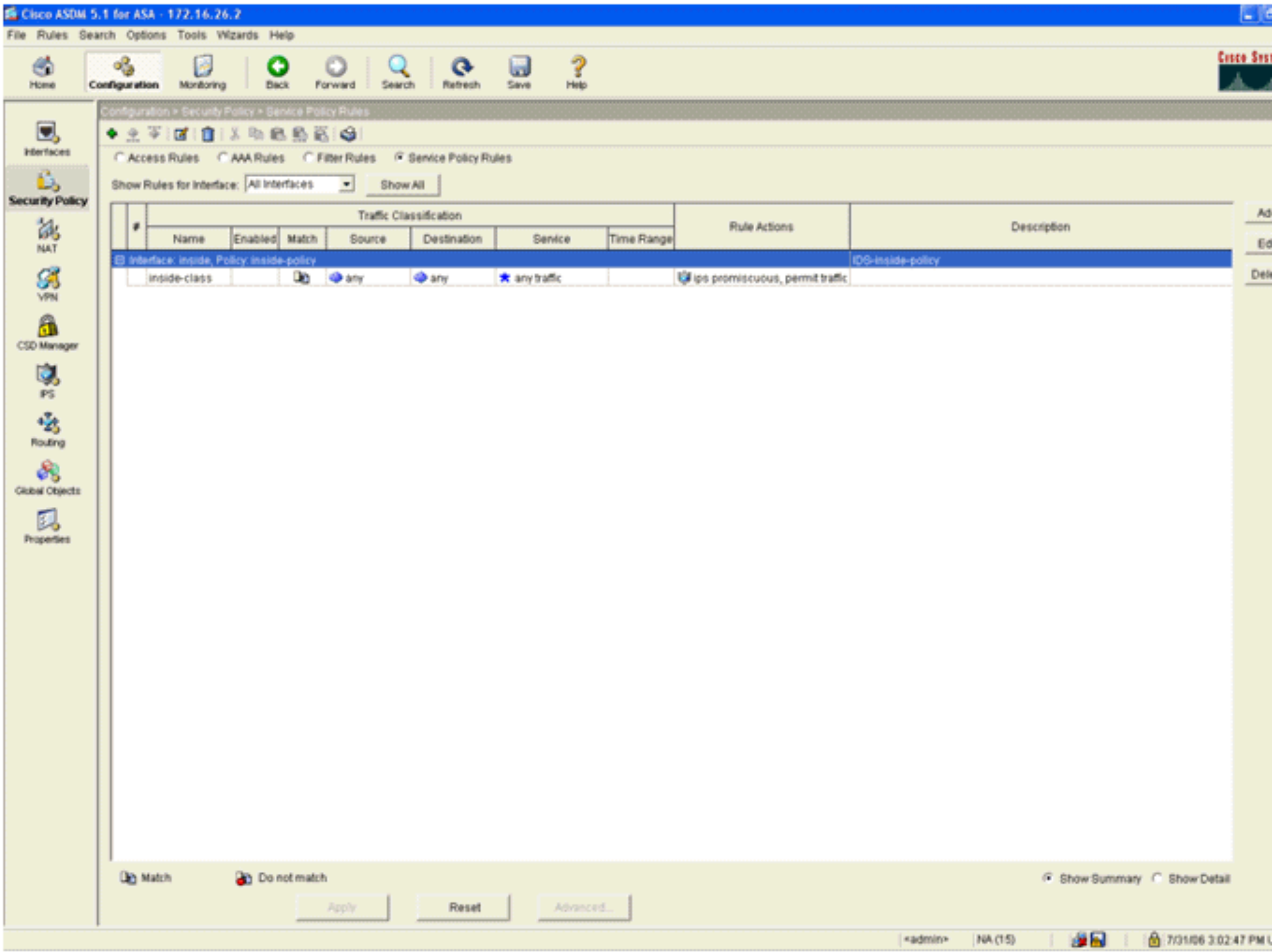
Cisco ASDM 5.1 for ASA - 172.16.26.2

Configuration > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU	Description
Ethernet0/0	outside	Yes	0	10.10.102.2	255.255.255.0	No	1500	
Ethernet0/1	inside	Yes	100	172.16.26.2	255.255.255.0	No	1500	
Ethernet0/2		No				No		
Management0/0	manage...	Yes	100	192.168.1.1	255.255.255.0	Yes	1500	

☐ Enable traffic between two or more interfaces which are configured with same security levels

3. Click **Security Policy** on the left−hand side of the window. On the resultant window, choose the **Service Policy Rules** tab.



○ Access Rules ○ AAA Rules ○ Filter Rules ● Service Policy Rules

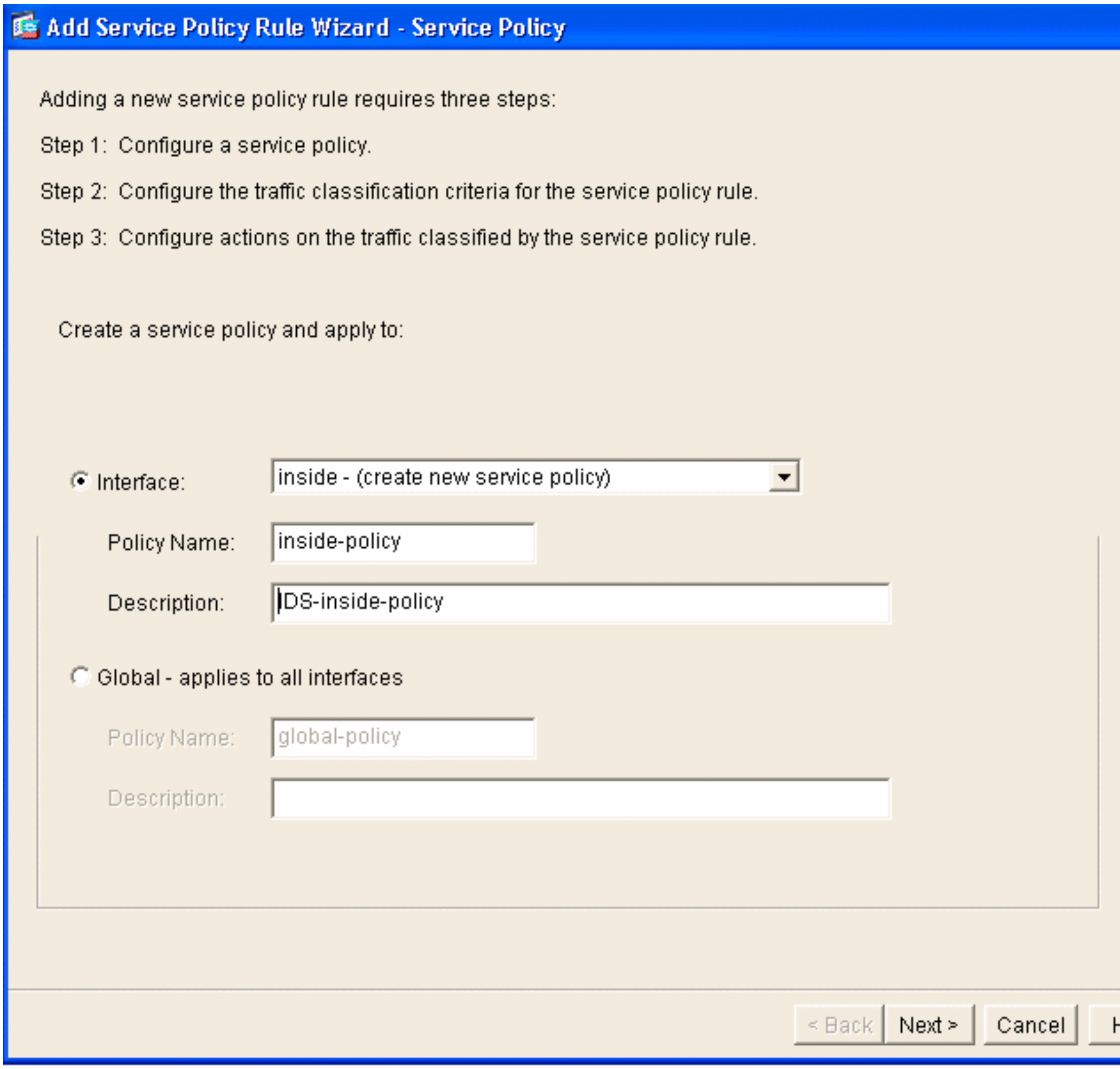
Show Rules for Interface: All Interfaces ▾ Show All

#	Traffic Classification							Rule Actions	Description
	Name	Enabled	Match	Source	Destination	Service	Time Range		
Interface: inside, Policy: inside-policy									IDS-inside-policy
	inside-class			any	any	any traffic		ips promiscuous, permit traffic	

● Show Summary ○ Show Detail

4. Click **Add** in order to create a new policy. The Add Service Policy Rule Wizard launches in a new window.

    a. Click **Interface** and then choose the correct interface from the drop−down list in order to create a new policy which is bound to one of the interfaces that passes traffic.
    b. Give the policy a name and a description of what the policy does using the two text boxes.
    c. Click **Next** in order to move to the next step.



Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

● Interface: inside - (create new service policy)

Policy Name: inside-policy

Description: IDS-inside-policy

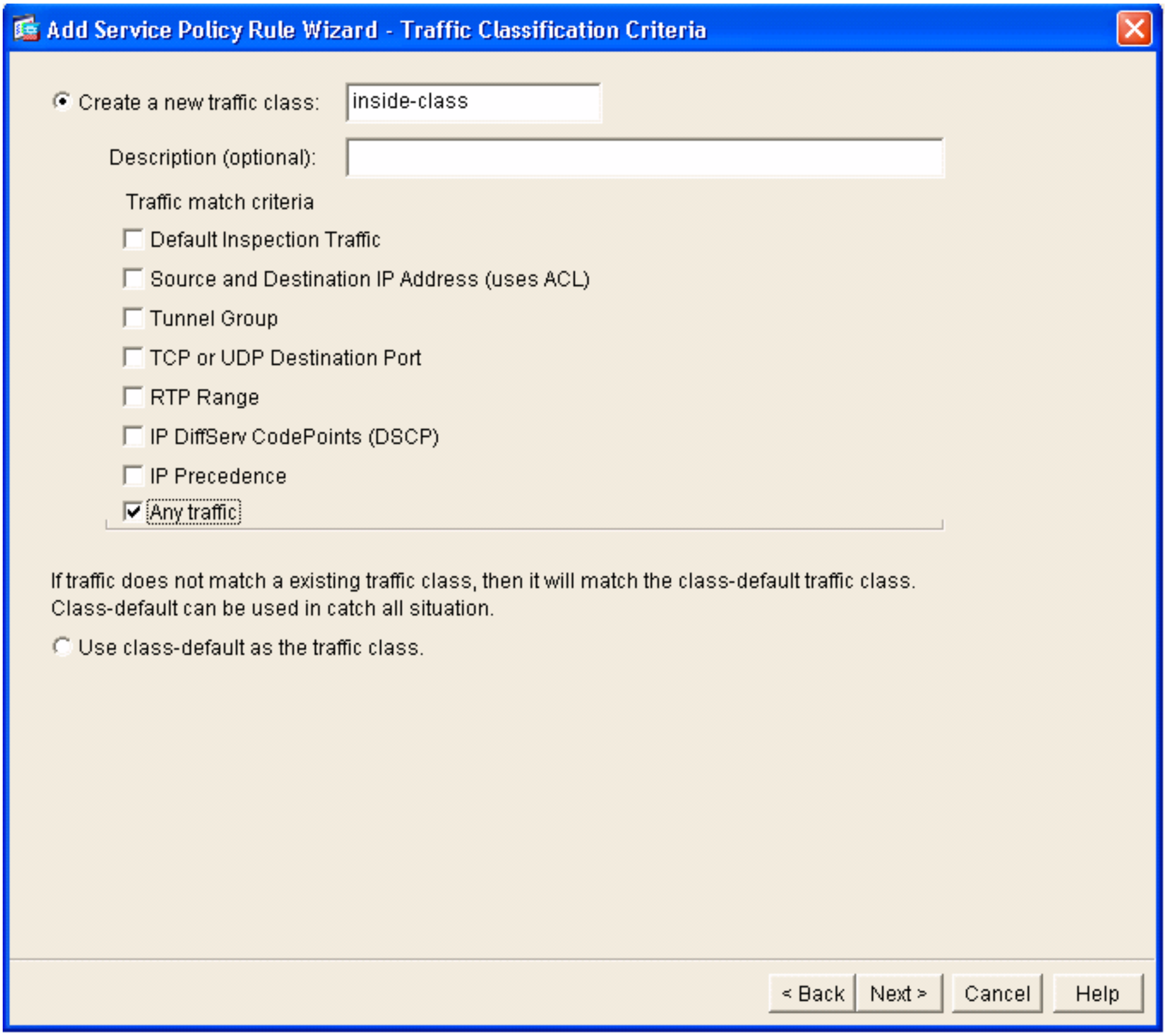
○ Global - applies to all interfaces

Policy Name: global-policy

Description:

5. Build a new traffic class to apply to the policy.

   It is reasonable to build specific classes in order to inspect specific data types, but in this example, Any Traffic is selected for simplicity. Click **Next** in order to proceed.



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: inside-class

Description (optional):

Traffic match criteria

☐ Default Inspection Traffic

☐ Source and Destination IP Address (uses ACL)

☐ Tunnel Group

☐ TCP or UDP Destination Port

☐ RTP Range

☐ IP DiffServ CodePoints (DSCP)

☐ IP Precedence

☑ Any traffic

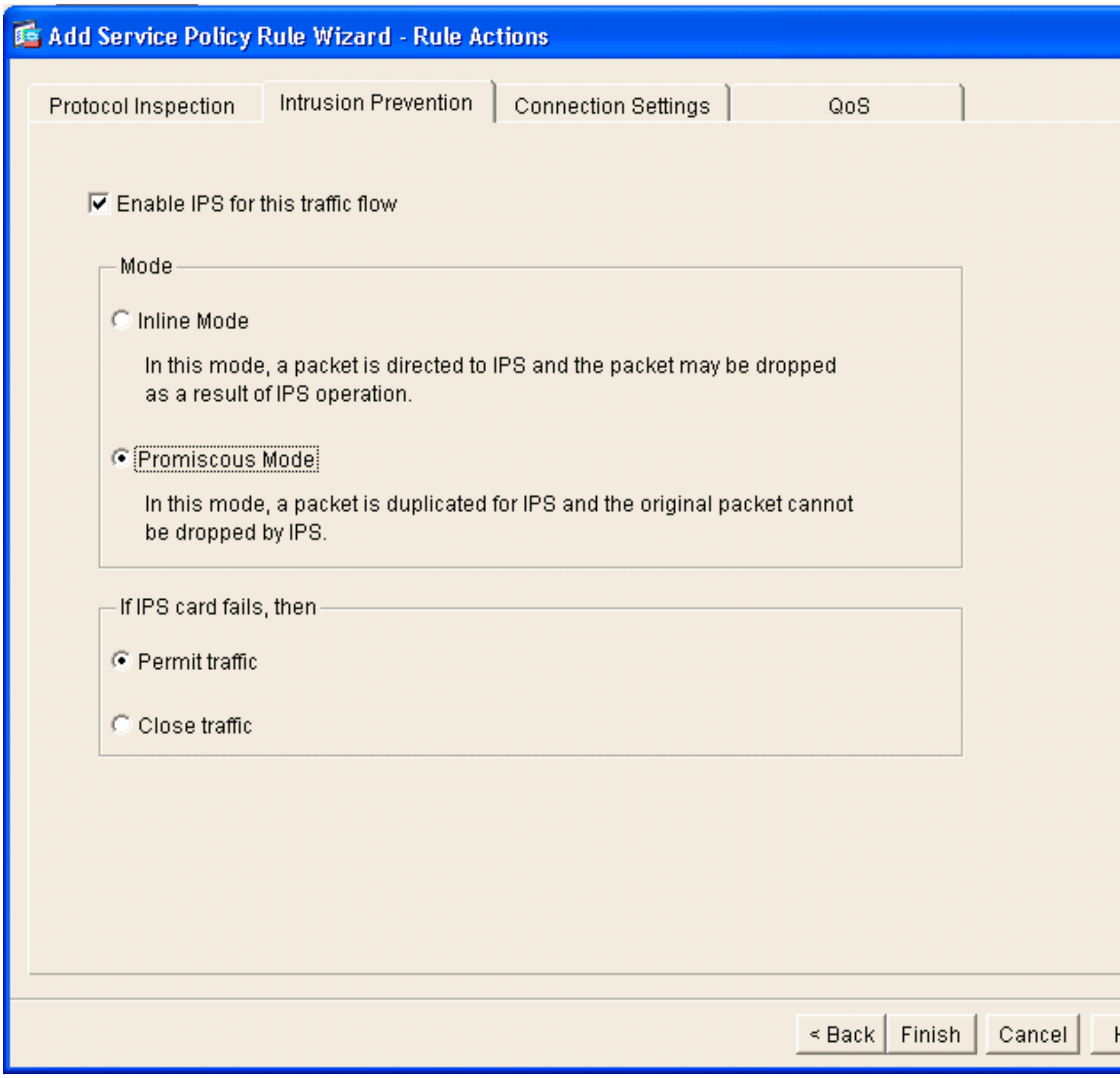
If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

○ Use class-default as the traffic class.

6. Complete these steps in order to

   instruct the ASA to direct the traffic over to its AIP−SSM.

   a. Check **Enable IPS for this traffic flow** in order to enable intrusion detection.
   b. Set the mode to **Promiscuous** so that a copy of the traffic is sent to the module out−of−band instead of placing the module inline with the data flow.
   c. Click **Permit traffic** in order to ensure that the ASA switches to a fail−open state in the event that the AIP−SSM fails.
   d. Click **Finish** in order to commit the change.



☑ Enable IPS for this traffic flow

Mode

○ Inline Mode

In this mode, a packet is directed to IPS and the packet may be dropped as a result of IPS operation.

● Promiscous Mode

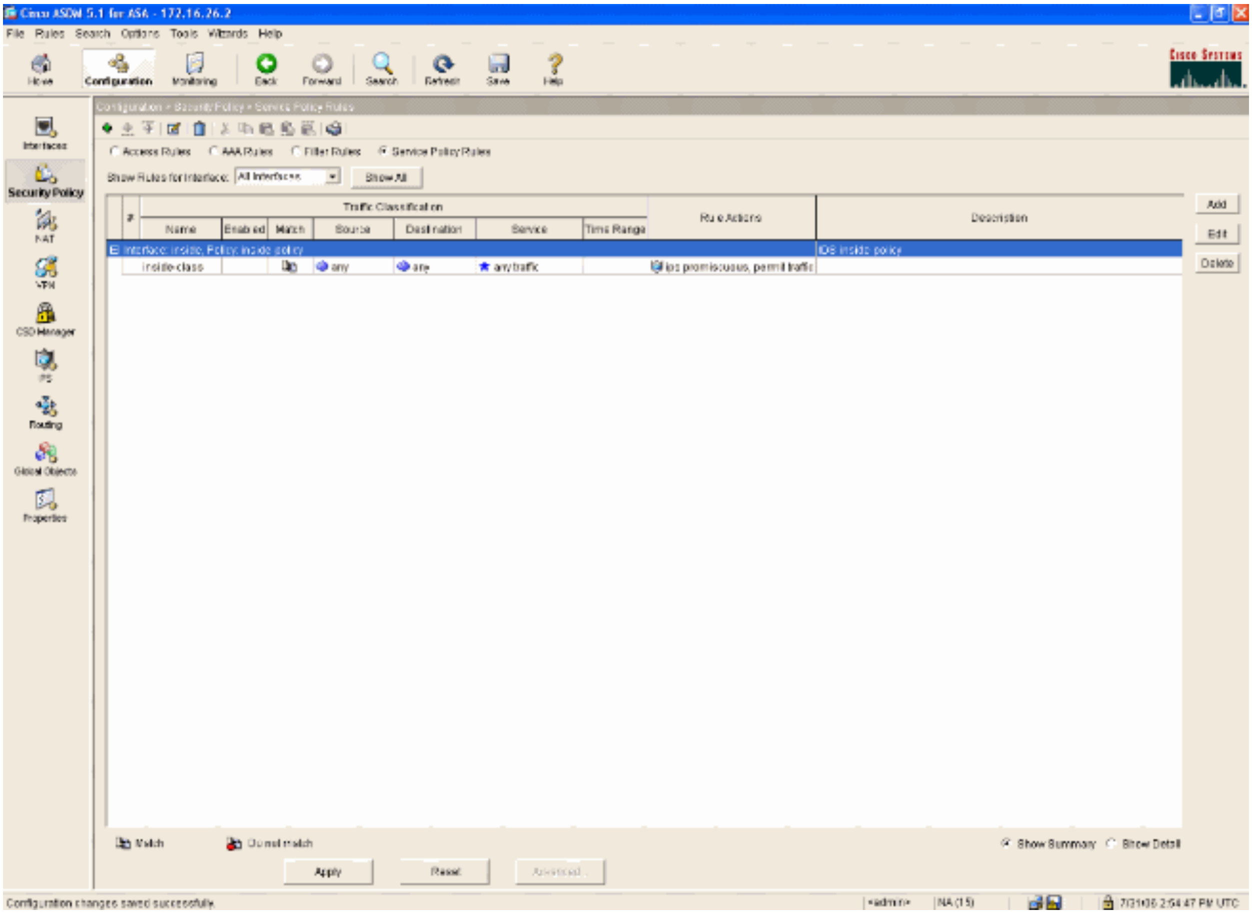
In this mode, a packet is duplicated for IPS and the original packet cannot be dropped by IPS.

