

# 无线 LAN 控制器和 IPS 集成指南

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[思科IDS概述](#)

[Cisco IDS和WLC — 集成概述](#)

[IDS顺宁](#)

[网络架构设计](#)

[配置Cisco IDS传感器](#)

[配置 WLC](#)

[Cisco IDS传感器配置示例](#)

[为IDS配置ASA](#)

[配置AIP-SSM以进行流量检测](#)

[配置WLC轮询客户端块的AIP-SSM](#)

[向AIP-SSM添加阻塞签名](#)

[使用IDM监控阻止和事件](#)

[无线控制器中的监控客户端排除](#)

[监控WCS中的事件](#)

[Cisco ASA配置示例](#)

[思科入侵防御系统传感器示例配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

思科统一入侵检测系统(IDS)/入侵防御系统(IPS)是思科自防御网络的一部分，是业内首款集成有线和无线安全解决方案。Cisco Unified IDS/IPS采用全面的安全方法 — 在无线边缘、有线边缘、广域网边缘以及通过数据中心。当关联的客户端通过思科统一无线网络发送恶意流量时，思科有线IDS设备会检测攻击并向思科无线局域网控制器(WLC)发送避开请求，然后将客户端设备取消关联。

Cisco IPS是基于网络的内联解决方案，旨在在恶意流量（包括蠕虫、间谍软件/广告软件、网络病毒和应用滥用）影响业务连续性之前，准确识别、分类和阻止它们。

借助Cisco IPS传感器软件版本5,Cisco IPS解决方案将内联防御服务与创新技术相结合，以提高准确性。结果是您完全放心地提供IPS解决方案保护，而无需担心合法流量被丢弃。Cisco IPS解决方案还通过其与其他网络安全资源协作的独特能力，为您的网络提供全面保护，并提供主动的网络保护方法。

Cisco IPS解决方案通过以下功能帮助用户更自信地阻止更多威胁：

- **准确的内联防御技术** — 提供无与伦比的信心，能够针对范围更广的威胁采取预防措施，而不会丢失合法流量。这些独特的技术可提供对数据的智能、自动的情景分析，并帮助确保您从入侵防御解决方案中获得最大收益。
- **多向量威胁识别** — 通过详细检查第2层到第7层的流量，保护您的网络免受策略违规、漏洞攻击和异常活动的影响。
- **独特的网络协作** — 通过网络协作（包括高效的流量捕获技术、负载均衡功能和对加密流量的可视性）增强可扩展性和恢复能力。
- **全面的部署解决方案** — 为所有环境提供解决方案，从中小型企业(SMB)和分支机构位置到大型企业和服务提供商安装。
- **强大的管理、事件关联和支持服务** — 支持完整的解决方案，包括配置、管理、数据关联和高级支持服务。特别是思科安全监控、分析和响应系统(MARS)可识别、隔离并建议精确删除违规元素，以实现网络范围的入侵防御解决方案。思科事件控制系统通过使网络快速适应并提供分布式响应来防止新的蠕虫和病毒爆发。

这些元素结合起来后，可提供全面的内联防御解决方案，让您有信心在最广泛的恶意流量影响业务连续性之前检测并阻止它们。思科自防御网络计划要求为网络解决方案提供集成和内置的安全性。当前基于轻量接入点协议(LWAPP)的WLAN系统仅支持基本的IDS功能，因为它本质上是第2层系统，并且线路处理能力有限。思科及时发布新代码，将新的增强功能包括到新代码中。版本4.0具有最新功能，包括将基于LWAPP的WLAN系统与Cisco IDS/IPS产品系列集成。在此版本中，目标是允许Cisco IDS/IPS系统指示WLC在从第3层到第7层的任何位置检测到攻击时阻止某些客户端访问无线网络，该攻击涉及客户端。

## [先决条件](#)

### [要求](#)

确保满足以下最低要求：

- WLC固件版本4.x及更高版本
- 需要了解如何配置Cisco IPS和Cisco WLC。

### [使用的组件](#)

#### 思科WLC

这些控制器随软件版本4.0一起提供，用于IDS修改：

- Cisco 2000 系列 WLC
- Cisco 2100 系列 WLC
- Cisco 4400 系列 WLC
- 思科无线服务模块(WiSM)
- 思科Catalyst 3750G系列统一接入交换机
- 思科无线局域网控制器模块(WLCM)

#### 访问点

- 思科Aironet 1100 AG系列轻量接入点
- 思科Aironet 1200 AG系列轻量接入点

- 思科Aironet 1300系列轻量接入点
- Cisco Aironet 1000系列轻量接入点

## 管理

- Cisco Wireless Control System (WCS)
- 思科4200系列传感器
- 思科IDS管理 — 思科IDS设备管理器(IDM)

## 思科统一IDS/IPS平台

- Cisco IPS 4200系列传感器，带Cisco IPS传感器软件5.x或更高版本。
- 适用于Cisco ASA 5500系列自适应安全设备的SSM10和SSM20，带Cisco IPS传感器软件5.x
- 带Cisco IPS传感器软件5.x的Cisco ASA 5500系列自适应安全设备
- 带Cisco IPS传感器软件5.x的Cisco IDS网络模块(NM-CIDS)
- 带Cisco IPS传感器软件5.x的Cisco Catalyst 6500系列入侵检测系统模块2(IDSM-2)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

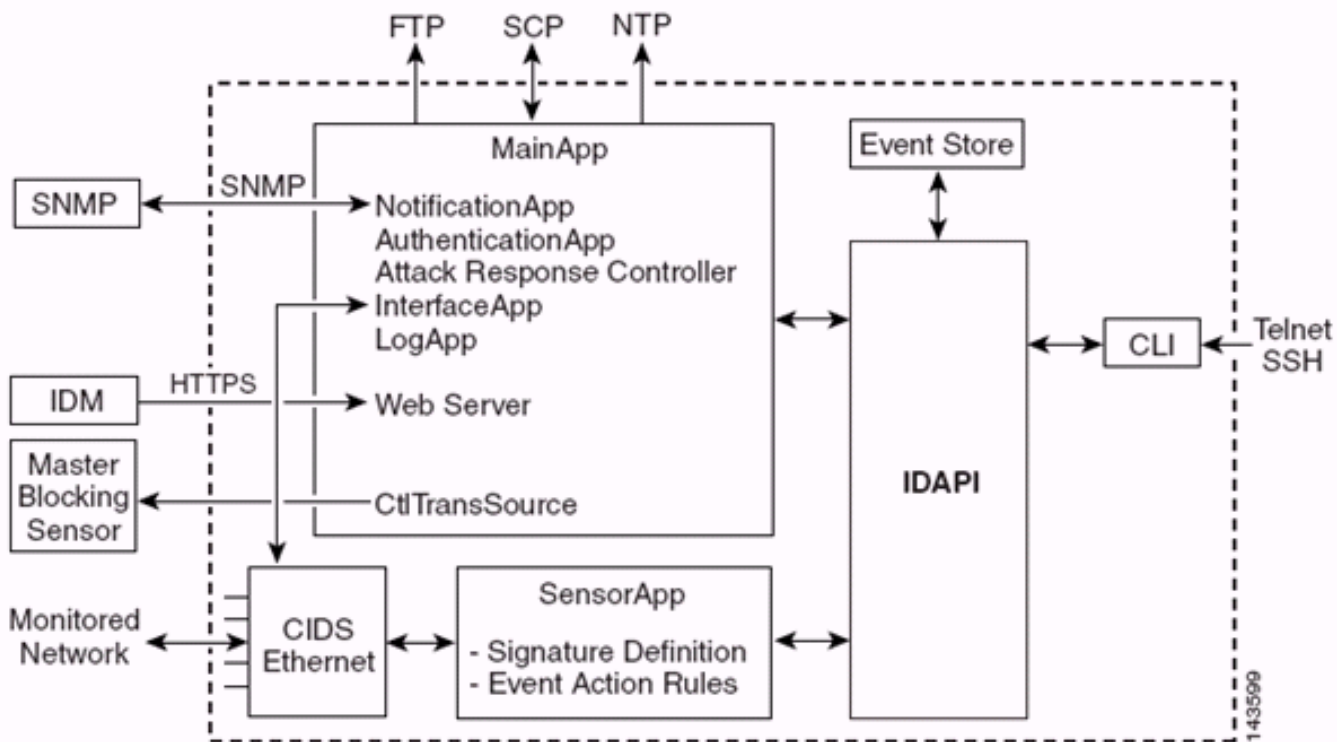
## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 思科IDS概述

思科IDS（版本5.0）的主要组件包括：

- **传感器应用** — 执行数据包捕获和分析。
- **事件存储管理和操作模块** — 提供违反策略的存储。
- **映像、安装和启动模块** — 加载、初始化和启动所有系统软件。
- **用户界面和UI支持模块** — 提供嵌入式CLI和IDM。
- **传感器OS** — 主机操作系统（基于Linux）。



传感器应用 ( IPS软件 ) 包括 :

- **主应用** — 初始化系统、启动和停止其他应用、配置操作系统并负责升级。它包含以下组件：  
**Control Transaction Server** — 允许传感器发送控制事务，这些事务用于启用攻击响应控制器（以前称为网络访问控制器）主阻塞传感器功能。  
**事件存储** — 用于存储IPS事件（错误、状态和警报系统消息）的索引存储，可通过CLI、IDM、自适应安全设备管理器(ASDM)或远程数据交换协议(RDEP)访问。
- **接口应用** — 处理旁路和物理设置并定义配对接口。物理设置包括速度、双工和管理状态。
- **Log App** — 将应用程序的日志消息写入日志文件，将错误消息写入事件存储。
- **攻击响应控制器(ARC) (以前称为网络访问控制器)** — 管理远程网络设备（防火墙、路由器和交换机），以在发生警报事件时提供阻止功能。ARC在受控网络设备上创建并应用访问控制列表(ACL)，或使用shun命令（防火墙）。
- **通知应用** — 当由警报、状态和错误事件触发时发送SNMP陷阱。为此，通知应用使用公共域SNMP代理。SNMP GET提供有关传感器运行状况的信息。  
**Web服务器 (HTTP RDEP2服务器)** — 提供Web用户界面。它还提供了通过RDEP2与其他IPS设备通信的方法，使用多个Servlet来提供IPS服务。  
**Authentication App** — 验证用户是否获得执行CLI、IDM、ASDM或RDEP操作的授权。
- **传感器应用 (分析引擎)** — 执行数据包捕获和分析。
- **CLI** — 用户通过Telnet或SSH成功登录传感器时运行的接口。通过CLI创建的所有帐户都使用CLI作为其外壳（服务帐户除外 — 仅允许一个服务帐户）。允许的CLI命令取决于用户的权限。

所有IPS应用都通过称为IDAPI的通用应用程序接口(API)相互通信。远程应用（其他传感器、管理应用和第三方软件）通过RDEP2和安全设备事件交换(SDEE)协议与传感器通信。

必须注意，传感器具有以下磁盘分区：

- **Application Partition** — 包含完整的IPS系统映像。
- **维护分区** — 用于重新映像IDSM-2的应用程序分区的特殊用途IPS映像。维护分区的重新映像会导致配置丢失。

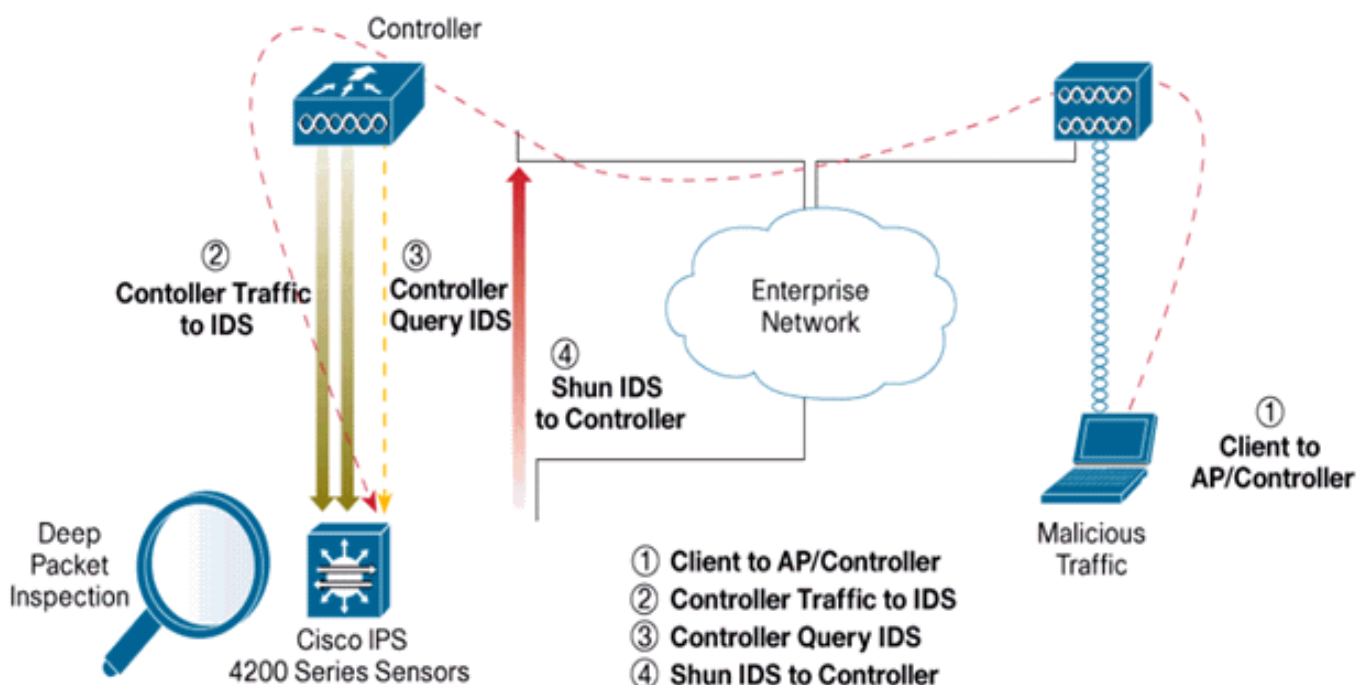
- **恢复分区** — 用于恢复传感器的特殊用途映像。通过引导到恢复分区，用户可以完全重新映像应用程序分区。网络设置将保留，但所有其他配置都将丢失。

## Cisco IDS和WLC — 集成概述

Cisco IDS的5.0版引入了在检测到策略违规（签名）时配置拒绝操作的功能。根据IDS/IPS系统中的用户配置，可以向防火墙、路由器或WLC发送避开请求，以阻止来自特定IP地址的数据包。

对于适用于思科无线控制器的思科统一无线网络软件版本4.0，需要向WLC发送避开请求，以触发控制器上可用的客户端黑名单或排除行为。控制器用于获取shun请求的接口是Cisco IDS上的命令和控制接口。

- 控制器允许在给定控制器上配置最多五个IDS传感器。
- 每个已配置的IDS传感器都由其IP地址或限定网络名称和授权凭证来标识。
- 每个IDS传感器都可以在控制器上配置唯一的查询速率（以秒为单位）。



## IDS顺宁

控制器以配置的查询速率查询传感器以检索所有避开事件。给定的避开请求分布在从IDS传感器检索请求的整个移动组中。对客户端IP地址的每个shun请求对指定的超时秒数值有效。如果超时值指示无限时间，则只有在IDS上删除了shun条目时，shun事件才会结束。即使重置任何或所有控制器，被避开的客户端状态也会在移动组中的每个控制器上保持。

**注意：**IDS传感器始终决定避开客户端。控制器不检测第3层攻击。确定客户端在第3层发起恶意攻击的过程要复杂得多。客户端在第2层进行身份验证，这足以让控制器授予第2层访问权限。

**注意：**例如，如果客户端分配了以前违规（被回避）的IP地址，则直到传感器超时才会取消阻止此新客户端的第2层访问。即使控制器在第2层提供访问，客户端流量仍可能在第3层路由器上被阻止，因为传感器也会通知路由器避开事件。

假设客户端有IP地址A。现在，当控制器轮询IDS以查找避开事件时，IDS会将避开请求发送到IP地

址为A的控制器作为目标IP地址。现在，控制器黑色列出此客户端A。在控制器上，客户端根据MAC地址禁用。

现在，假设客户端将其IP地址从A更改为B。在下次轮询中，控制器将根据IP地址获取避开的客户端列表。这一次，IP地址A仍在被回避的列表中。但是，由于客户端已将其IP地址从A更改为B（不在被回避的IP地址列表中），因此，当控制器上达到黑名单客户端的超时时间后，会释放此IP地址为B的客户端。现在，控制器开始允许此客户端使用新的IP地址B（但客户端MAC地址保持不变）。

