Initializing the Sensor

This chapter describes how to use the **setup** command to initialize the sensor, and contains the following sections:

Initializing Notes and Caveats

The following notes and caveats apply to initializing the sensor:

- You must be administrator to use the **setup** command.
- You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.
- The currently supported Cisco IPS appliances are the IPS 4240, IPS 4255, and IPS 4260 [IPS 7.1(5) and later], IPS 4270-20 [IPS 7.1(3) and later], IPS 4345 and IPS 4360 [IPS 7.1(3) and later], and IPS 4510 and IPS 4520 [IPS 7.1(4) and later].
- You do not need to configure interfaces on the ASA IPS modules (ASA 5500 AIP SSM, ASA 5500-X IPS SSP, and ASA 5585-X IPS SSP). You should ignore the modify interface default VLAN setting in setup. The separation of traffic across virtual sensors is configured differently for the ASA IPS modules than for other sensors.

Understanding Initialization

After you install the sensor on your network, you must use the **setup** command to initialize it so that you can communicate with it over the network. You cannot use the IDM or the IME to configure the sensor until you initialize the sensor using the **setup** command.

With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, global correlation servers, and time settings. You can continue using advanced setup in the CLI to enable Telnet, configure the web server, and assign and enable virtual sensors and interfaces, or you can use the Startup Wizard in the IDM or the IME. After you configure the sensor with the **setup** command, you can change the network settings in the IDM or the IME.

Note You must be administrator to use the **setup** command.

Participating in the SensorBase Network

The Cisco IPS contains a security capability, Cisco Global Correlation, which uses the immense security intelligence that we have amassed over the years. At regular intervals, the Cisco IPS receives threat updates from the Cisco SensorBase Network, which contain detailed information about known threats on the Internet, including serial attackers, Botnet harvesters, Malware outbreaks, and dark nets. The IPS uses this information to filter out the worst attackers before they have a chance to attack critical assets. It then incorporates the global threat data in to its system to detect and prevent malicious activity even earlier.

If you agree to participate in the SensorBase Network, Cisco will collect aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent by secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco will be anonymous and treated as strictly confidential.

Table 3-1 shows how we use the data.

Table 3-1 Cisco Network Participation Data Use

Participation Level	Type of Data	Purpose
Partial	Protocol attributes (TCP maximum segment size and options string, for example)	Tracks potential threats and helps us to understand threat exposure.
	Attack type (signature fired and risk rating, for example)	Used to understand current attacks and attack severity.
	Connecting IP address and port	Identifies attack source.
	Summary IPS performance (CPU utilization, memory usage, inline vs. promiscuous, for example)	Tracks product efficacy.
Full	Victim IP address and port	Detects threat behavioral patterns.

When you enable Partial or Full Network Participation, the Network Participation Disclaimer appears. You must click **Agree** to participate. If you do not have a license installed, you receive a warning telling you that global correlation inspection and reputation filtering are disabled until the sensor is licensed. You can obtain a license at http://www.cisco.com/go/license.

For More Information

- For more information about global correlation, see Chapter 10, "Configuring Global Correlation."
- For the procedure for obtaining a sensor license, see Installing the License Key, page 4-56.

Simplified Setup Mode

The sensor automatically calls the **setup** command when you connect to the sensor using a console cable and the sensor basic network settings have not yet been configured. The sensor does not call automatic setup under the following conditions:

- When initialization has already been successfully completed.
- If you have recovered or downgraded the sensor.
- If you have set the host configuration to default after successfully configuring the sensor using automatic setup.

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the default values last set.

System Configuration Dialog

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the current values.

You must go through the entire System Configuration Dialog until you come to the option that you want to change. To accept default settings for items that you do not want to change, press **Enter**.

To return to the EXEC prompt without making changes and without going through the entire System Configuration Dialog, press **Ctrl-C**. The System Configuration Dialog also provides help text for each prompt. To access the help text, enter `?` at a prompt.

When you complete your changes, the System Configuration Dialog shows you the configuration that you created during the setup session. It also asks you if you want to use this configuration. If you enter `yes`, the configuration is saved. If you enter `no`, the configuration is not saved and the process begins again. There is no default for this prompt; you must enter either `yes` or `no`.

You can configure daylight savings time either in recurring mode or date mode. If you choose recurring mode, the start and end days are based on week, day, month, and time. If you choose date mode, the start and end days are based on month, day, year, and time. Choosing disable turns off daylight savings time.

Note You only need to set the date and time in the System Configuration Dialog if the system is an appliance and is NOT using NTP.

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

Example 3-1 shows a sample System Configuration Dialog.

Example 3-1 Example System Configuration Dialog

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.