If IPS card fails, then

● Permit traffic

○ Close traffic

7. The ASA is now configured to send traffic to the IPS module. Click **Save** on the top row in order to write the changes to the ASA.



Show Rules for Interface: All Interfaces

#	Traffic Classification							Rule Actions	Description
	Name	Enabled	Match	Source	Destination	Service	Time Range		
⊟ Interface: inside, Policy: inside-policy									IDS inside policy
	inside-class			any	any	any traffic		ips promiscuous, permit traffic	

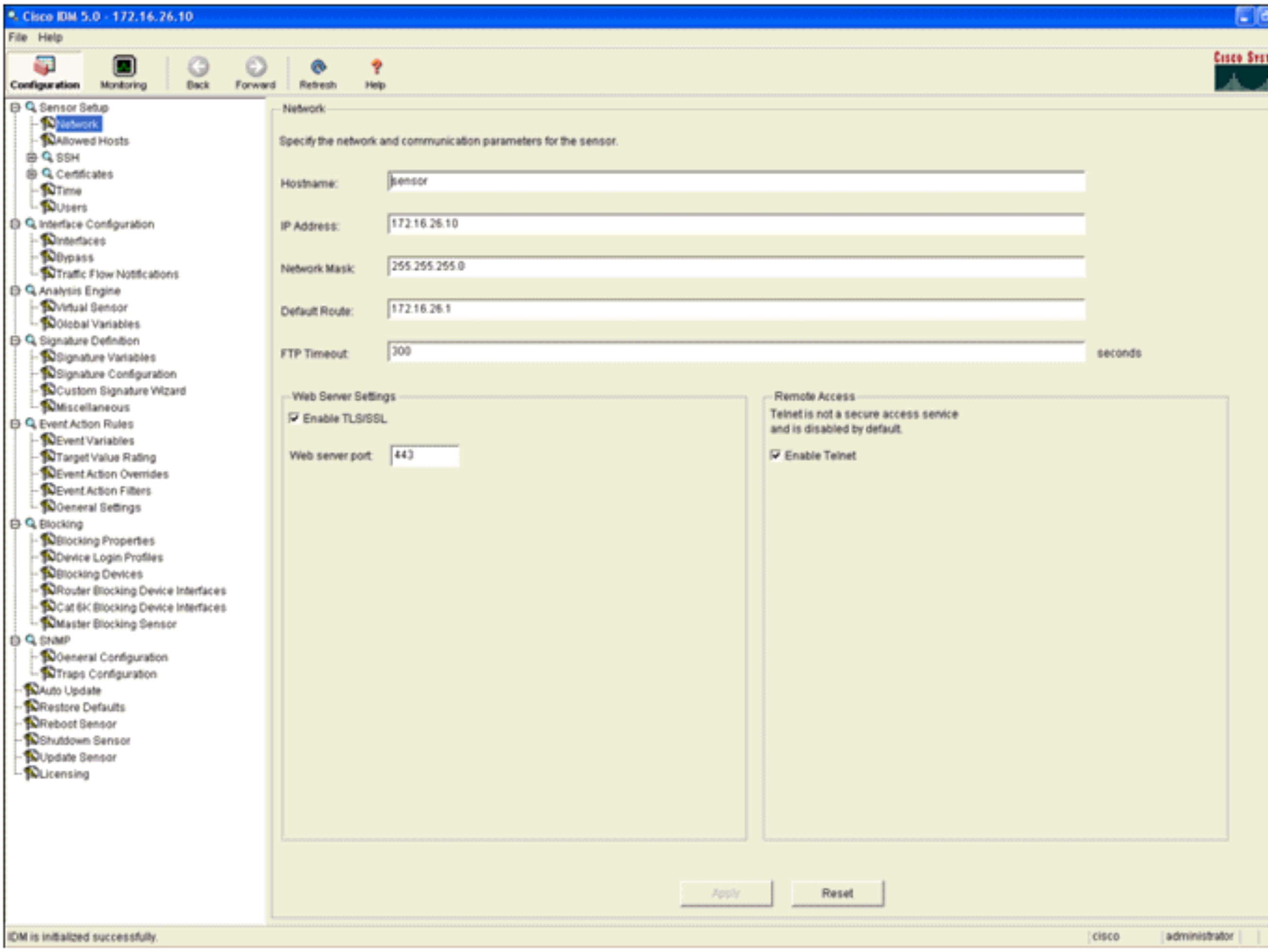
Configuration changes saved successfully.

<admin> NA (15) 7/31/06 2:54:47 PM UTC

Configure the AIP−SSM for Traffic Inspection

While the ASA sends data to the IPS module, associate the AIP−SSM interface to its virtual Sensor engine.

1. Login to the AIP−SSM using IDM.



Network

Specify the network and communication parameters for the sensor.

Hostname: sensor

IP Address: 172.16.26.10

Network Mask: 255.255.255.0

Default Route: 172.16.26.1

FTP Timeout: 300 seconds

Web Server Settings

☑ Enable TLS/SSL

Web server port: 443

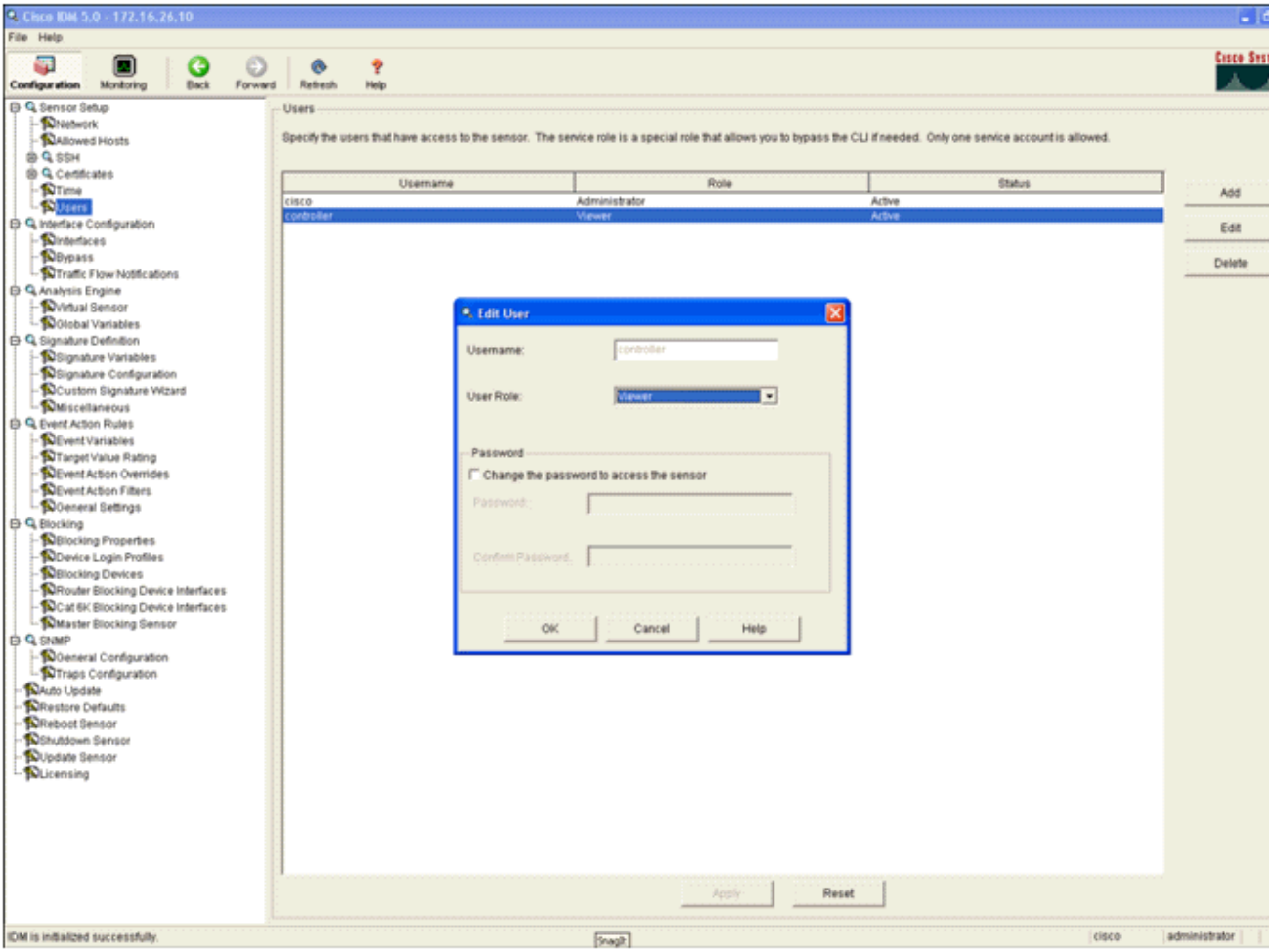
Remote Access

Telnet is not a secure access service and is disabled by default.