因此，尽管客户端在控制器排除时间的持续时间内保持禁用状态，并且如果它重新获取其先前的DHCP地址，则重新排除该客户端，但如果被避开的客户端的IP地址发生更改，则不再禁用该客户端。例如，如果客户端连接到同一网络且DHCP租用超时未过期。

控制器仅支持与IDS的连接，以便客户端避开使用控制器上管理端口的请求。控制器通过传输无线客户端流量的适用VLAN接口连接到IDS进行数据包检测。

在控制器上，Disable Clients页面显示已通过IDS传感器请求禁用的每个客户端。CLI **show**命令还显示列入黑名单的客户端列表。

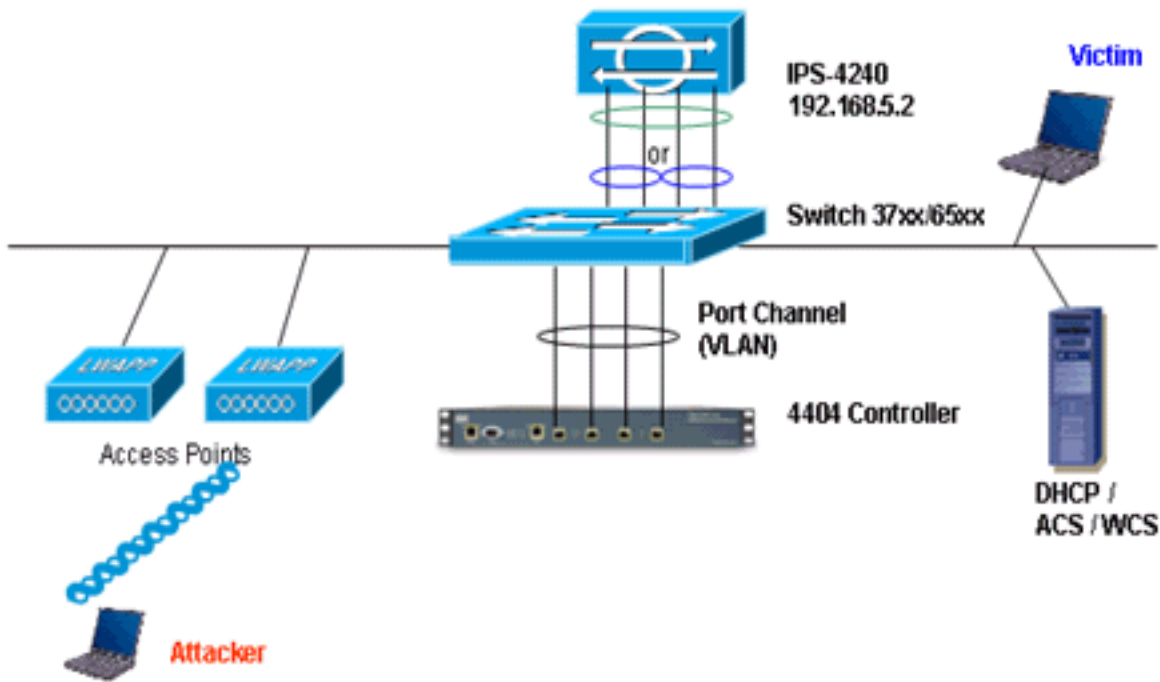
在WCS上，排除的客户端显示在Security子选项卡下。

以下是完成Cisco IPS传感器和Cisco WLC集成的步骤。

1. 在无线控制器所在的交换机上安装并连接IDS设备。
2. 镜像(SPAN)将无线客户端流量传输到IDS设备的WLC端口。
3. IDS设备接收每个数据包的副本并检查第3层到第7层的流量。
4. IDS设备提供可下载的签名文件，也可以自定义。
5. 当检测到攻击签名时，IDS设备生成警报，事件操作为shun。
6. WLC轮询IDS以获取警报。
7. 当检测到与WLC关联的无线客户端的IP地址的警报时，它会将客户端放入排除列表。
8. WLC生成陷阱，并通知WCS。
9. 在指定的时间段后，用户将从排除列表中删除。

## [网络架构设计](#)





Cisco WLC连接到Catalyst 6500上的千兆接口。为千兆接口创建端口通道，并在WLC上启用链路聚合(LAG)。

```
(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

控制器连接到Catalyst 6500上的千兆5/1和千兆5/2接口。

```
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
```

IPS传感器的感应接口可以在混杂模式下单独运行，或者您可以将它们配对，为内联感应模式创建内联接口。

在混合模式下，数据包不会通过传感器。传感器会分析受监控流量的副本，而不是实际转发的数据包。在混合模式下运行的优点是传感器不会影响转发流量的数据包流。

**注意：**体系结构图只是WLC和IPS集成架构的一个示例设置。此处显示的示例配置说明了IDS感应接口在混杂模式下工作。架构图显示了成对在内联对模式下工作的感应接口。有关内联接口模式的详细信息，请参阅[内联模式](#)。

在此配置中，假设传感接口在混杂模式下工作。Cisco IDS传感器的监控接口连接到Catalyst 6500的千兆接口5/3。在Catalyst 6500上创建监控会话，其中端口通道接口是数据包的源，目的地是连接Cisco IPS传感器监控接口的千兆接口。这会将所有入口和出口流量从控制器有线接口复制到IDS，以便进行第3层到第7层检查。

```
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#
```

## [配置Cisco IDS传感器](#)

Cisco IDS传感器的初始配置是从控制台端口完成的，或通过将显示器和键盘连接到传感器完成的。

1. 登录设备：将控制台端口连接到传感器。将显示器和键盘连接到传感器。
2. 在登录提示符下键入用户名和密码。**注意：**默认用户名和密码均为cisco。首次登录设备时，系统会提示您更改它们。您必须先输入UNIX密码，即cisco。然后您必须输入两次新密码。

```
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](mailto:export@cisco.com).

\*\*\*LICENSE NOTICE\*\*\*

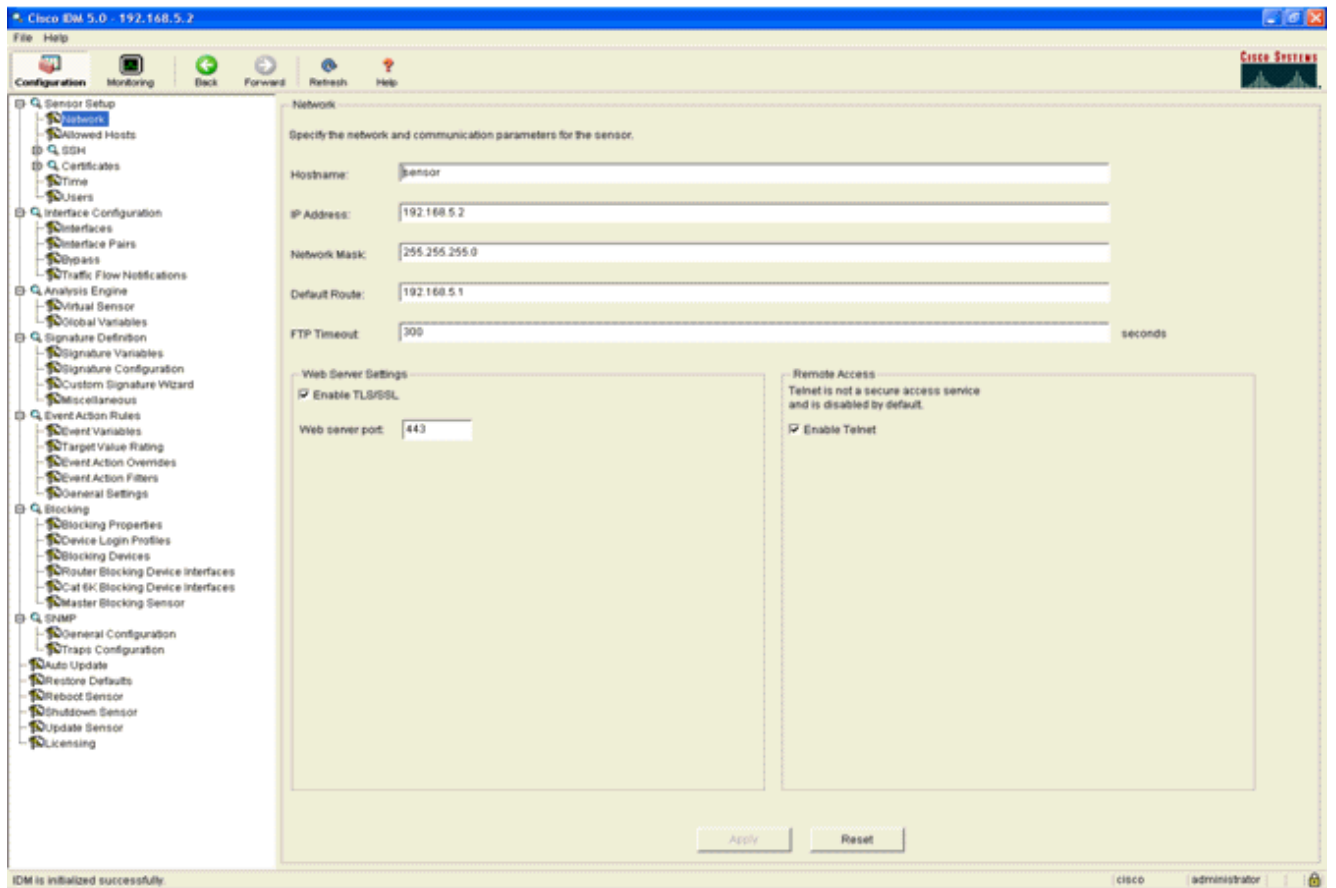
There is no license key installed on the system.

Please go to <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> (registered customers only) to obtain a new license or install a license.

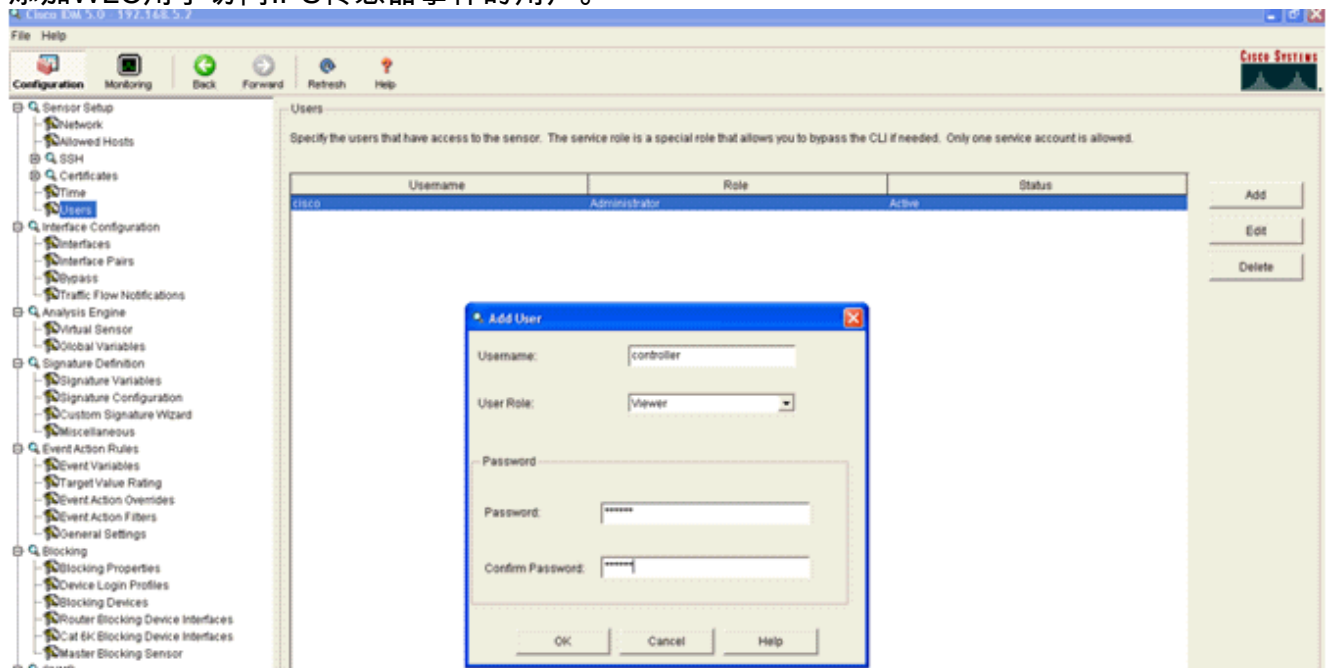
3. 在传感器上配置IP地址、子网掩码和访问列表。**注意**：这是IDS上用于与控制器通信的命令和控制接口。此地址应可路由到控制器管理接口。感应接口不需要编址。访问列表应包括控制器管理接口地址以及用于管理IDS的允许地址。

```
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#
```

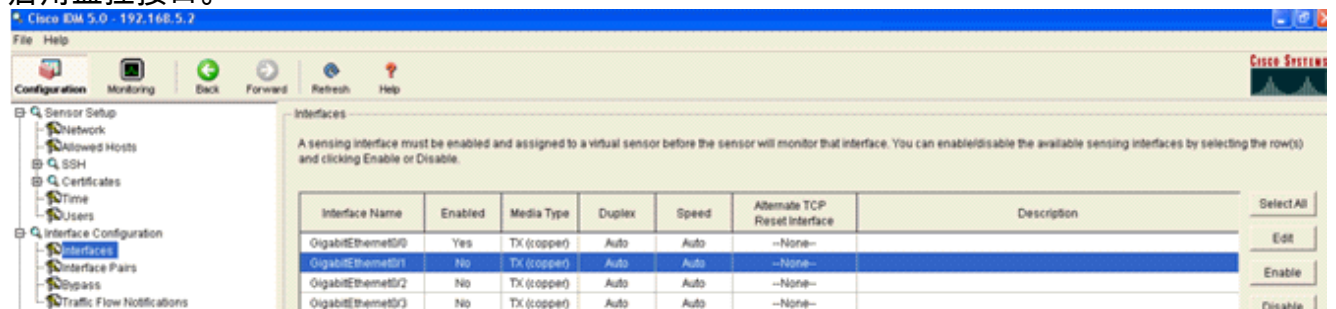
4. 现在，您可以从GUI配置IPS传感器。将浏览器指向传感器的管理IP地址。此图显示传感器配置了192.168.5.2的示例。



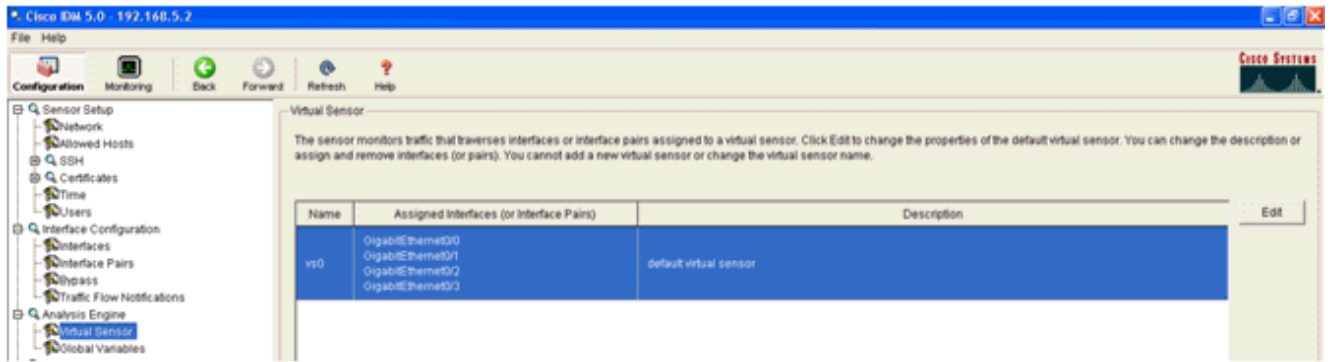
## 5. 添加WLC用于访问IPS传感器事件的用户。



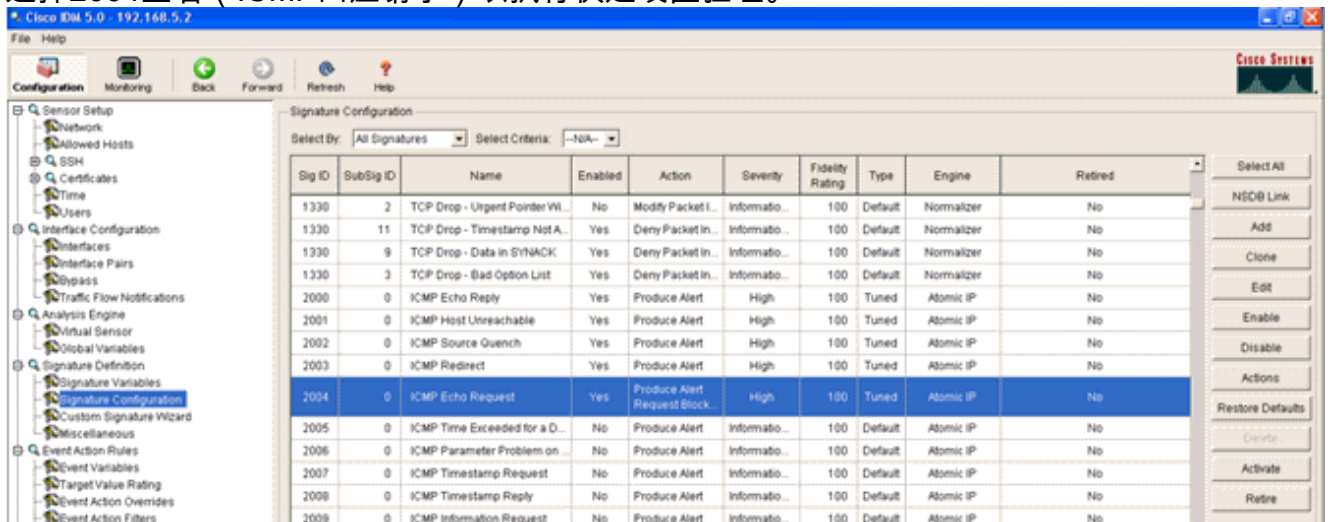
## 6. 启用监控接口。



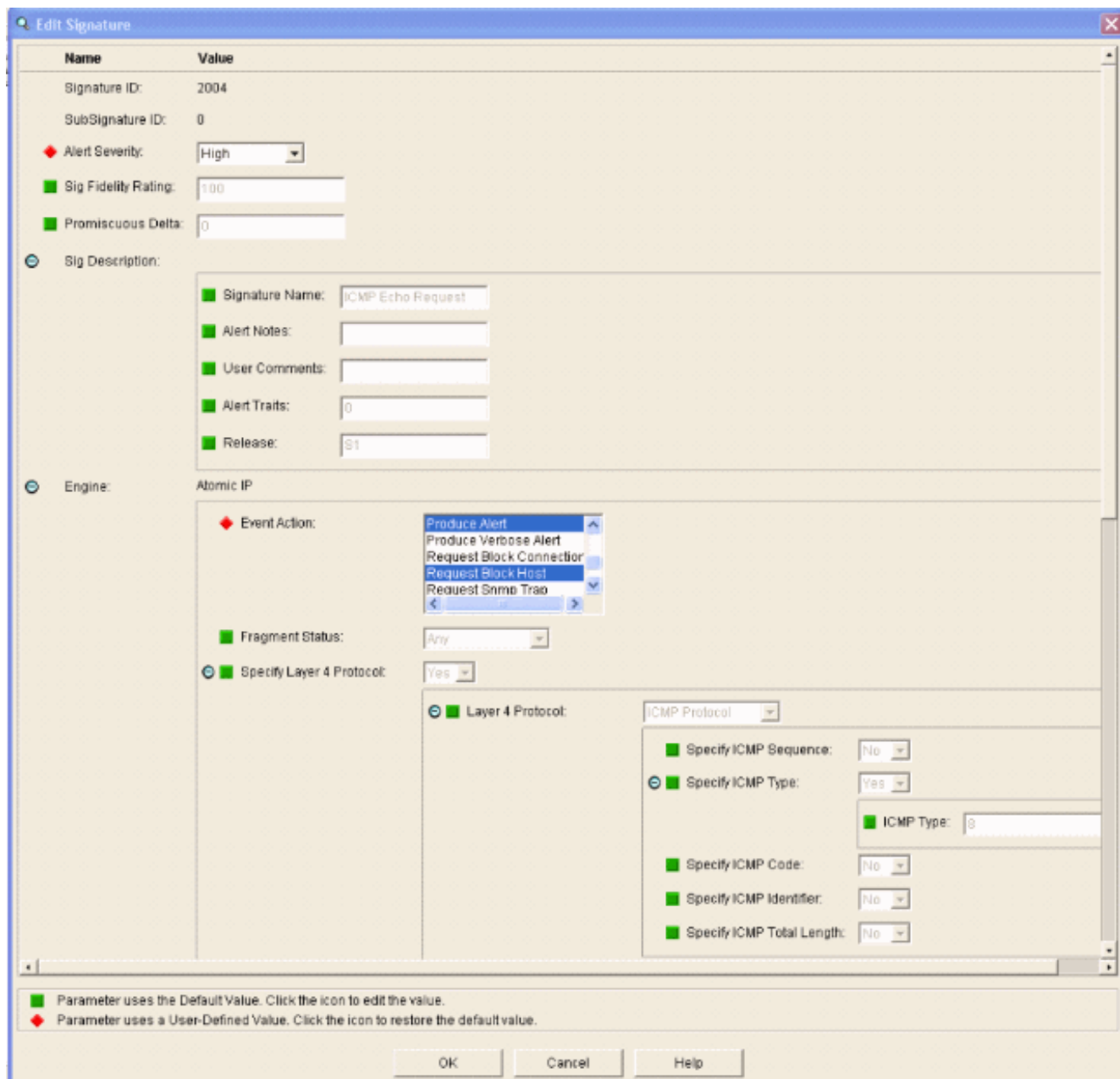
监控接口必须添加到分析引擎，如下窗口所示



7. 选择2004签名（ICMP回应请求）以执行快速设置验证。



应启用签名，将警报严重性设置为高，将事件操作设置为生成警报和请求阻止主机，以完成此验证步骤。



## 配置 WLC

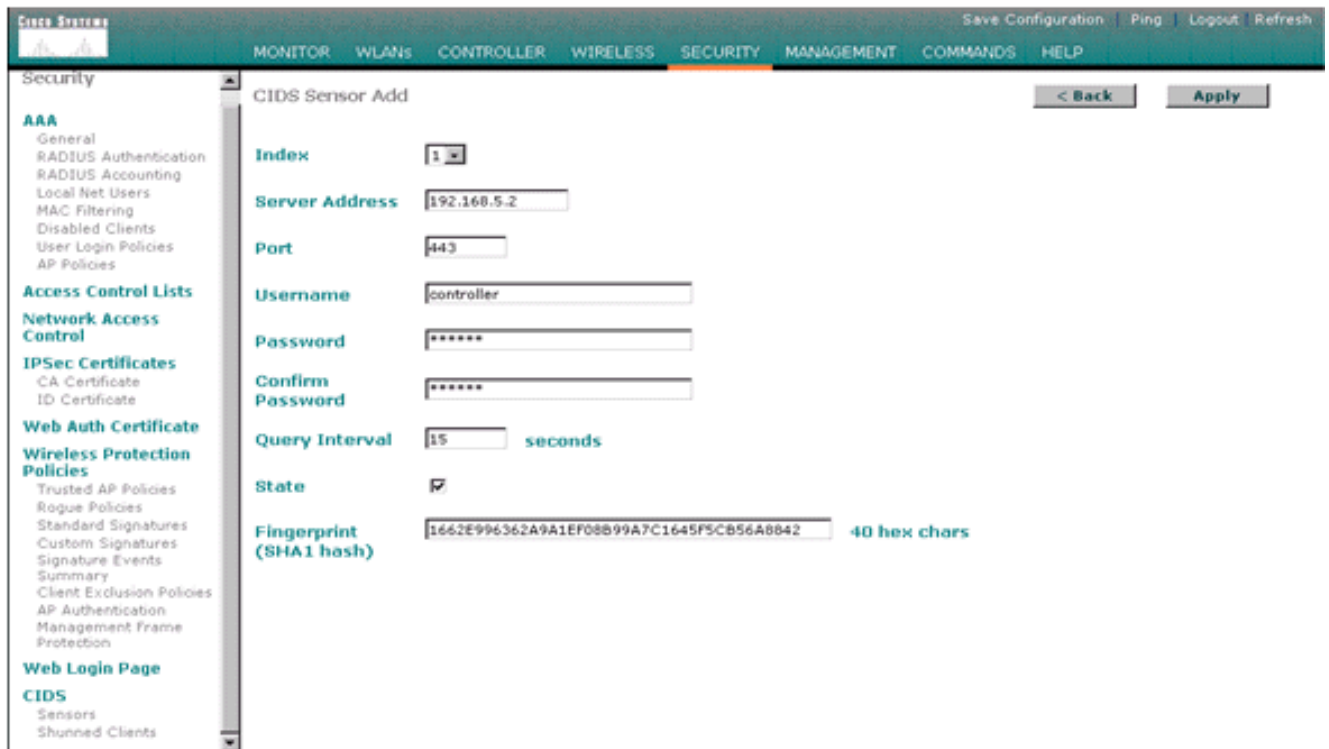
要配置WLC，请完成以下步骤：

1. 配置IPS设备并准备好在控制器中添加后，选择**Security > CIDS > Sensors > New**。
2. 添加您之前创建的IP地址、TCP端口号、用户名和密码。要从IPS传感器获取指纹，请在IPS传感器中执行此命令，并在WLC上添加SHA1指纹（不带冒号）。这用于保护控制器到IDS的轮询通信。

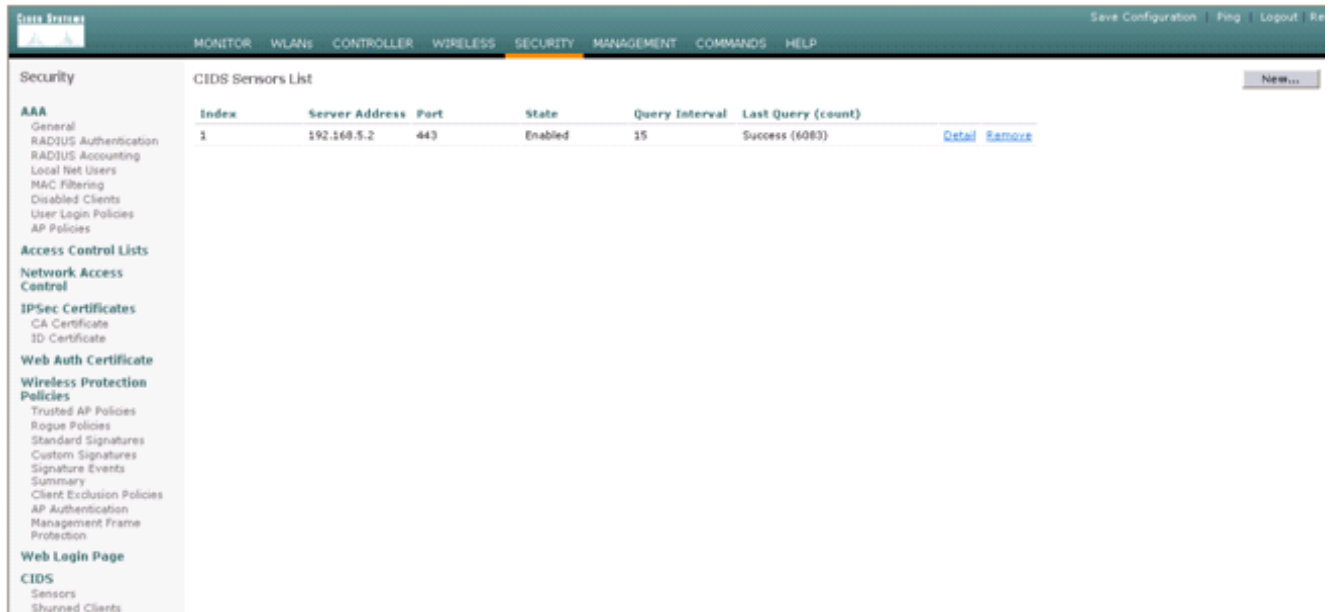
```
sensor#show tls fingerprint
```

```
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
```