☑ Enable Telnet

IDM is initialized successfully. cisco administrator

2. Add a user with at least viewer privileges.



Users

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
cisco	Administrator	Active
controller	Viewer	Active

Edit User

Username: controller

User Role: Viewer

Password

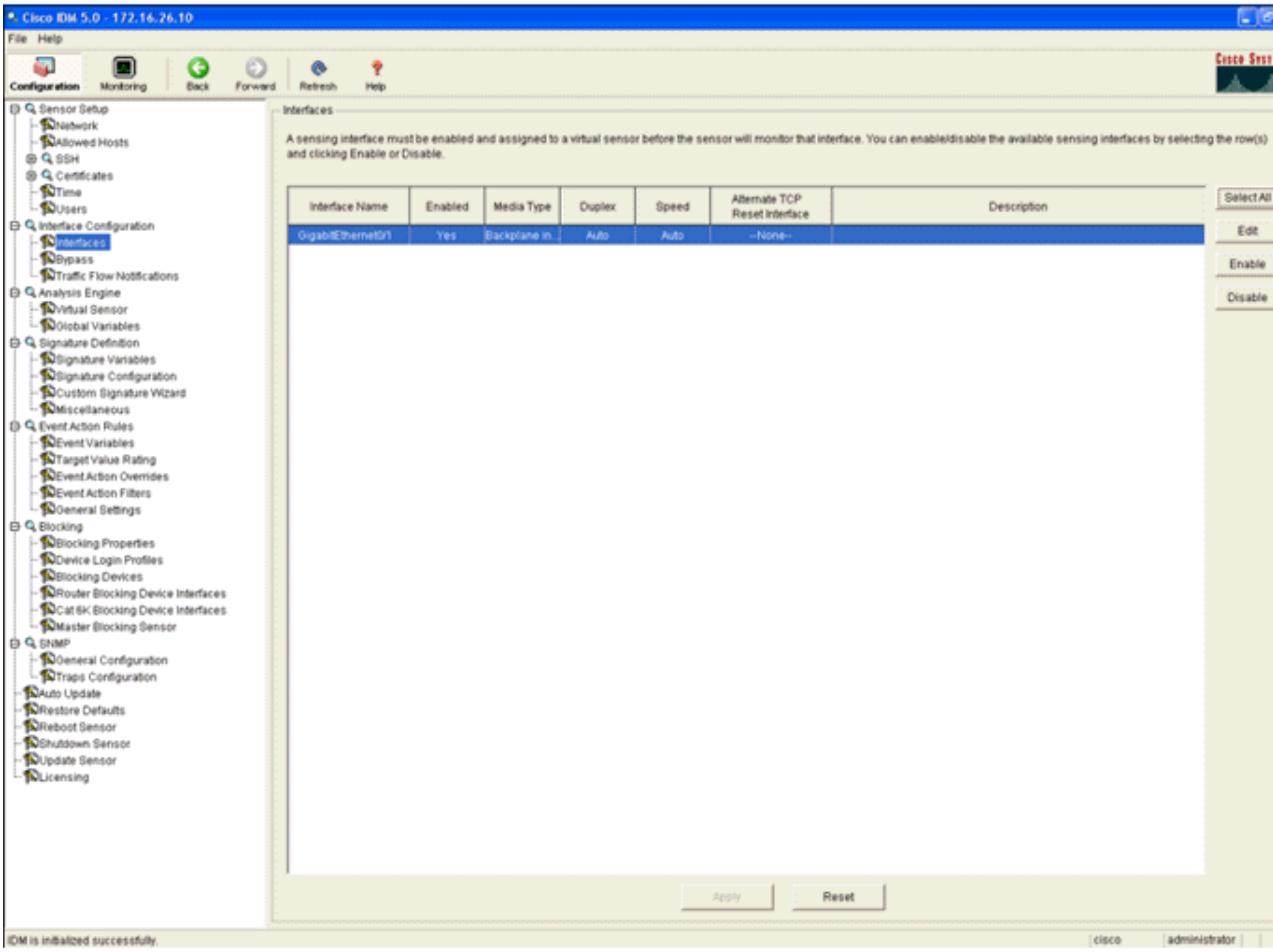
□ Change the password to access the sensor

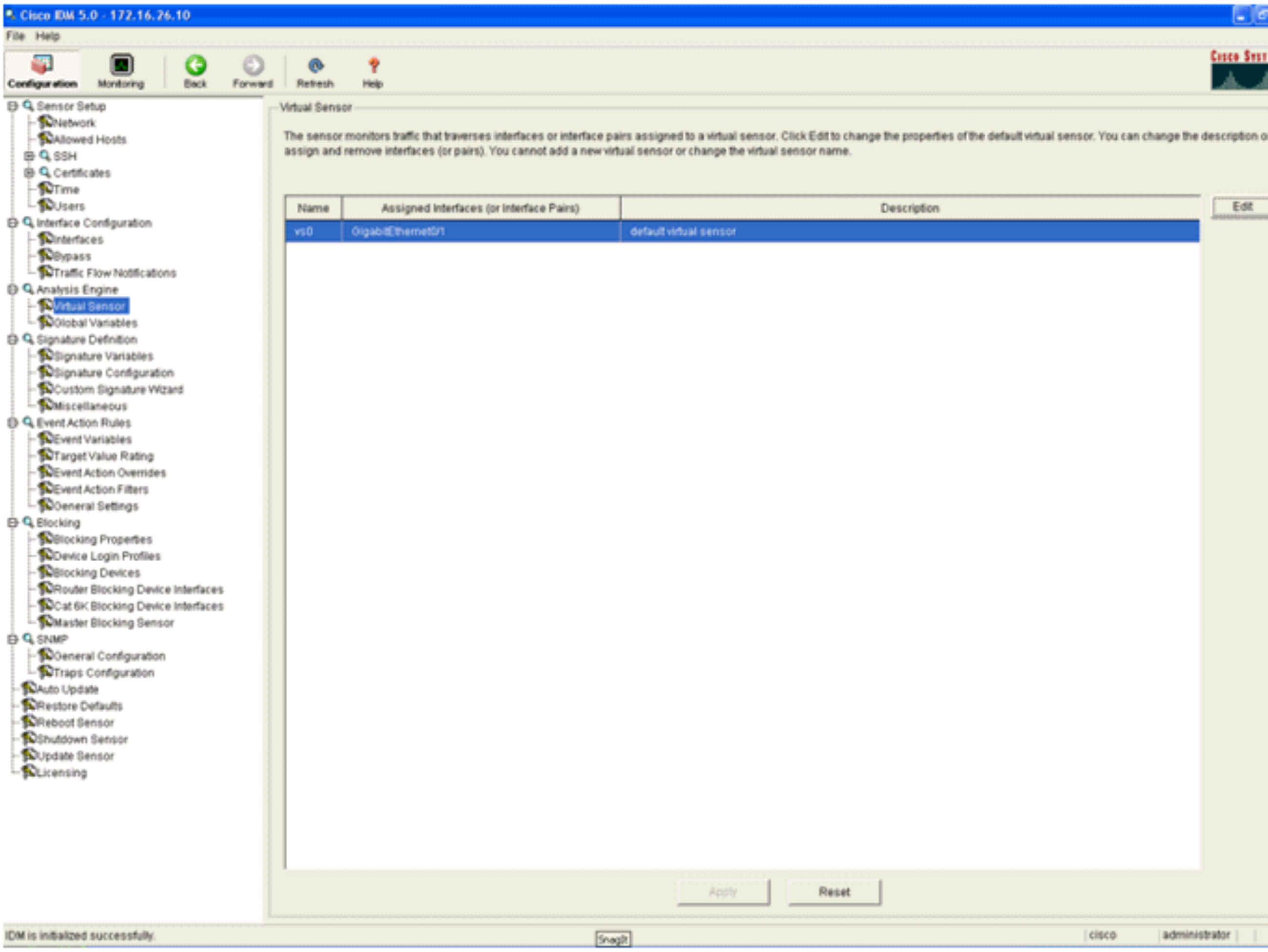
Password:

Confirm Password:

IDM is initialized successfully. cisco administrator

3. Enable the interface.





The sensor monitors traffic that traverses interfaces or interface pairs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the description o
assign and remove interfaces (or pairs). You cannot add a new virtual sensor or change the virtual sensor name.

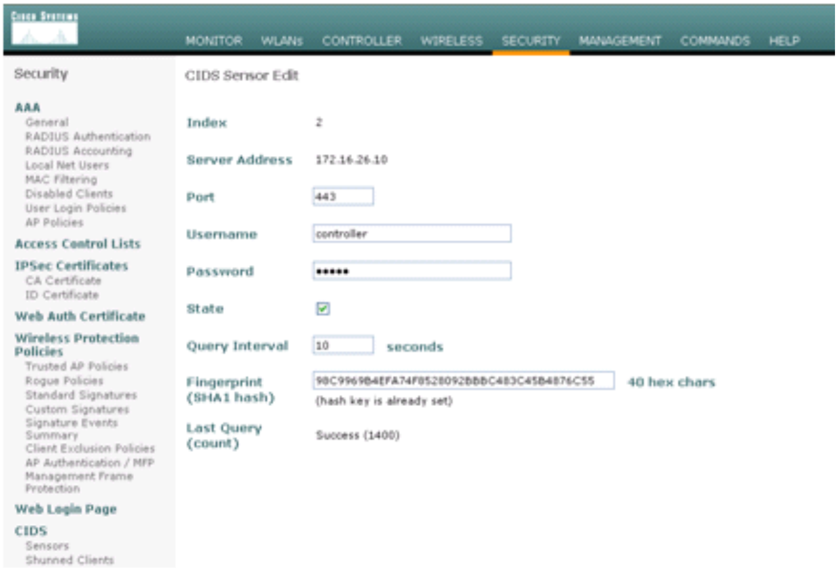
Name	Assigned Interfaces (or Interface Pairs)	Description
vs0	GigabitEthernet0/1	default virtual sensor

Configure a WLC to Poll the AIP−SSM for Client Blocks

Complete these steps once the Sensor is configured and ready to be added in the controller:

1. Choose **Security** > **CIDS** > **Sensors** > **New** in the WLC.
2. Add the IP address, TCP port number, username and password you created in the previous section.
3. In order to obtain the fingerprint from the Sensor, execute this command in the Sensor and add the SHA1 fingerprint on the WLC (without the colon). This is used to secure the controller−to−IDS polling communication.

```
sensor#show tls fingerprint
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```



CIDS Sensor Edit

Index 2

Server Address 172.16.26.10

Port 443

Username controller

Password •••••

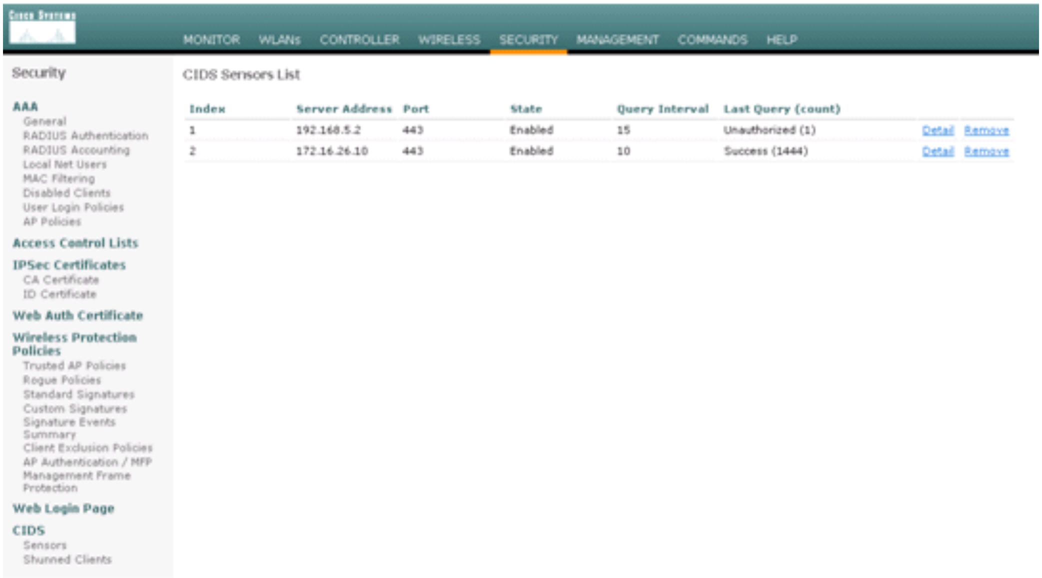
State ☑

Query Interval 10 seconds

Fingerprint (SHA1 hash) 98C9969B4EFA74F8528092BBBC483C45B4876C55 40 hex chars
(hash key is already set)

Last Query (count) Success (1400)

4. Check the status of the connection between the AIP−SSM and the WLC.



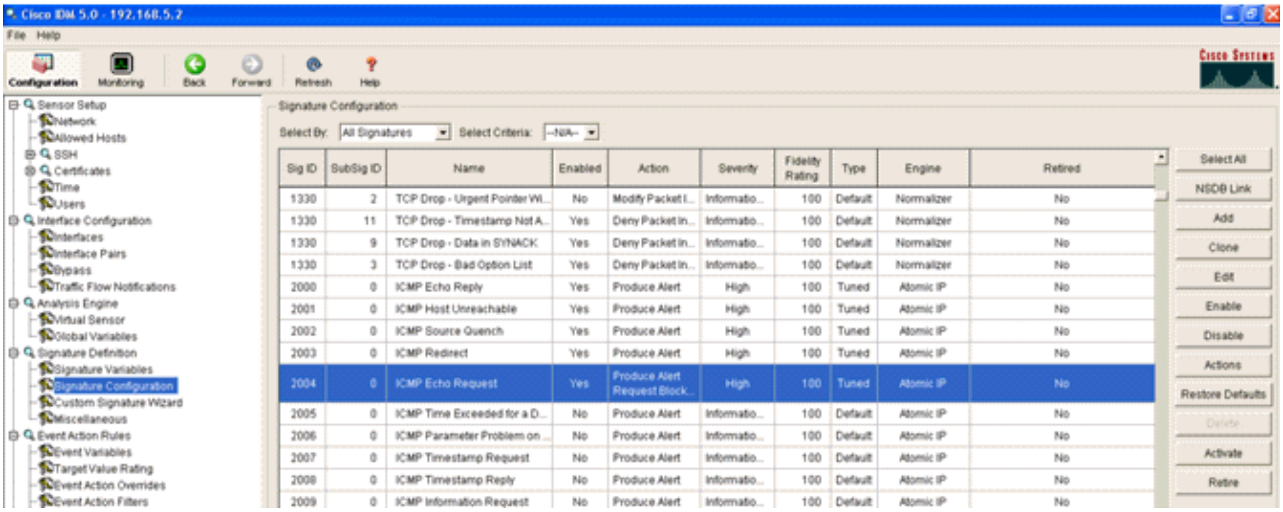
CIDS Sensors List

Index	Server Address	Port	State	Query Interval	Last Query (count)		
1	192.168.5.2	443	Enabled	15	Unauthorized (1)	Detail	Remove
2	172.16.26.10	443	Enabled	10	Success (1444)	Detail	Remove

Add a Blocking Signature to the AIP−SSM

Add an inspection signature to block traffic. Although there are many signatures that can do the job based on the tools available, this example creates a signature that blocks ping packets.

1. Select the **2004 signature (ICMP Echo Request)** in order to perform a quick setup verification.

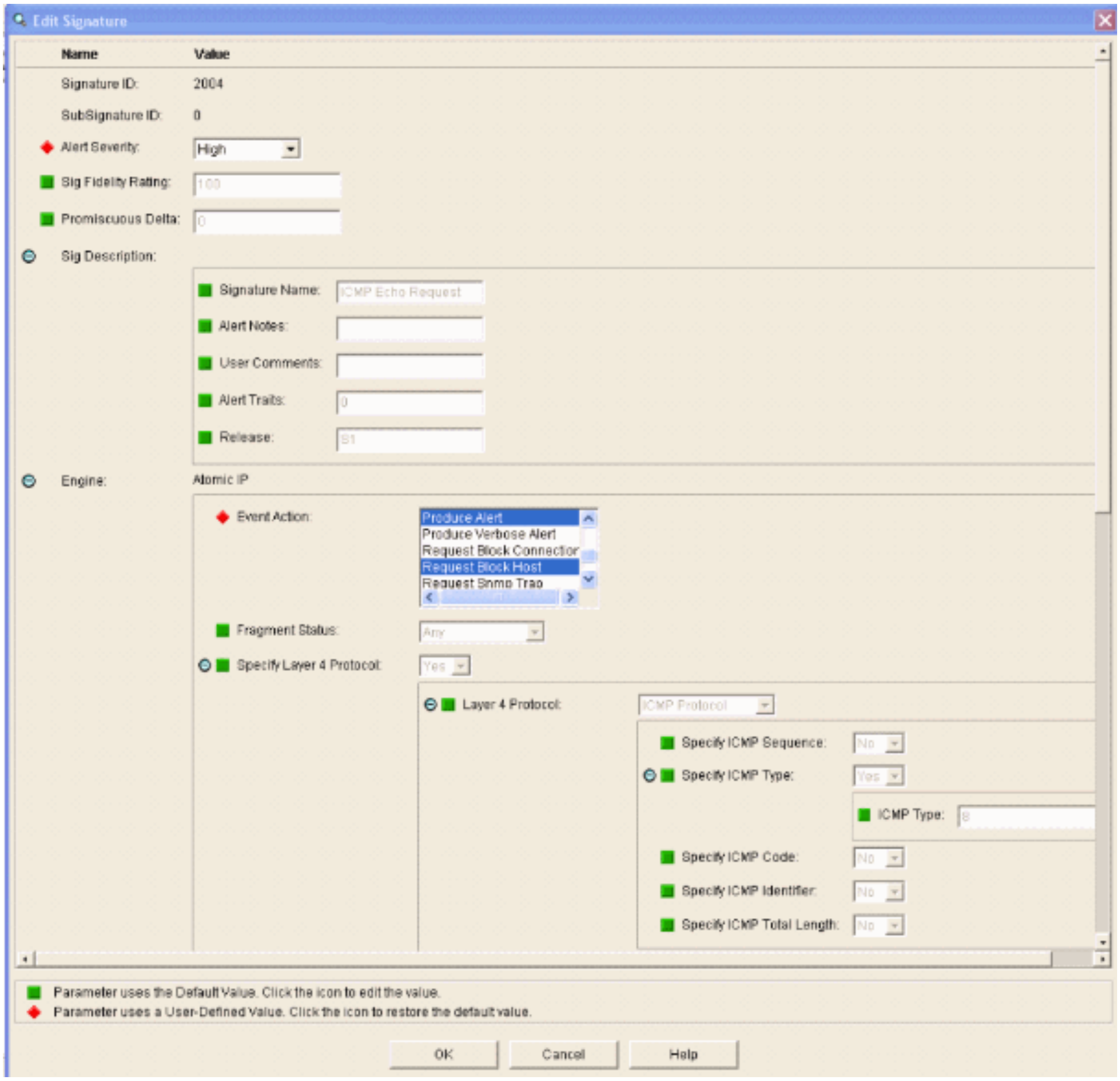


Signature Configuration

Select By: All Signatures Select Criteria: --N/A--

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired
1330	2	TCP Drop - Urgent Pointer Wi...	No	Modify Packet I...	Informatio...	100	Default	Normalizer	No
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2004	0	ICMP Echo Request	Yes	Produce Alert Request Block...	High	100	Tuned	Atomic IP	No
2005	0	ICMP Time Exceeded for a D...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2006	0	ICMP Parameter Problem on ...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2009	0	ICMP Information Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No

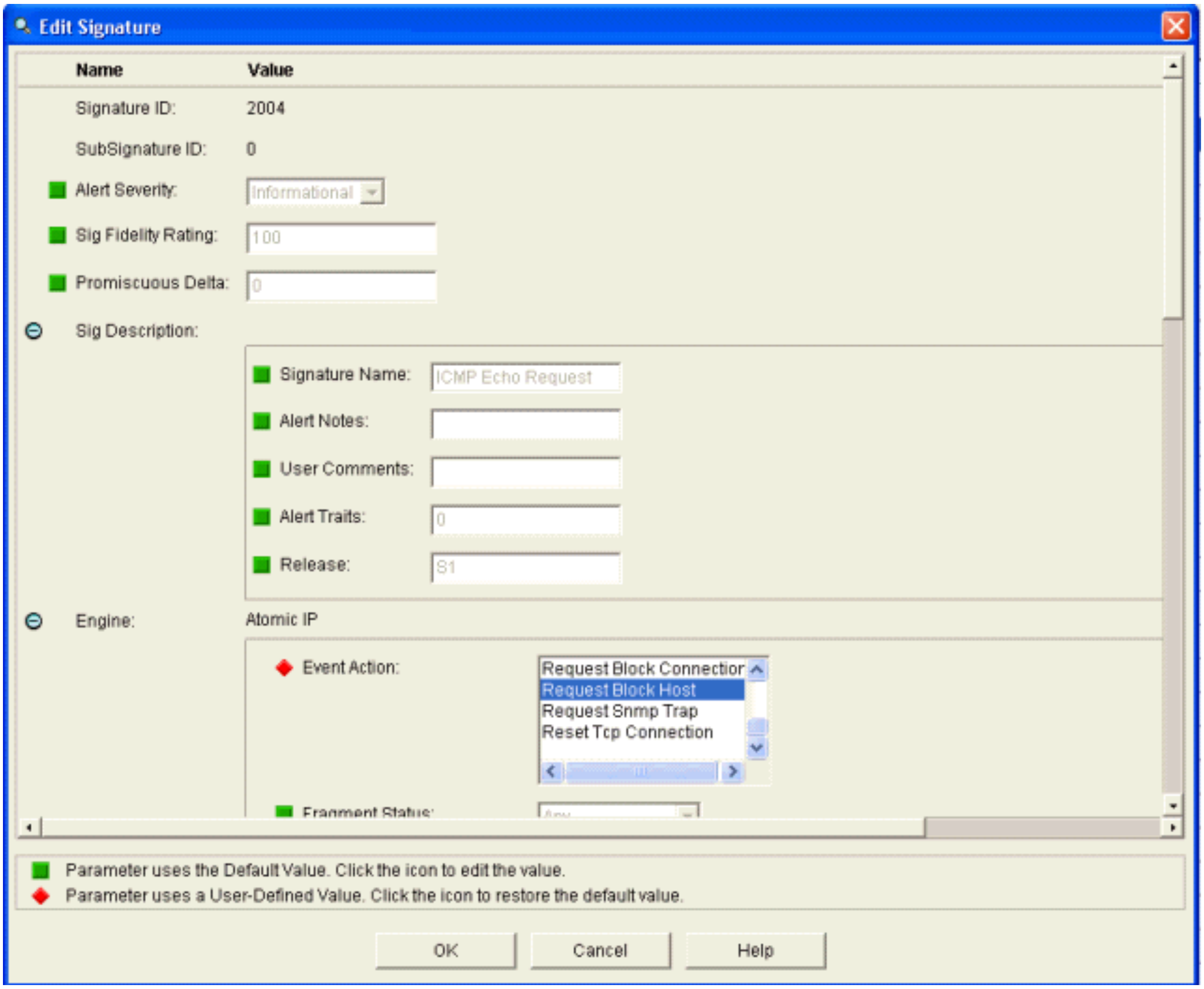
2. Enable the signature, set the Alert Severity to **High** and set Event Action to **Produce Alert** and **Request Block Host** in order to complete this verification step. Note that the Request Block Host action is the key to signaling the WLC to create client exceptions.



Name	Value
Signature ID:	2004