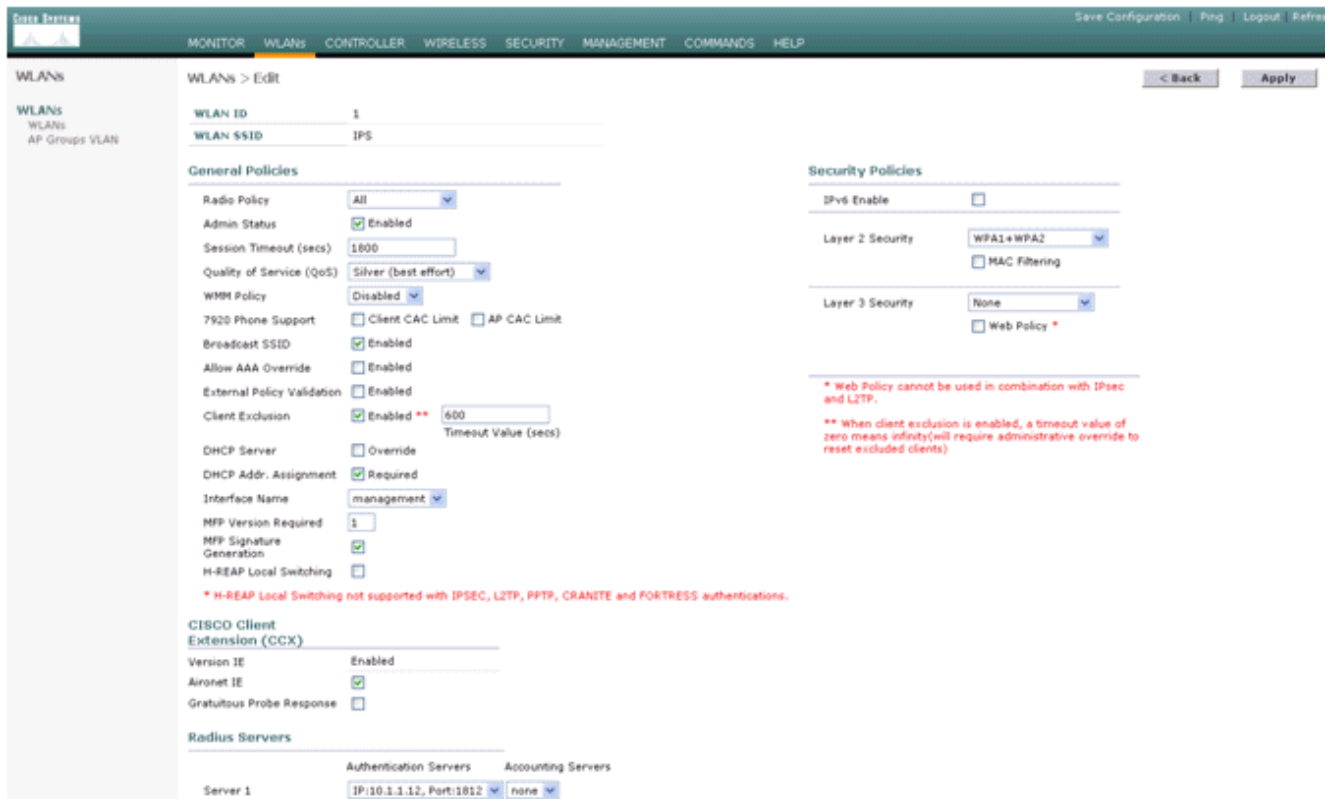
```
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



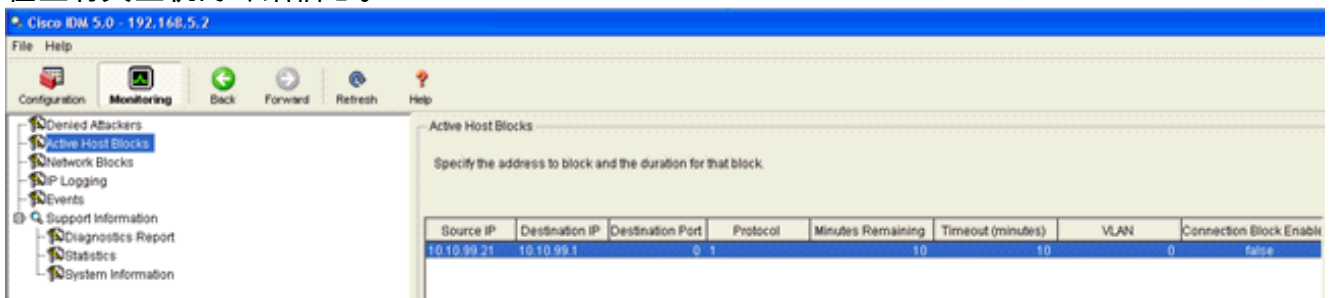
### 3. 检查IPS传感器和WLC之间连接的状态。



4. 与Cisco IPS传感器建立连接后，请确保WLAN配置正确并启用“客户端排除”。默认客户端排除超时值为60秒。另请注意，无论客户端排除计时器如何，只要IDS调用的客户端块保持活动状态，客户端排除就会持续。IDS中的默认阻止时间为30分钟。

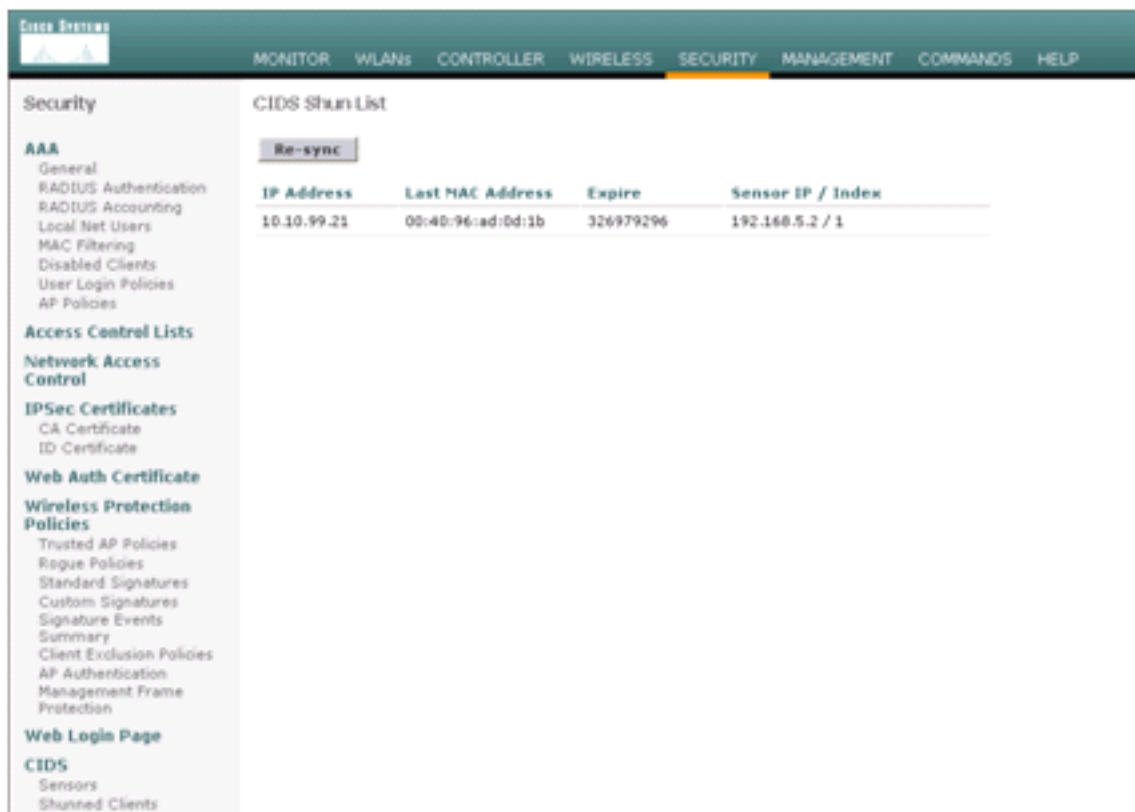


5. 当您网络中的某些设备执行NMAP扫描或对Cisco IPS传感器监控的某些主机执行ping操作时，可以触发Cisco IPS系统中的事件。在Cisco IPS中触发警报后，请转至**监控和活动主机**块以检查有关主机的详细信息。



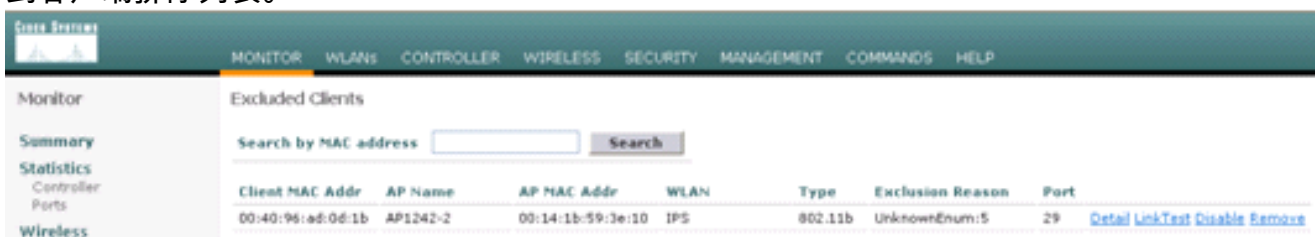
控制器中的Sived Clients列表现在填充了主机的IP和MAC地址。



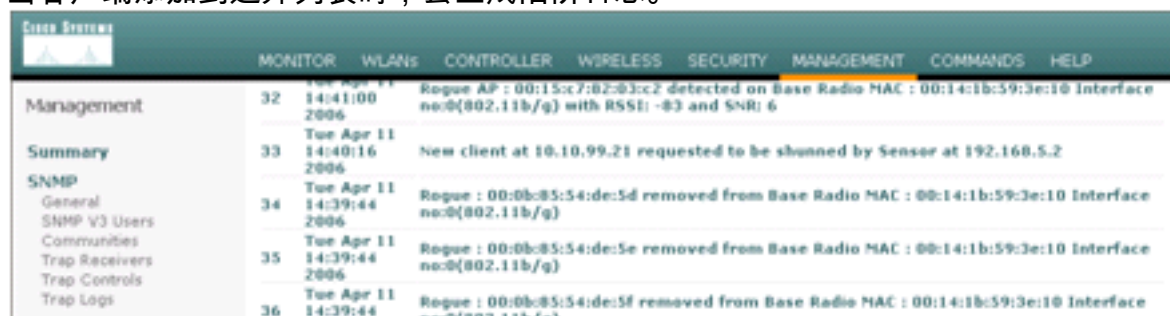


到客户端排除列表。

用户将添加

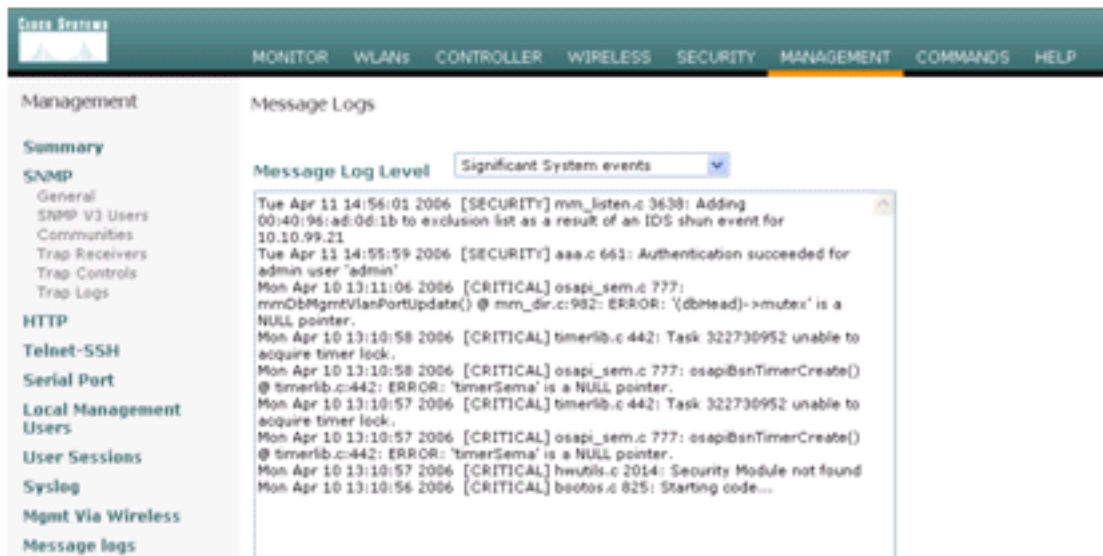


当客户端添加到避开列表时，会生成陷阱日志。

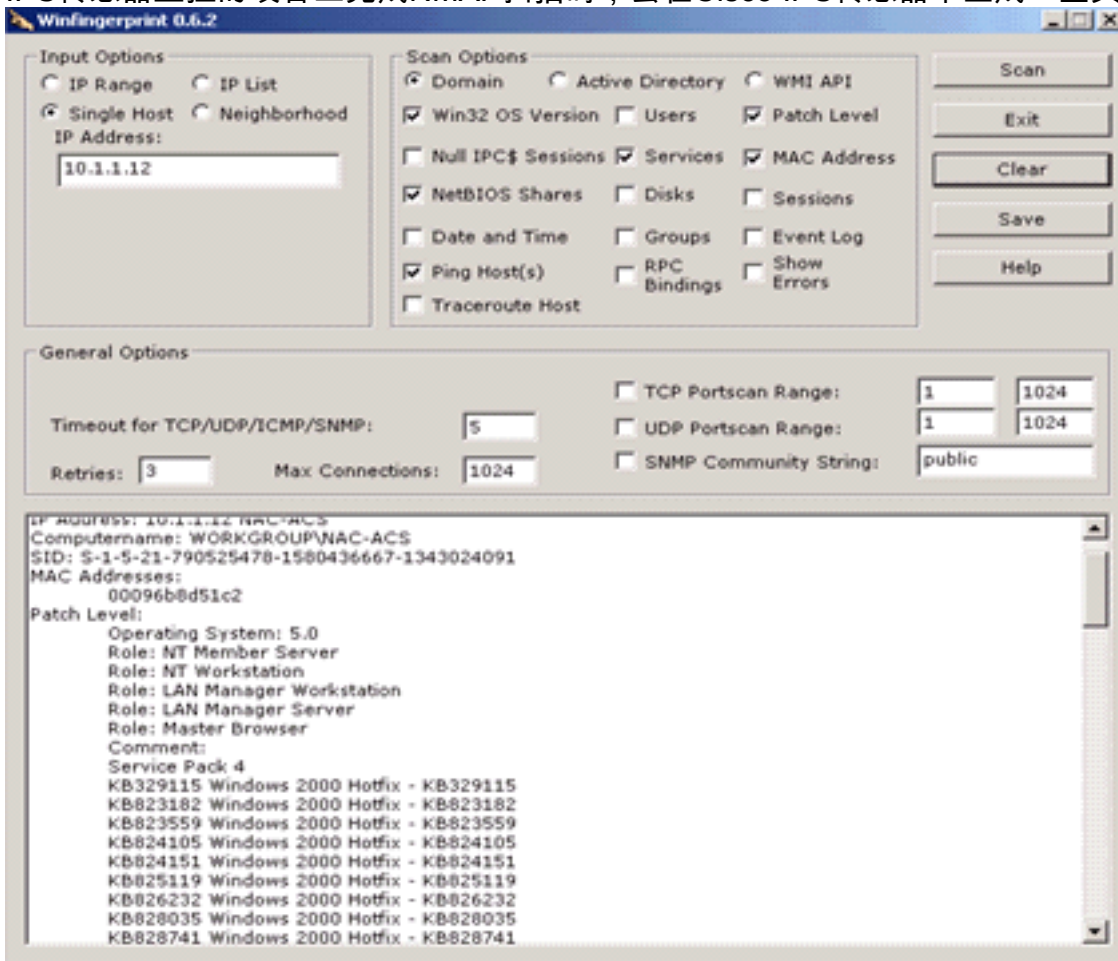


件生成消息日志。

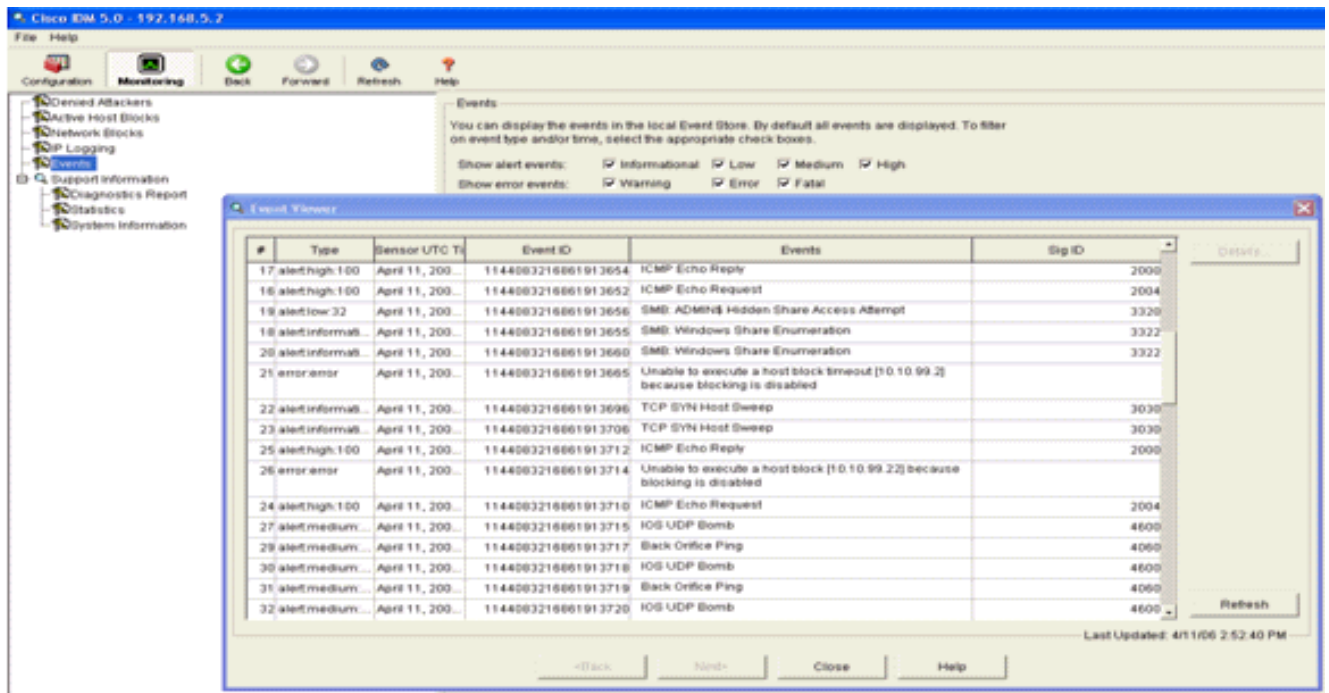
还会为事



当在Cisco IPS传感器监控的设备上完成NMAP扫描时，会在Cisco IPS传感器中生成一些其他事件。



此窗口显示在Cisco IPS传感器中生成的事件。



## Cisco IDS传感器配置示例

以下是安装脚本的输出：

```

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

```

```

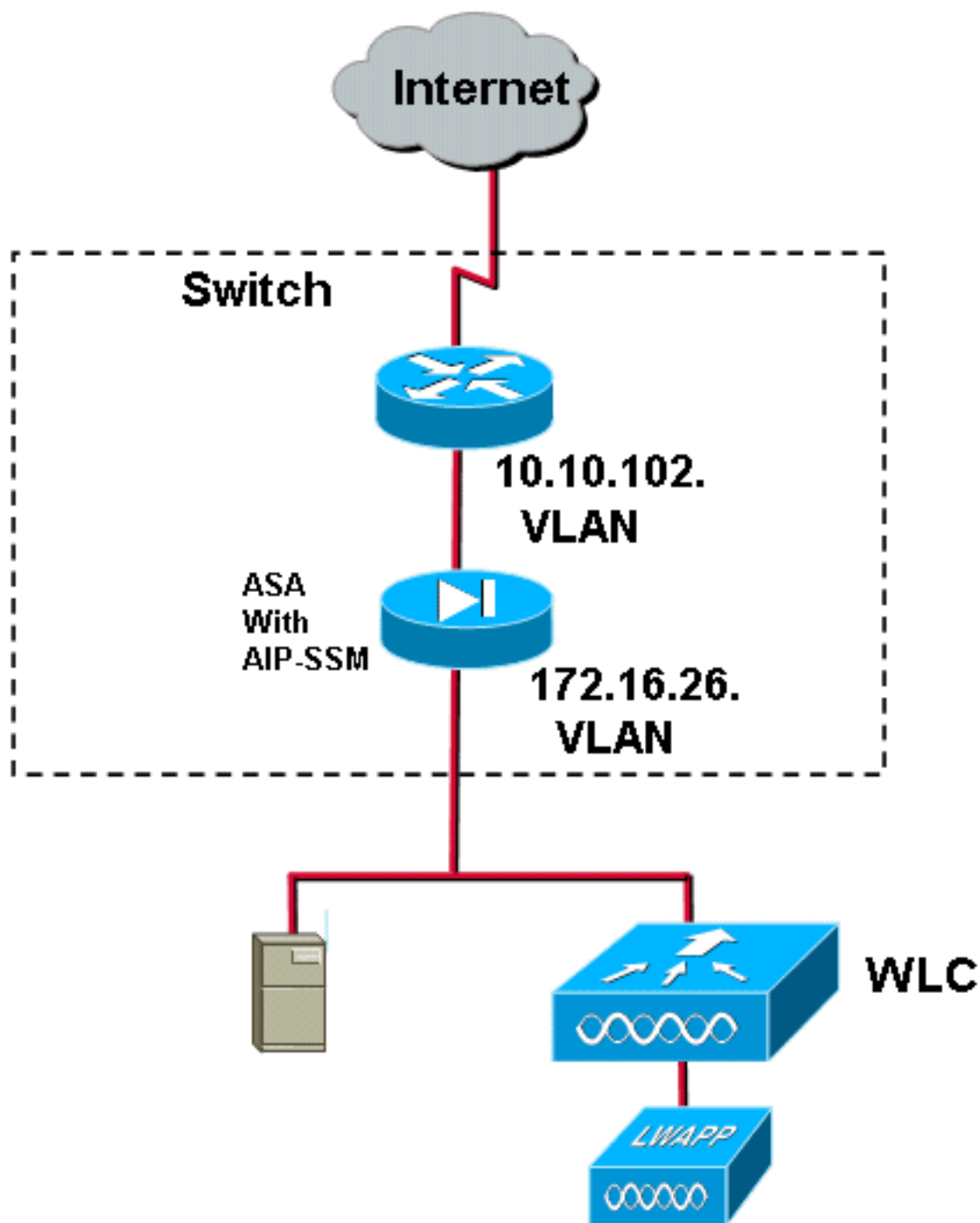
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! -----
service event-action-rules 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#

```

## [为IDS配置ASA](#)

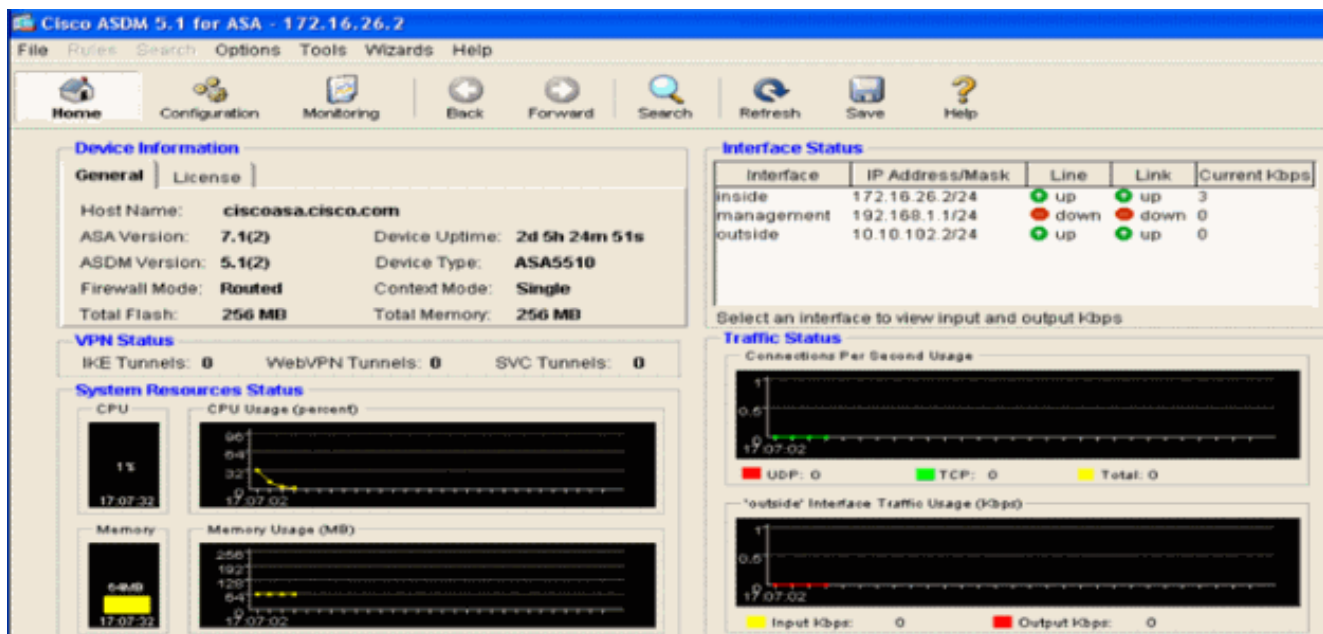
与传统的入侵检测传感器不同，ASA必须始终在数据路径中。换句话说，ASA必须在一个接口上接收数据，在内部进行处理，然后将数据从另一个端口转发出去，而不是将流量从交换机端口传输到

传感器上的被动嗅探端口。对于IDS，请使用模块化策略框架(MPF)将ASA接收的流量复制到内部高级检测和防御安全服务模块(AIP-SSM)进行检测。

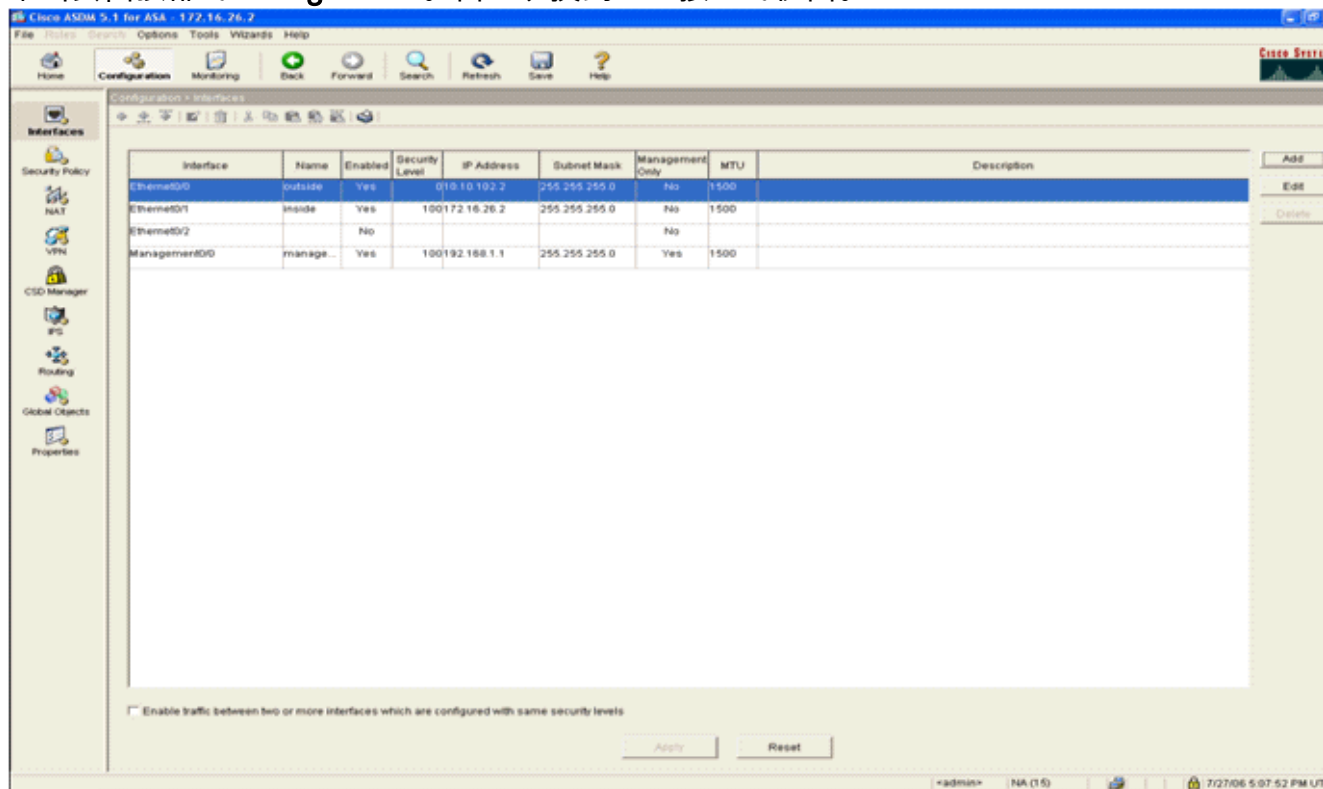


在本例中，使用的ASA已设置并传递流量。这些步骤演示如何创建将数据发送到AIP-SSM的策略。

1. 使用ASDM登录ASA。成功登录后，系统将显示ASA Main System窗口。

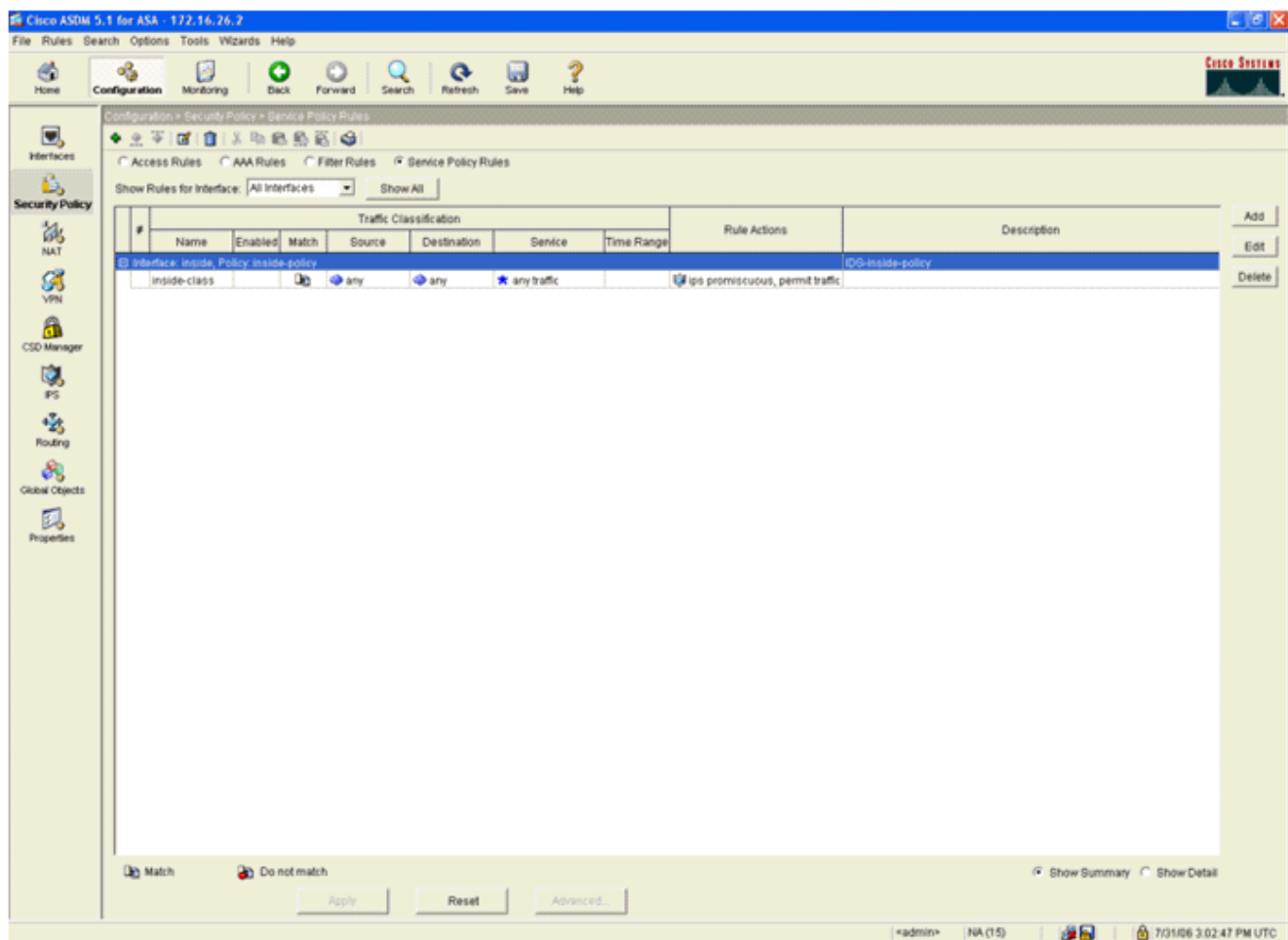


2. 单击页面顶部的 Configuration。窗口切换到 ASA 接口的视图。



3. 单击窗口左侧的 Security Policy。在结果窗口中，选择服务策略规则选项卡。





- 单击**Add**以创建新策略。添加服务策略规则向导将在新窗口中启动。单击**Interface**，然后从下拉列表中选择正确的接口，以创建一个新策略，该策略绑定到传递流量的接口之一。使用两个文本框为策略指定名称和说明。单击**Next**以转到下一步。

**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:

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

< Back   Next >   Cancel   Help

5. 构建新的流量类以应用到策略。构建特定类以检查特定数据类型是合理的，但在本例中，为简单起见，选择Any Traffic。单击**Next**以继续。