SubSignature ID:	0
◆ Alert Severity:	High
🟩 Sig Fidelity Rating:	100
🟩 Promiscuous Delta:	0
⊖ Sig Description:	
🟩 Signature Name:	ICMP Echo Request
🟩 Alert Notes:	
🟩 User Comments:	
🟩 Alert Traits:	0
🟩 Release:	S1
⊖ Engine:	Atomic IP
◆ Event Action:	Produce Alert (selected) Produce Verbose Alert Request Block Connection Request Block Host (selected) Request Snmp Trap
🟩 Fragment Status:	Any
⊖ 🟩 Specify Layer 4 Protocol:	Yes
⊖ 🟩 Layer 4 Protocol:	ICMP Protocol
🟩 Specify ICMP Sequence:	No
⊖ 🟩 Specify ICMP Type:	Yes
🟩 ICMP Type:	8
🟩 Specify ICMP Code:	No
🟩 Specify ICMP Identifier:	No
🟩 Specify ICMP Total Length:	No

🟩 Parameter uses the Default Value. Click the icon to edit the value.

◆ Parameter uses a User-Defined Value. Click the icon to restore the default value.



Signature ID: 2004

SubSignature ID: 0

🟩 Alert Severity: Informational

🟩 Sig Fidelity Rating: 100

🟩 Promiscuous Delta: 0

⊖ Sig Description:

🟩 Signature Name: ICMP Echo Request

🟩 Alert Notes:

🟩 User Comments:

🟩 Alert Traits: 0

🟩 Release: S1

⊖ Engine: Atomic IP

◆ Event Action: Request Block Connection, Request Block Host (selected), Request Snmp Trap, Reset Tcp Connection

🟩 Fragment Status:

🟩 Parameter uses the Default Value. Click the icon to edit the value.

◆ Parameter uses a User-Defined Value. Click the icon to restore the default value.

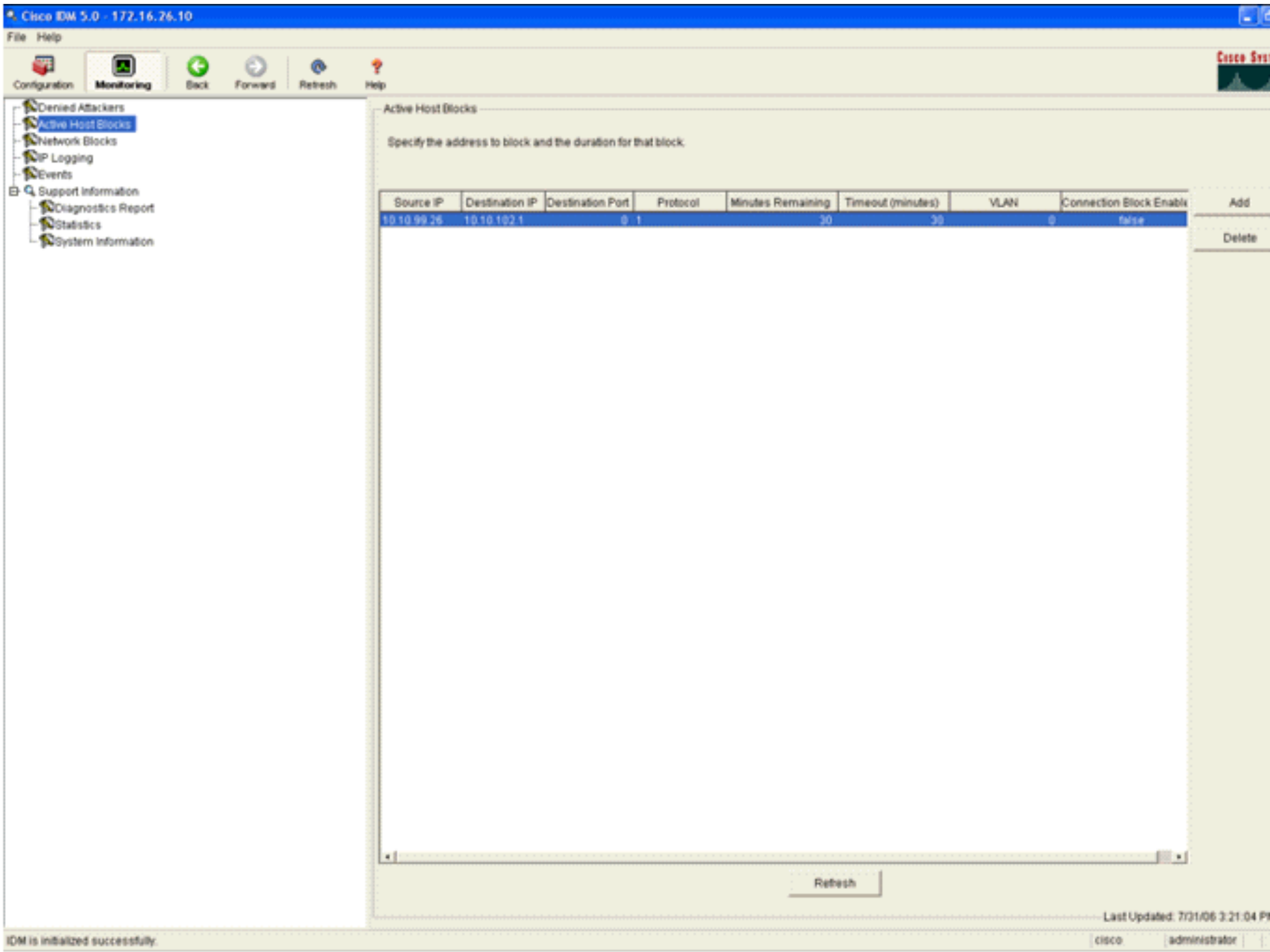
3. Click **OK** in order to save the signature.
4. Verify that the signature is active and that it is set to perform a blocking action.
5. Click **Apply** in order to commit the signature to the module.

Monitor Blocking and Events with IDM

Complete these steps:

1. When the signature fires successfully, there are two places within IDM to note this.

   The first method shows the active blocks that the AIP−SSM has installed. Click **Monitoring** along the top row of actions. Within the list of items that appears on the left−hand side, select **Active Host Blocks**. Whenever the ping signature triggers, the Active Host Blocks window shows the IP address of the offender, the address of the device under attack, and the time that remains for which the block is in effect. The default blocking time is 30 minutes and is tunable. However, changing this value is not discussed in this document. Consult the ASA configuration documentation as necessary for information on how to change this parameter. Remove the block immediately, select it from the list and then click **Delete**.