**Add Service Policy Rule Wizard - Traffic Classification Criteria**

Create a new traffic 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

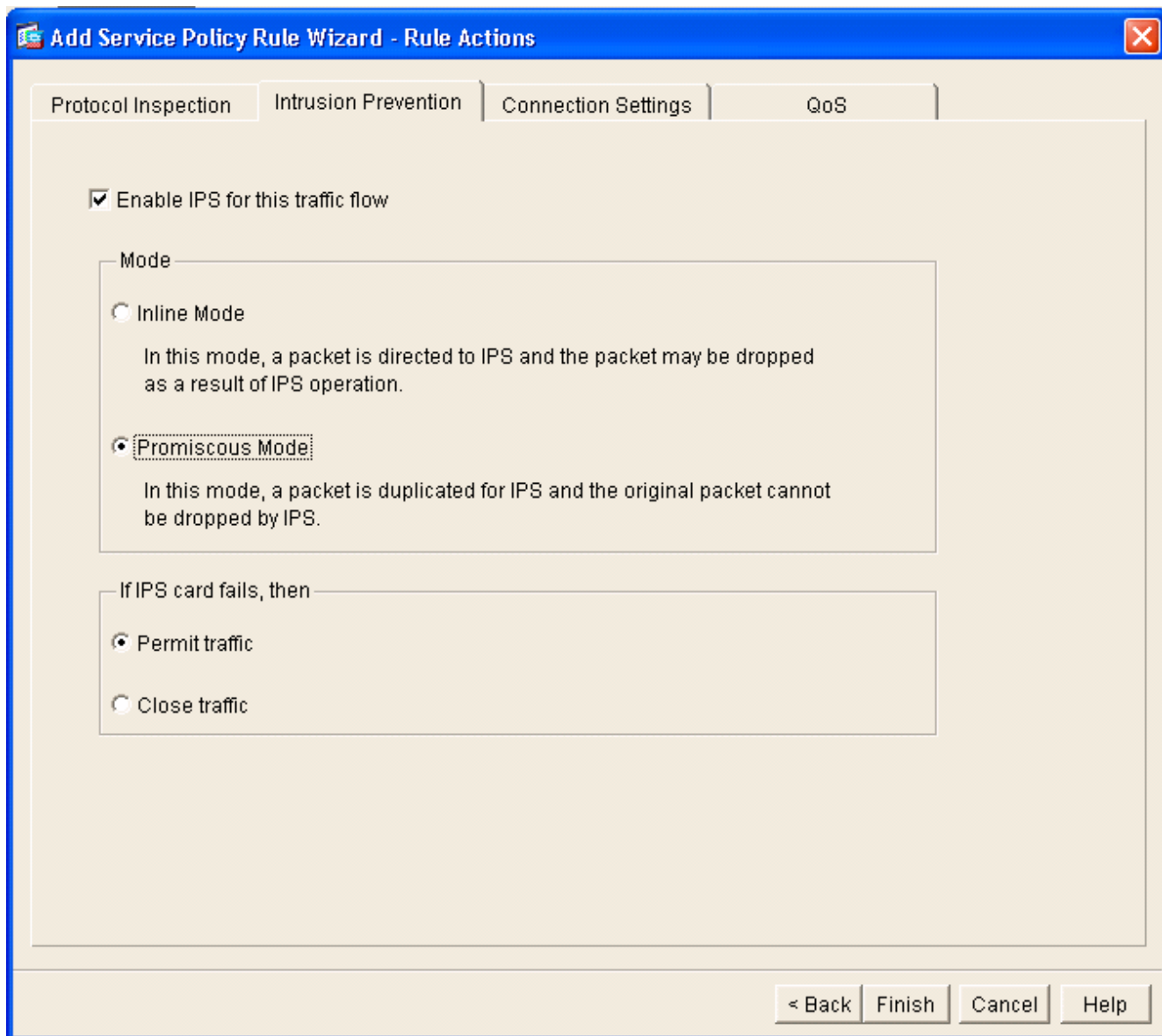
Any traffic

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.

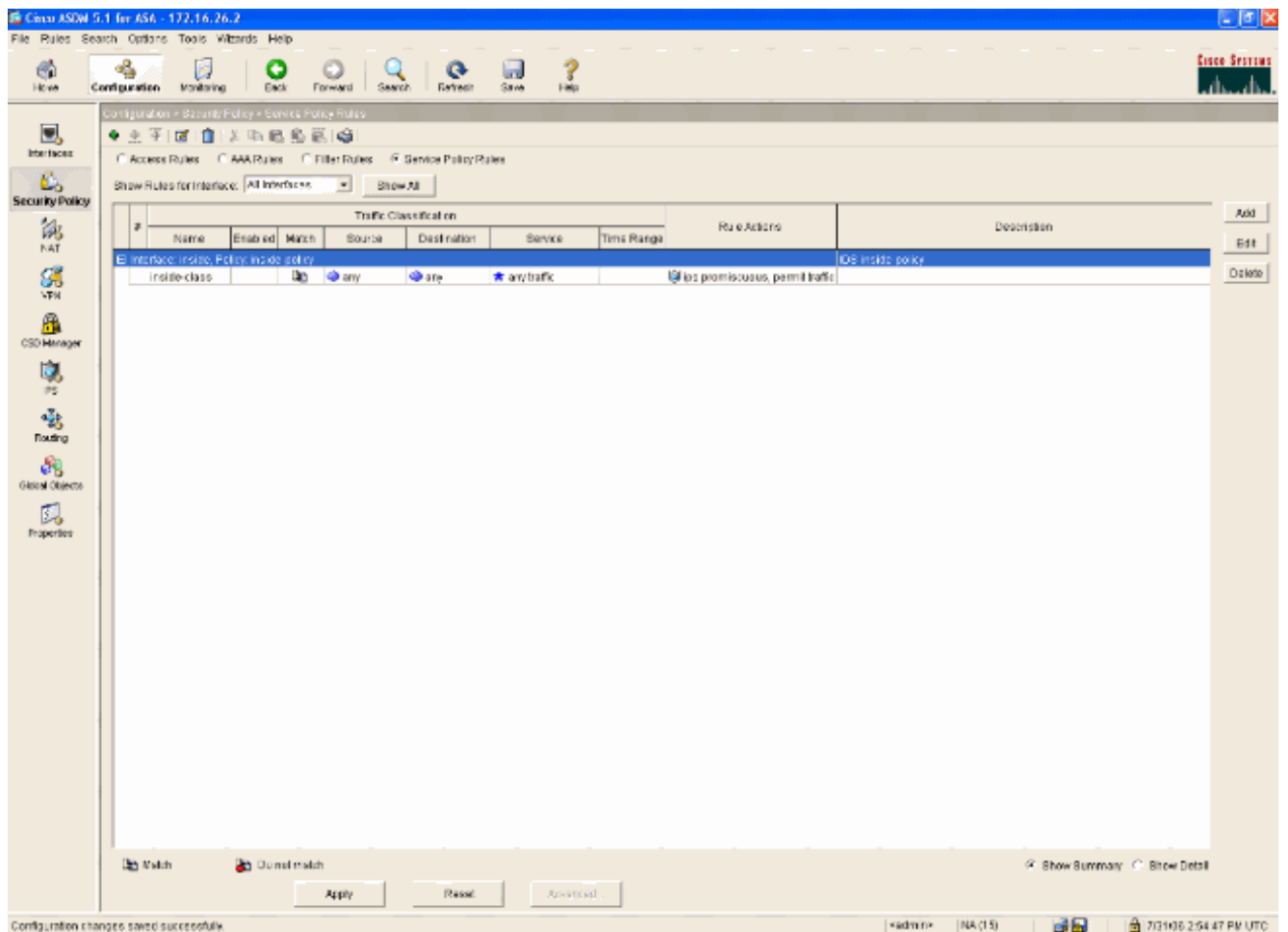
Use class-default as the traffic class.

< Back   Next >   Cancel   Help

6. 完成以下步骤以指示ASA将流量转发到其AIP-SSM。选中**Enable IPS for this traffic flow**以启用入侵检测。将模式设置为**Promiscuous**，以便流量的副本以带外方式发送到模块，而不是将模块与数据流内联。单击**Permit traffic**以确保ASA在AIP-SSM发生故障时切换到失效开放状态。单击**Finish**以提交更改。



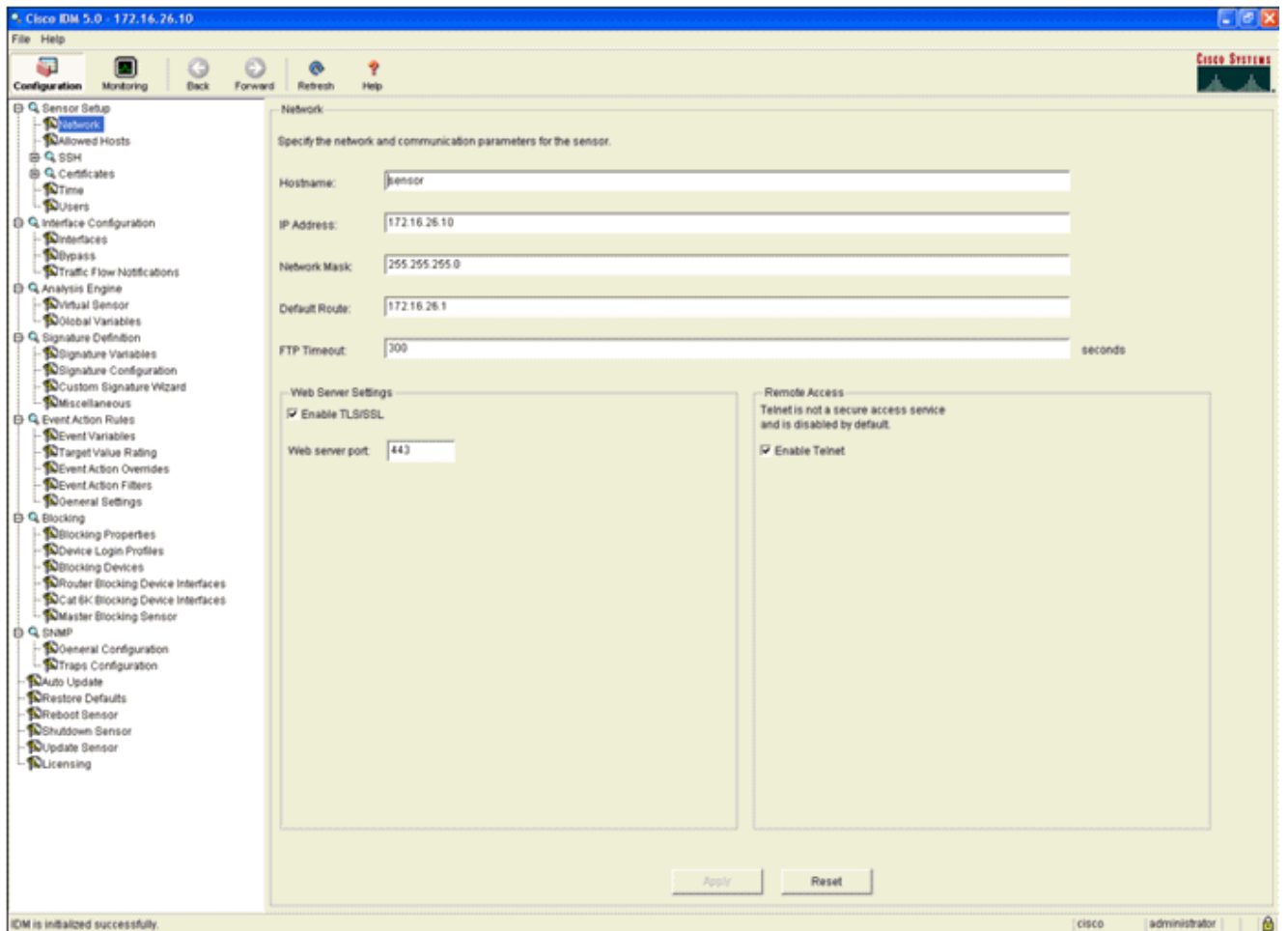
7. 现在，ASA已配置为将流量发送到IPS模块。单击顶行上的**Save**，将更改写入ASA。



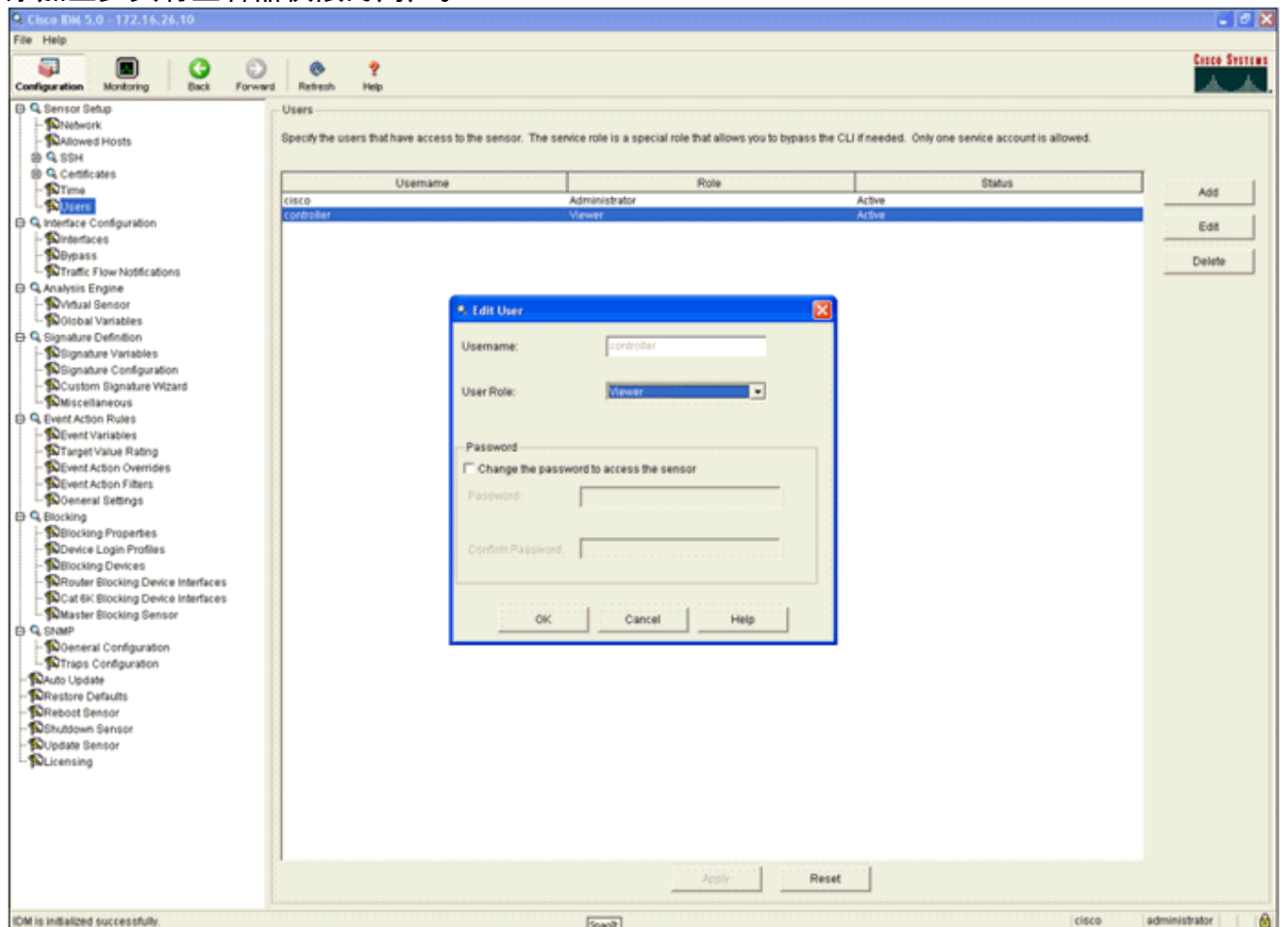
## 配置AIP-SSM以进行流量检测

当ASA向IPS模块发送数据时，将AIP-SSM接口关联到其虚拟传感器引擎。

1. 使用IDM登录AIP-SSM。

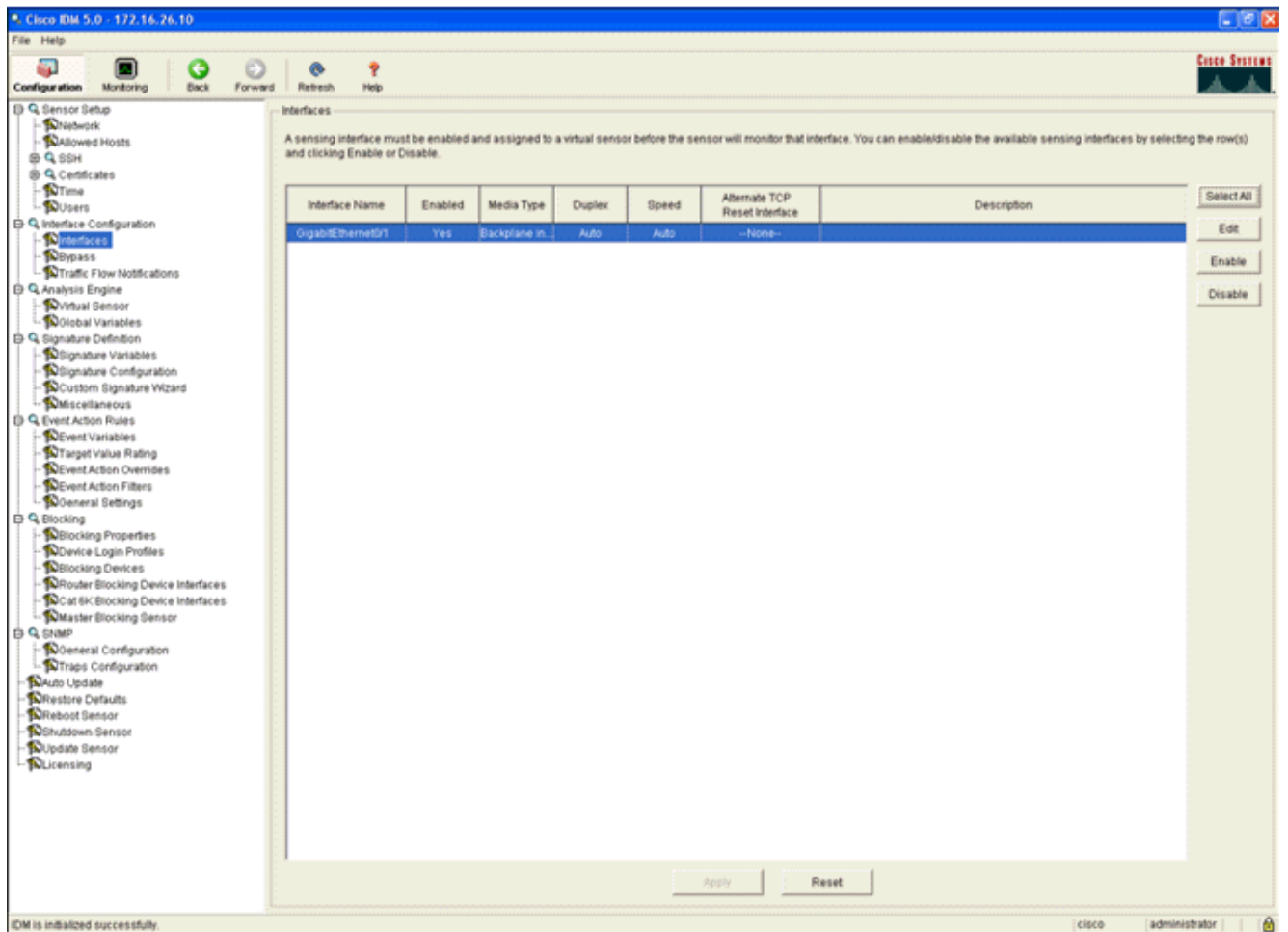


2. 添加至少具有查看器权限的用户。

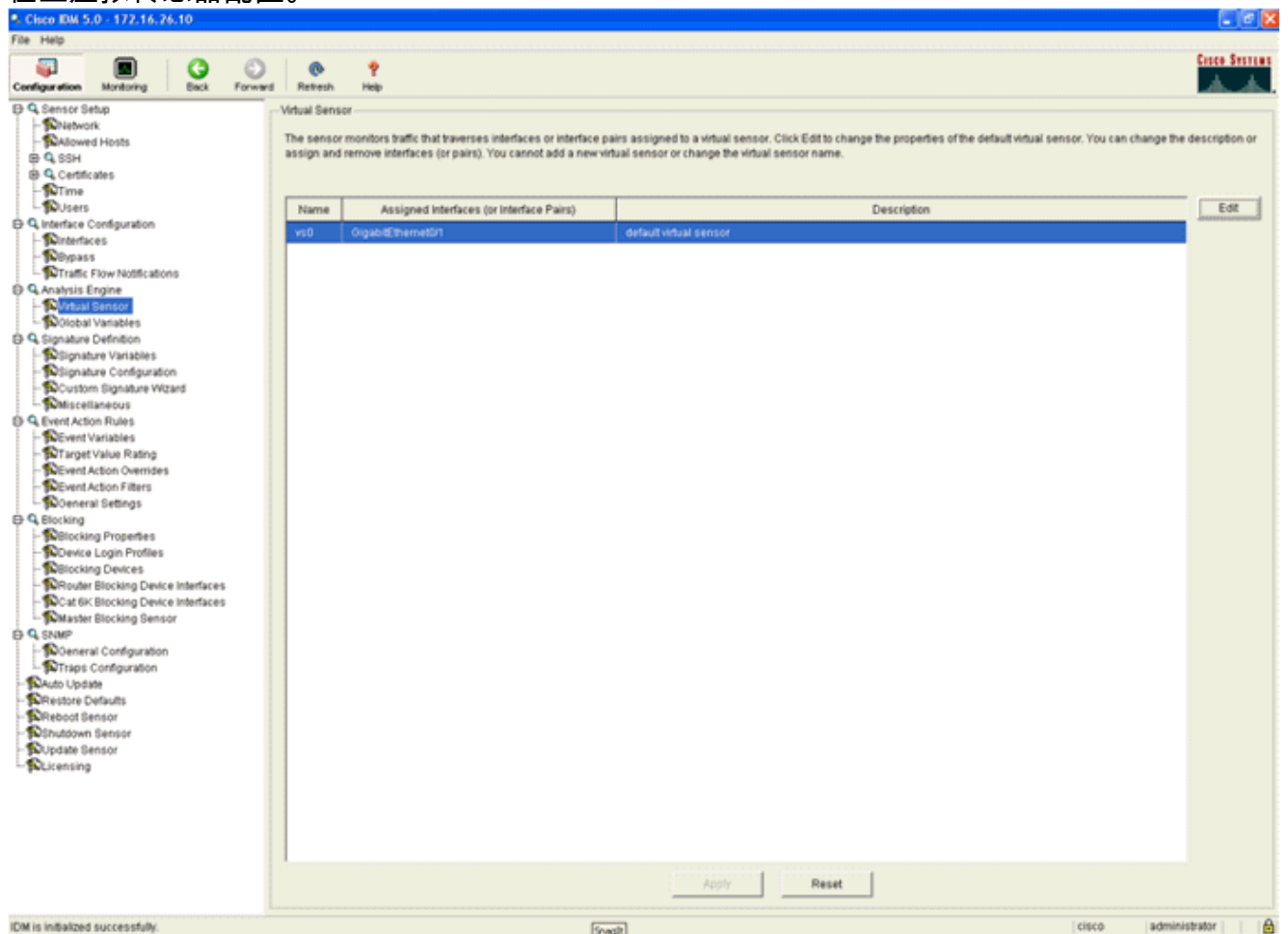


3. 启用该接口。





#### 4. 检查虚拟传感器配置。



## 配置WLC轮询客户端块的AIP-SSM

配置好传感器并准备好添加到控制器中后，请完成以下步骤：

1. 在WLC中选择**Security > CIDS > Sensors > New**。
2. 添加您在上一节中创建的IP地址、TCP端口号、用户名和密码。
3. 要从传感器获取指纹，请在传感器中执行此命令，并在WLC上添加SHA1指纹（不带冒号）。

```
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
```

The screenshot displays the Cisco WLC web interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'SECURITY' tab is selected. On the left, a sidebar menu lists various security settings under categories like AAA, Access Control Lists, and Wireless Protection Policies. The main content area is titled 'CIDS Sensor Edit' and shows the following configuration details:

Index	2
Server Address	172.16.26.10
Port	443
Username	controller
Password	*****
State	<input checked="" type="checkbox"/>
Query Interval	10 seconds
Fingerprint (SHA1 hash)	98C9969B4EFA74F8528092BBBC483C45B4876C55 40 hex chars (hash key is already set)
Last Query (count)	Success (1400)

4. 检查AIP-SSM和WLC之间连接的状态。

The screenshot shows the Cisco ICM 5.0 Security page. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, and Web Login Page. The main content area displays the 'CIDS Sensors List' table.

Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Unauthorized (1)	<a href="#">Detail</a> <a href="#">Remove</a>
2	172.16.26.10	443	Enabled	10	Success (1444)	<a href="#">Detail</a> <a href="#">Remove</a>

## 向AIP-SSM添加阻塞签名

添加检查签名以阻止流量。虽然有许多签名可以根据可用工具执行此工作，但此示例创建的签名会阻止ping数据包。

1. 选择2004签名 (ICMP回应请求) 以执行快速设置验证。

The screenshot shows the Cisco ICM 5.0 Signature Configuration page. The left sidebar shows a tree view with 'Signature Configuration' selected. The main content area displays a table of signatures.

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired	
1330	2	TCP Drop - Urgent Pointer VI...	No	Modify Packet L...	Informatio...	100	Default	Normalizer	No	Select All
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No	NSDB Link
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No	Add
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No	Clone
2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edit
2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Enable
2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Actions
2004	0	ICMP Echo Request	Yes	Produce Alert Request Block...	High	100	Tuned	Atomic IP	No	Restore Defaults
2005	0	ICMP Time Exceeded for a D...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No	Create
2006	0	ICMP Parameter Problem on ...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No	Activate
2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No	Retire
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. 启用签名，将Alert Severity设置为High，并将Event Action设置为Produce Alert和Request Block Host，以完成此验证步骤。请注意，Request Block Host操作是向WLC发出信号以创建客户端异常的关键。

**Edit Signature**

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: B1

**Engine:** Atomic IP

Event Action: Produce Alert

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

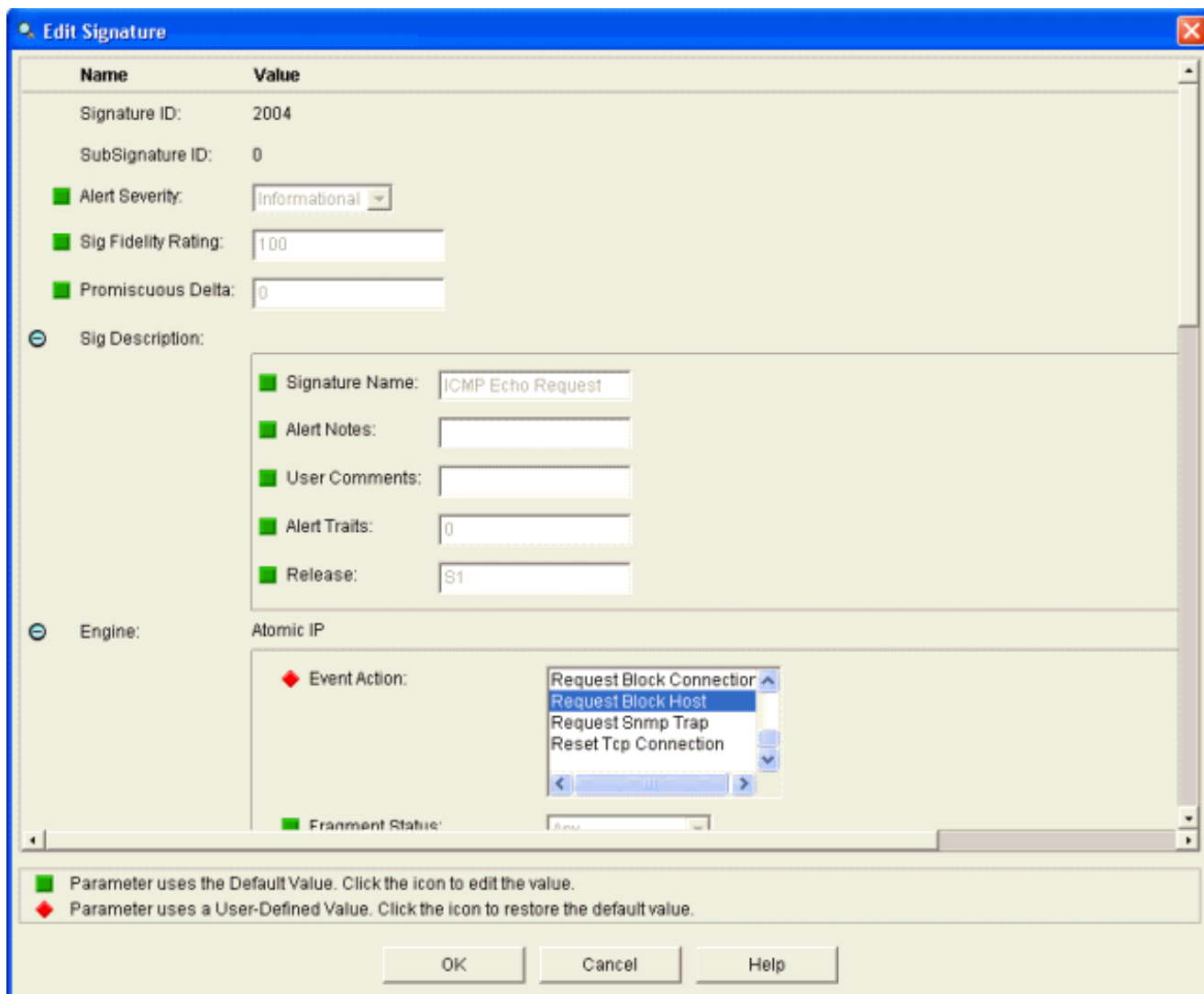
Specify ICMP Identifier: No

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.

OK Cancel Help

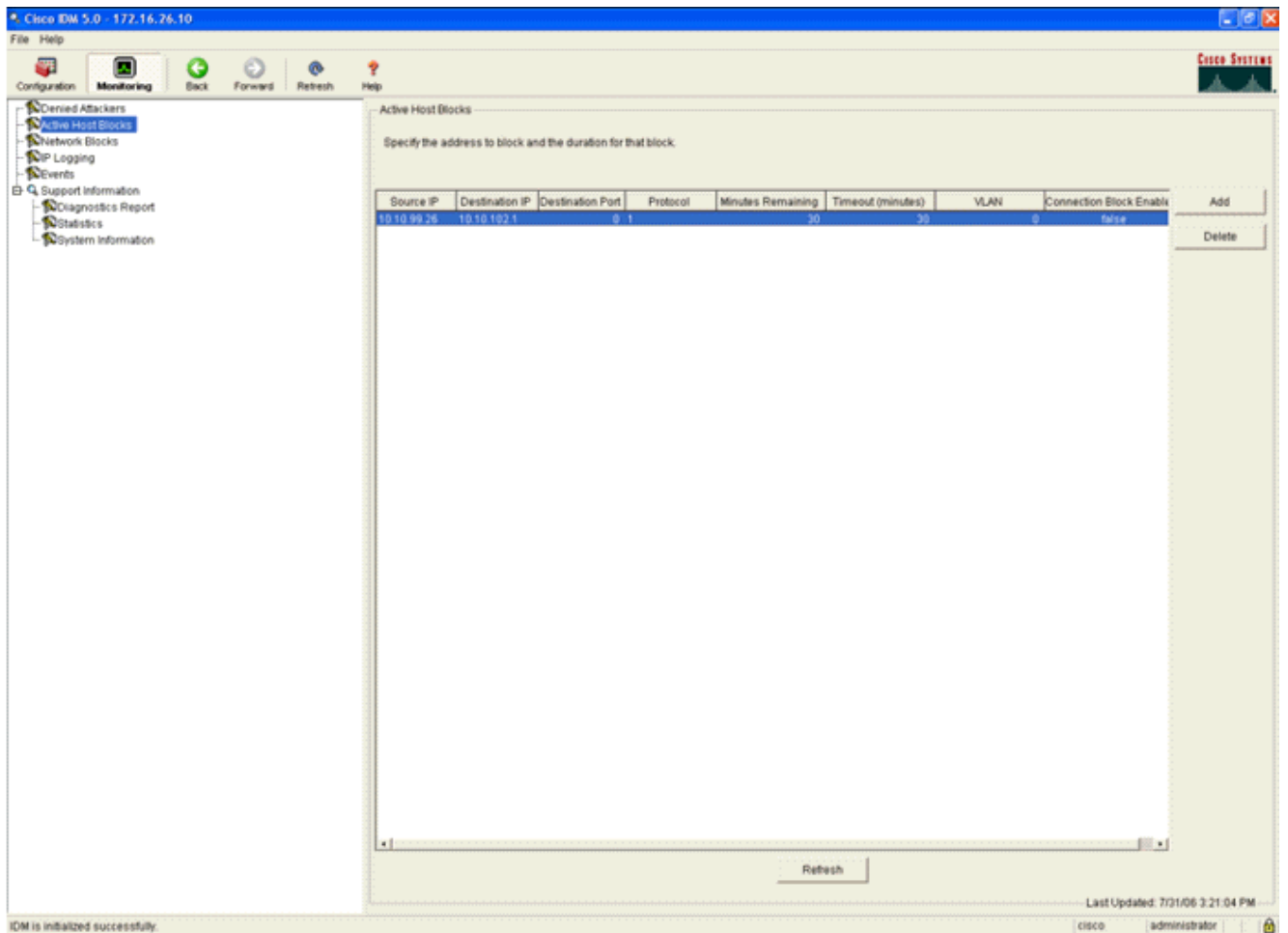


3. 单击OK以保存签名。
4. 验证签名是否处于活动状态且已设置为执行阻止操作。
5. 单击Apply将签名提交到模块。

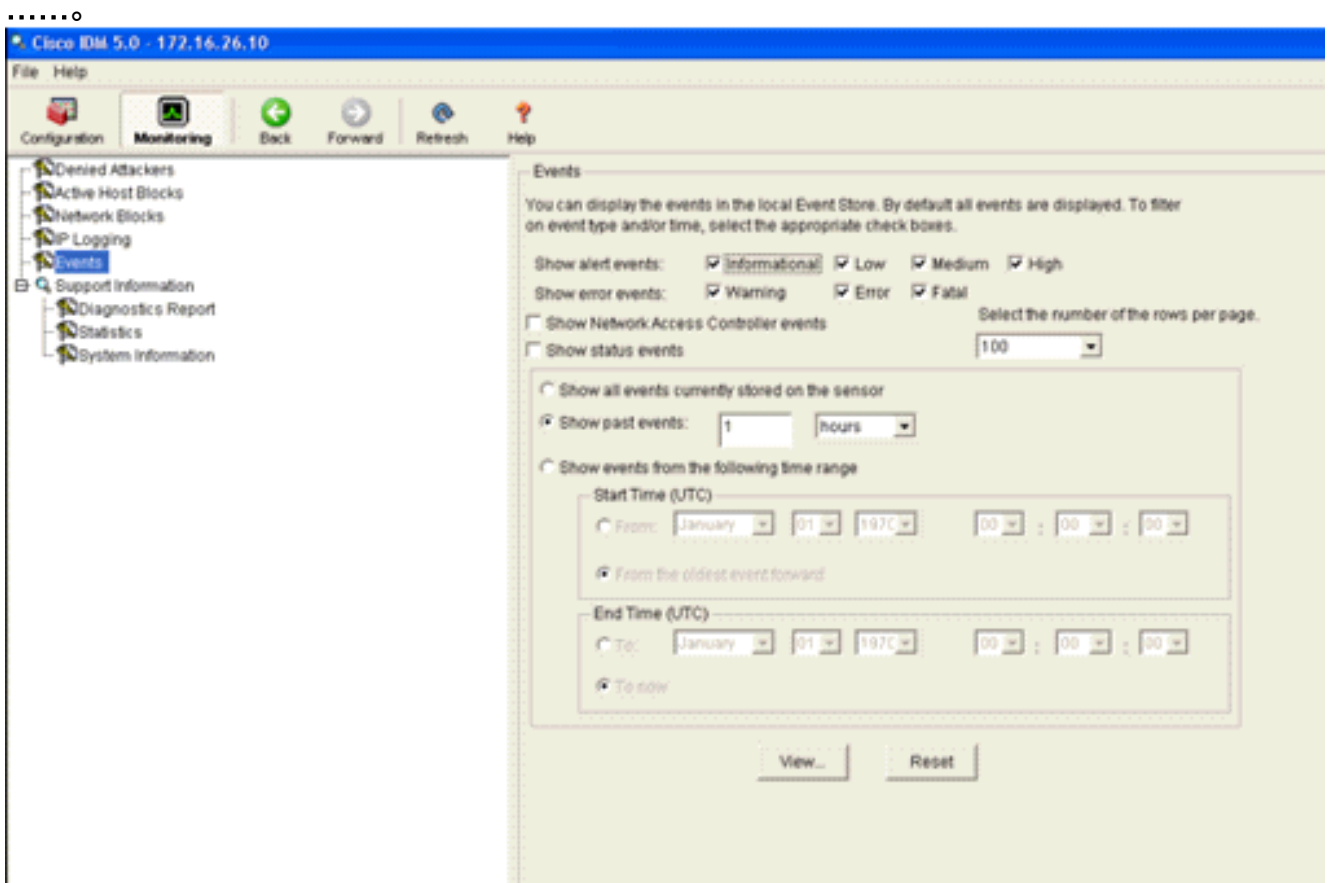
## 使用IDM监控阻止和事件

请完成以下步骤：

1. 当签名成功触发时，IDM中有两个位置可以注意这一点。第一种方法显示AIP-SSM已安装的活动块。单击顶行**Monitoring**。在左侧显示的项目列表中，选择“活动主机块”。每当触发ping签名时，Active Host Blocks窗口都会显示违规者的IP地址、受攻击设备的地址以及阻止生效的剩余时间。默认阻塞时间为30分钟，可调。但是，本文档不讨论更改此值。有关如何更改此参数的信息，请根据需要查阅ASA配置文档。立即删除该块，从列表中选择该块，然后单击“删除”。



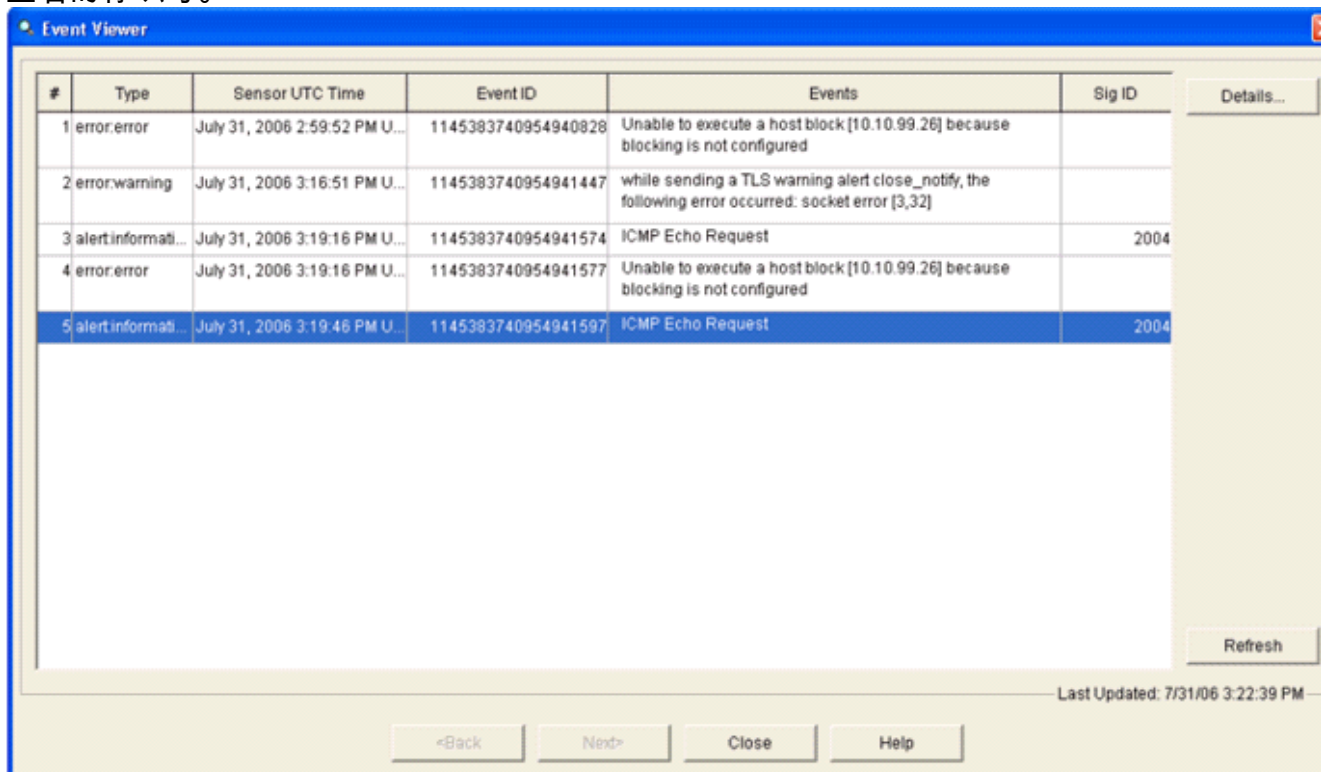
查看触发签名的第二种方法使用AIP-SSM事件缓冲区。从“IDM监控”页中，在左侧的“项目”列表中选择“事件”。系统将显示Events搜索实用程序。设置适当的搜索条件，然后单击查看



2. 然后，系统将显示事件查看器，其中包含符合给定条件的事件列表。滚动列表，查找在前面的配置步骤中修改的ICMP回应请求签名。在“事件”列中查找签名的名称，或在“签名ID”列下搜索

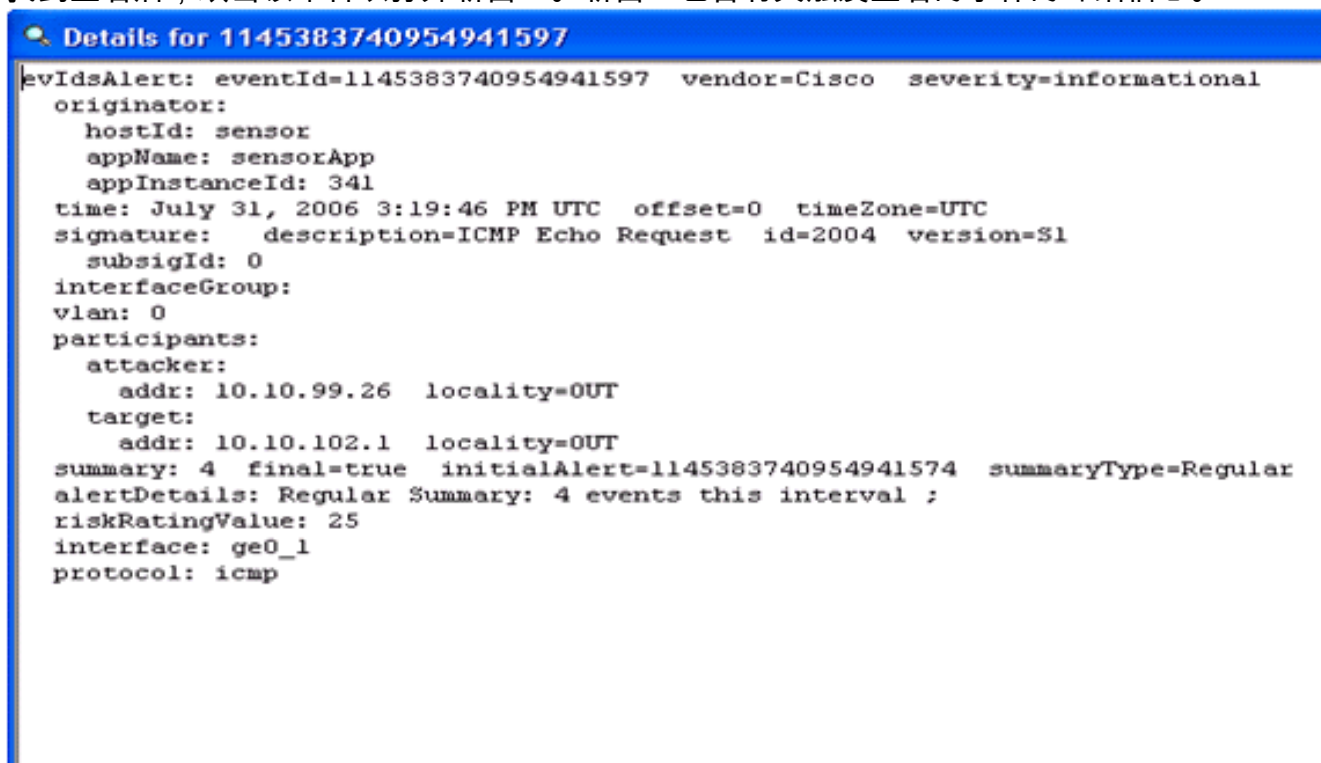


签名的标识号。



#	Type	Sensor UTC Time	Event ID	Events	Sig ID	Details...
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	

3. 找到签名后，双击该条目以打开新窗口。新窗口包含有关触发签名的事件的详细信息。