Active Host Blocks

Specify the address to block and the duration for that block.

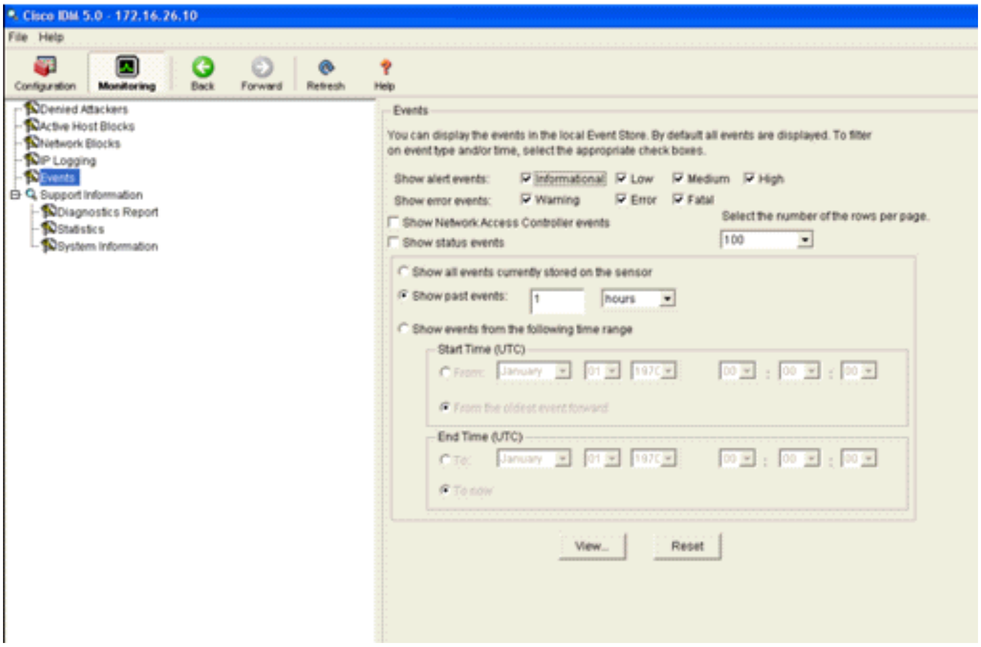
Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	VLAN	Connection Block Enabl
10.10.99.26	10.10.102.1	0	1	30	30	0	false

Last Updated: 7/31/06 3:21:04 P

IDM is initialized successfully.

cisco administrator

The second method to view triggered signatures uses the AIP−SSM event buffer. From the IDM Monitoring page, select **Events** in the items list on the left−hand side. The Events search utility appears. Set appropriate search criteria and click **View...**.



Events

You can display the events in the local Event Store. By default all events are displayed. To filter on event type and/or time, select the appropriate check boxes.

Show alert events: ☑ Informational ☑ Low ☑ Medium ☑ High

Show error events: ☑ Warning ☑ Error ☑ Fatal

☐ Show Network Access Controller events

☐ Show status events

Select the number of the rows per page. 100

○ Show all events currently stored on the sensor

● Show past events: 1 hours

○ Show events from the following time range

Start Time (UTC)

○ From: January 01 1970 00 : 00 : 00

● From the oldest event forward

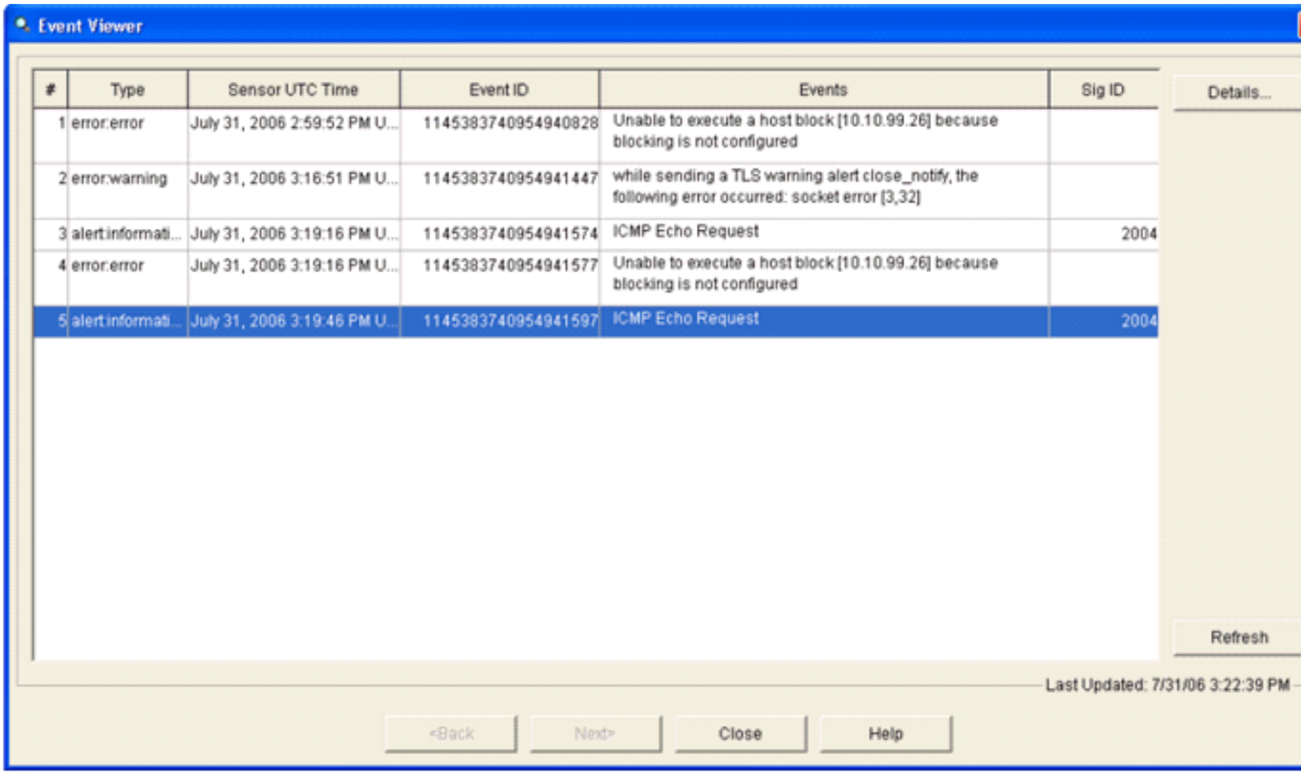
End Time (UTC)

○ To: January 01 1970 00 : 00 : 00

● To now

2. The Event Viewer then appears with a list of events that match the criteria given. Scroll through the list and find the ICMP Echo Request signature modified in the previous configuration steps.

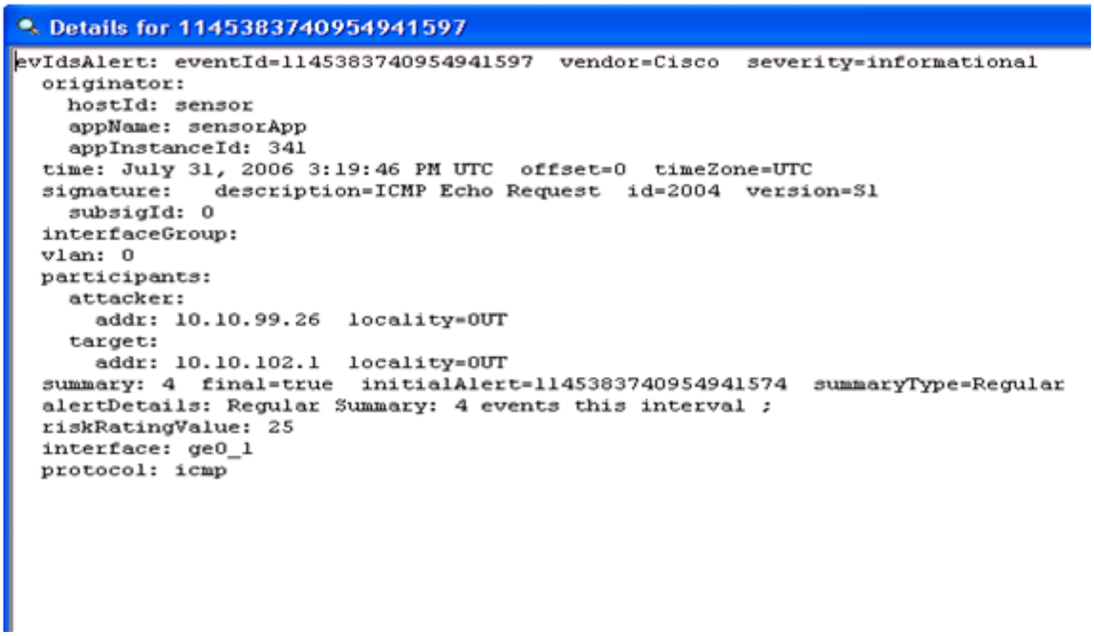
Look in the Events column for the name of the signature, or else search for the identification number of the signature under the Sig ID column.



#	Type	Sensor UTC Time	Event ID	Events	Sig ID
1	error:error	July 31, 2006 2:59:52 PM U...	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured	
2	error:warning	July 31, 2006 3:16:51 PM U...	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]	
3	alert:informati...	July 31, 2006 3:19:16 PM U...	1145383740954941574	ICMP Echo Request	2004
4	error:error	July 31, 2006 3:19:16 PM U...	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured	
5	alert:informati...	July 31, 2006 3:19:46 PM U...	1145383740954941597	ICMP Echo Request	2004

Last Updated: 7/31/06 3:22:39 PM

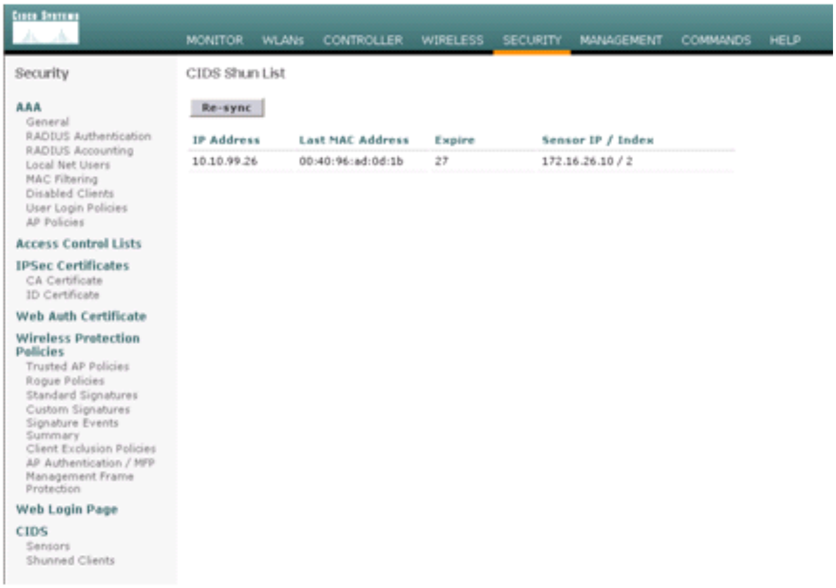
3. After you locate the signature, double−click the entry in order to open a new window. The new window contains detailed information on the event that triggered the signature.