```
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
```

## 无线控制器中的监控客户端排除

此时，控制器中的Sived Clients列表会填充主机的IP和MAC地址。

The screenshot shows the Cisco Systems Security page. The left sidebar contains a navigation menu with categories: AAA, Access Control Lists, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, and Web Login Page. The main content area is titled "CIDS Shun List" and features a "Re-sync" button. Below the button is a table with the following data:

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

用户将添加到客户端排除列表。

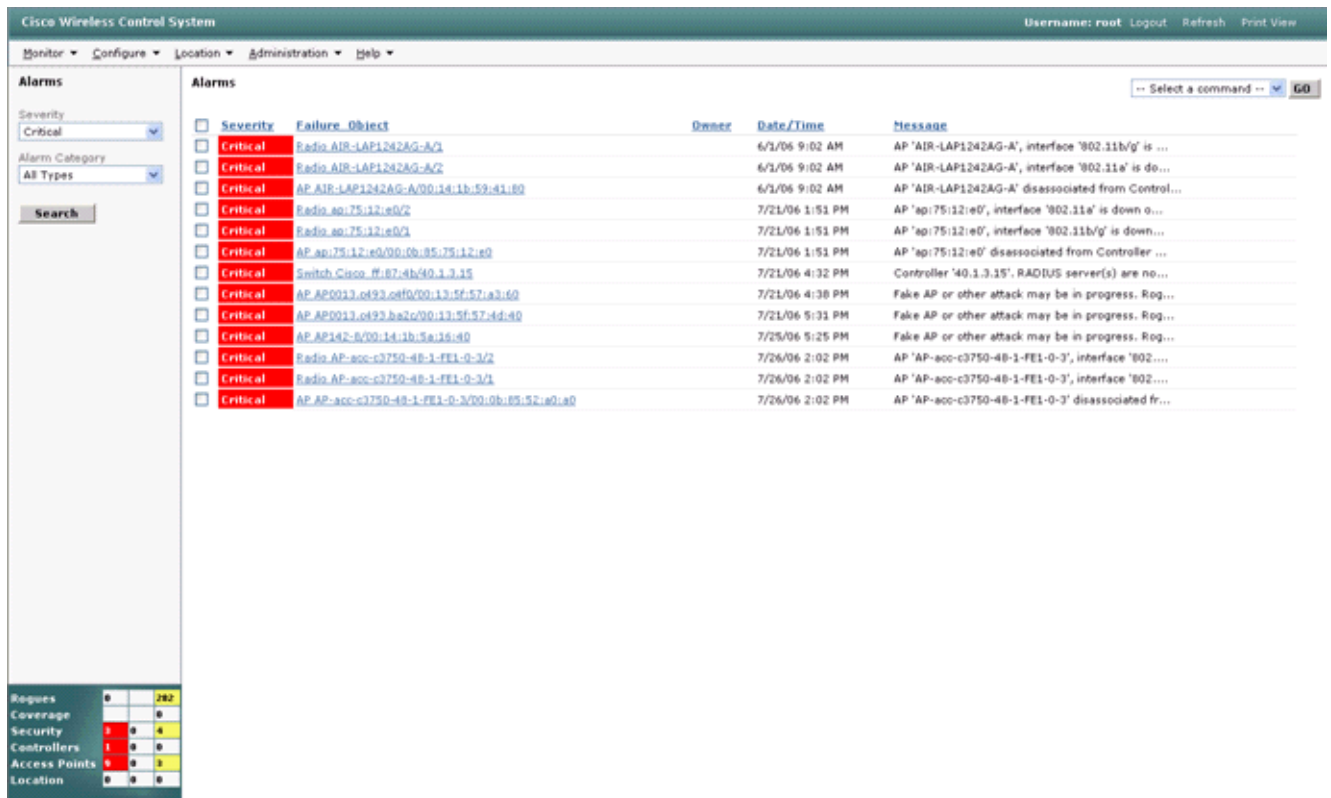
The screenshot shows the Cisco Systems Monitor page. The left sidebar contains a navigation menu with categories: Summary, Statistics, and Wireless. The main content area is titled "Excluded Clients" and features a search bar labeled "Search by MAC address" with a "Search" button. Below the search bar is a table with the following data:

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	<a href="#">Detail</a> <a href="#">Link</a> <a href="#">Test</a> <a href="#">Disable</a> <a href="#">Remove</a>

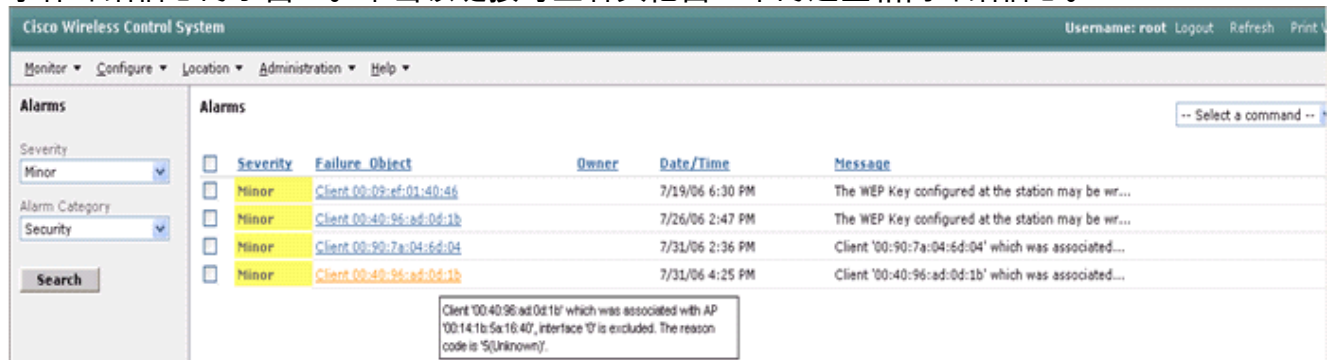
## 监控WCS中的事件

触发AIP-SSM内块的安全事件导致控制器将违规者的地址添加到客户端排除列表。WCS中也会生成事件。

1. 使用WCS主菜单中的Monitor > Alarms实用程序查看排除事件。WCS最初显示所有未清除的警报，还在窗口左侧显示搜索功能。
2. 修改搜索条件以查找客户端块。在“严重性”下，选择次要，并将“警报类别”设置为“安全”。
3. 单击搜索。



4. 然后，“警报”窗口仅列出严重性次要的安全警报。将鼠标指向触发AIP-SSM内块的事件。特别是，WCS显示导致警报的客户端站的MAC地址。通过指向适当的地址，WCS会弹出一个包含事件详细信息的小窗口。单击该链接可查看其他窗口中的这些相同详细信息。



## Cisco ASA配置示例

```

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#
```

## 思科入侵防御系统传感器示例配置

```
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#

## [验证](#)

当前没有可用于此配置的验证过程。

## [故障排除](#)

目前没有针对此配置的故障排除信息。

## [相关信息](#)

- [安装和使用思科入侵防御系统设备管理器5.1](#)
- [Cisco ASA 5500系列自适应安全设备 — 配置指南](#)
- [使用命令行界面5.0配置Cisco入侵防御系统传感器 — 配置接口](#)
- [WLC配置指南4.0](#)
- [无线技术支持](#)
- [无线局域网控制器\(WLC\)常见问题](#)
- [无线 LAN 控制器和轻量接入点基本配置示例](#)
- [配置安全解决方案](#)
- [技术支持和文档 - Cisco Systems](#)