```
evIdsAlert: eventId=1145383740954941597  vendor=Cisco  severity=informational
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 341
  time: July 31, 2006 3:19:46 PM UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: 10.10.99.26  locality=OUT
    target:
      addr: 10.10.102.1  locality=OUT
  summary: 4  final=true  initialAlert=1145383740954941574  summaryType=Regular
  alertDetails: Regular Summary: 4 events this interval ;
  riskRatingValue: 25
  interface: ge0_1
  protocol: icmp
```

Monitor Client Exclusion in a Wireless Controller

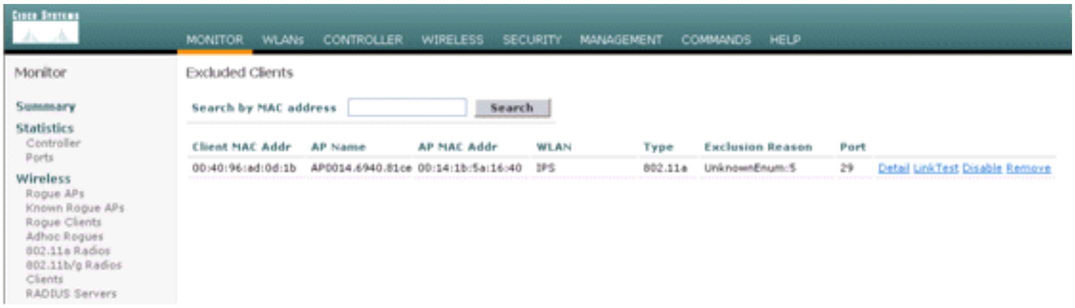
The Shunned Clients list in the controller is populated at this point of time with the IP and MAC address of the host.



CIDS Shun List

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.26	00:40:96:ad:0d:1b	27	172.16.26.10 / 2

The user is added to the Client Exclusion list.



Excluded Clients

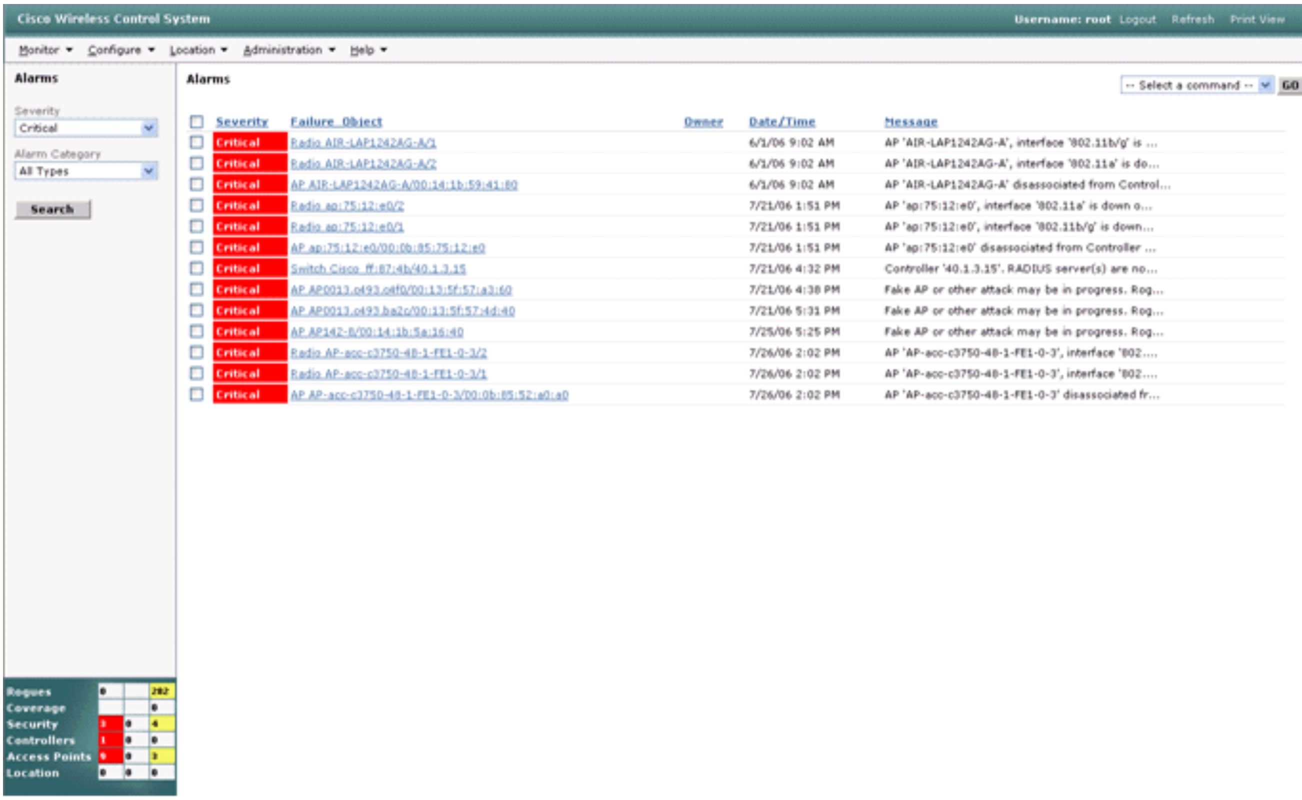
Search by MAC address

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:0d:1b	AP0014.6940.81ce	00:14:1b:5a:16:40	IPS	802.11a	UnknownEnum:5	29	Detail LinkTest Disable Remove

Monitor Events in WCS

Security events that trigger a block within the AIP−SSM cause the controller to add the address of the offender to the client exclusion list. An event is also generated within WCS.

1. Use the **Monitor** > **Alarms** utility from the WCS main menu in order to view the exclusion event. WCS initially displays all uncleared alarms and also presents a searching function on the left−hand side of the window.
2. Modify the search criteria to find the client block. Under Severity, choose **Minor**, and also set the Alarm Category to **Security**.
3. Click **Search**.



Alarms

Severity: Critical

Alarm Category: All Types

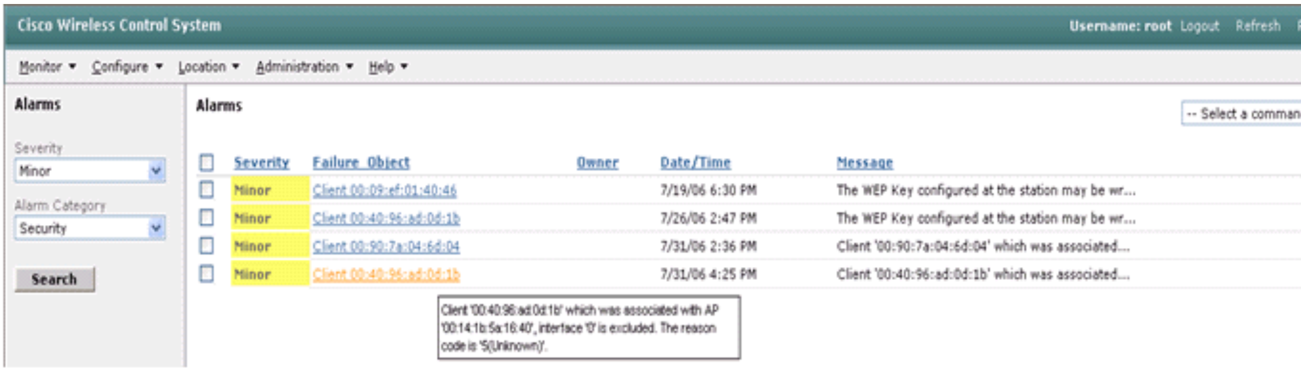
Alarms

□	Severity	Failure Object	Owner	Date/Time	Message
□	Critical	Radio AIR-LAP1242AG-A/1		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11b/g' is ...
□	Critical	Radio AIR-LAP1242AG-A/2		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11a' is do...
□	Critical	AP AIR-LAP1242AG-A/00:14:1b:59:41:80		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A' disassociated from Control...
□	Critical	Radio ap:75:12:e0/2		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11a' is down o...
□	Critical	Radio ap:75:12:e0/1		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11b/g' is down...
□	Critical	AP ap:75:12:e0/00:0b:85:75:12:e0		7/21/06 1:51 PM	AP 'ap:75:12:e0' disassociated from Controller ...
□	Critical	Switch Cisco_ff:87:4b/40.1.3.15		7/21/06 4:32 PM	Controller '40.1.3.15'. RADIUS server(s) are no...
□	Critical	AP AP0013.c493.c4f0/00:13:5f:57:a3:60		7/21/06 4:38 PM	Fake AP or other attack may be in progress. Rog...
□	Critical	AP AP0013.c493.ba2c/00:13:5f:57:4d:40		7/21/06 5:31 PM	Fake AP or other attack may be in progress. Rog...
□	Critical	AP AP142-B/00:14:1b:5a:16:40		7/25/06 5:25 PM	Fake AP or other attack may be in progress. Rog...
□	Critical	Radio AP-acc-c3750-48-1-FE1-0-3/2		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802....
□	Critical	Radio AP-acc-c3750-48-1-FE1-0-3/1		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802....
□	Critical	AP AP-acc-c3750-48-1-FE1-0-3/00:0b:85:52:a0:a0		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3' disassociated fr...

Rogues	0		282
Coverage			0
Security	3	0	4
Controllers	1	0	0
Access Points	9	0	3
Location	0	0	0

4. The Alarm window then lists only security alarms with minor severity. Point the mouse at the event that triggered the block within the AIP−SSM.

   In particular, WCS shows the MAC address of the client station that caused the alarm. By pointing at the appropriate address, WCS pops−up a small window with the event details. Click the link in order to view these same details on another window.



Alarms

Severity: Minor

Alarm Category: Security

Alarms

□	Severity	Failure Object	Owner	Date/Time	Message
□	Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr...
□	Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr...
□	Minor	Client 00:90:7a:04:6d:04		7/31/06 2:36 PM	Client '00:90:7a:04:6d:04' which was associated...
□	Minor	Client 00:40:96:ad:0d:1b		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated...

Client '00:40:96:ad:0d:1b' which was associated with AP '00:14:1b:5a:16:40', interface '0' is excluded. The reason code is '5(Unknown)'.

Cisco ASA Sample Configuration

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain−name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security−level 0
 ip address 10.10.102.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.26.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
mtu outside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
nat (inside) 102 0.0.0.0 0.0.0.0
route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.12 255.255.255.255 inside
http 0.0.0.0 0.0.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd enable management
!
class-map inside-class
 match any
!
!
policy-map inside-policy
 description IDS-inside-policy
 class inside-class
  ips promiscuous fail-open
!
```

```
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Cisco Intrusion Prevention System Sensor Sample Configuration

```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Tue Jul 25 12:15:19 2006
! ------------------------------
service host
network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0.0/8
access-list 40.0.0.0/8
exit
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2004 0
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service authentication
exit
! ------------------------------
service web-server
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
exit
! ------------------------------
service interface
exit
! ------------------------------
service trusted-certificates
exit
```

```
sensor#
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Installing and Using Cisco Intrusion Prevention System Device Manager 5.1**
- **Cisco ASA 5500 Series Adaptive Security Appliances − Configuration Guides**
- **Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.0 − Configuring Interfaces**
- **WLC Configuration Guide 4.0**
- **Wireless Technical Support**
- **Wireless LAN Controller (WLC) FAQ**
- **Wireless LAN Controller and Lightweight Access Point Basic Configuration Example**
- **Configuring Security Solutions**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map

Updated: Aug 04, 2008 Document ID: 71231