Current time: Wed Nov 11 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.168.1.2/24,192.168.1.1]:
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Global Correlation?[no]:
  DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Global Correlation?[no]:
  HTTP proxy server IP address[128.107.241.169]:
  HTTP proxy server Port number[8080]:
Modify system clock settings?[no]: yes
  Modify summer time settings?[no]:yes
    Use USA SummerTime Defaults?[yes]:no
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
```

```
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances.  We do not collect the data content of
traffic or other sensitive business or personal information.  All data is aggregated and
sent via secure HTTP to the Cisco SensorBase Network servers in periodic intervals.  All
data shared with Cisco will be anonymous and treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
  * Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs. promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
  * Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

Basic Sensor Setup

You can perform basic sensor setup using the **setup** command, and then finish setting up the sensor using the CLI, IDM, or IME. To perform basic sensor setup using the **setup** command, follow these steps:

Step 1 Log in to the sensor using an account with administrator privileges.

Note Both the default username and password are **cisco**.

Step 2 The first time you log in to the sensor you are prompted to change the default password. Passwords must be at least eight characters long and be strong, that is, not be a dictionary word. After you change the password, basic setup begins.

Step 3 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 4 Specify the hostname. The hostname is a case-sensitive character string up to 64 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

Step 5 Specify the IP interface. The IP interface is in the form of IP Address/Netmask,Gateway: *X.X.X.X/nn*,*Y.Y.Y.Y*, where *X.X.X.X* specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods, *nn* specifies the number of bits in the netmask, and *Y.Y.Y.Y* specifies the default gateway as a 32-bit address written as 4 octets separated by periods.

Step 6 Enter **yes** to modify the network access list:

a. If you want to delete an entry, enter the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.

b. Enter the IP address and netmask of the network you want to add to the access list.

Note For example, 10.0.0.0/8 permits all IP addresses on the 10.0.0.0 network (10.0.0.0-10.255.255.255) and 10.1.1.0/24 permits only the IP addresses on the 10.1.1.0 subnet (10.1.1.0-10.1.1.255). If you want to permit access to a single IP address than the entire network, use a 32-bit netmask. For example, 10.1.1.1/32 permits just the 10.1.1.1 address.

c. Repeat Step b until you have added all networks that you want to add to the access list, and then press **Enter** at a blank permit line to go to the next step.

Step 7 You must configure a DNS server or an HTTP proxy server for global correlation to operate:

a. Enter **yes** to add a DNS server, and then enter the DNS server IP address.

b. Enter **yes** to add an HTTP proxy server, and then enter the HTTP proxy server IP address and port number.

Caution You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

Step 8 Enter **yes** to modify the system clock settings:

a. Enter **yes** to modify summertime settings.

Note Summertime is also known as DST. If your location does not use Summertime, go to Step m.

b. Enter **yes** to choose the USA summertime defaults, or enter **no** and choose recurring, date, or disable to specify how you want to configure summertime settings. The default is recurring.

c. If you chose recurring, specify the month you want to start summertime settings. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is march.

d. Specify the week you want to start summertime settings. Valid entries are first, second, third, fourth, fifth, and last. The default is second.

e. Specify the day you want to start summertime settings. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

f. Specify the time you want to start summertime settings. The default is 02:00:00.

Note The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2:00 a.m. on the second Sunday in March, and a stop time of 2:00 a.m. on the first Sunday in November. The default summertime offset is 60 minutes.

g. Specify the month you want summertime settings to end. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is november.

h. Specify the week you want the summertime settings to end. Valid entries are first, second, third, fourth, fifth, and last. The default is first.

i. Specify the day you want the summertime settings to end. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

j. Specify the time you want summertime settings to end. The default is 02:00:00.

k. Specify the DST zone. The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:,_/-]+$.

l. Specify the summertime offset. Specify the summertime offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 60.

m. Enter **yes** to modify the system time zone.

n. Specify the standard time zone name. The zone name is a character string up to 24 characters long.

o. Specify the standard time zone offset. Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 0.

p. Enter **yes** if you want to use NTP. To use authenticated NTP, you need the NTP server IP address, the NTP key ID, and the NTP key value. If you do not have those at this time, you can configure NTP later. Otherwise, you can choose unauthenticated NTP.

Step 9 Enter **off**, **partial**, or **full** to participate in the SensorBase Network Participation:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network except the attacker/victim IP addresses that you exclude.

The SensorBase Network Participation disclaimer appears. It explains what is involved in participating in the SensorBase Network.

Step 10 Enter **yes** to participate in the SensorBase Network.

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24, 192.168.1.1
host-name sensor
telnet-option disabled
sshv1-fallback enabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
```

```
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option enabled
ntp-keys 1 md5-key 8675309
ntp-servers 10.10.1.2 key-id 1
exit
service global-correlation
network-participation full
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

Step 11 Enter **2** to save the configuration (or **3** to continue with advanced setup using the CLI).

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 12 If you changed the time setting, enter **yes** to reboot the sensor.

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 21-1.

Advanced Setup

This section describes how to continue with Advanced Setup in the CLI for the various Cisco IPS platforms. It contains the following sections:

Advanced Setup for the Appliance

Note The currently supported Cisco IPS appliances are the IPS 4240, IPS 4255, and IPS 4260 [IPS 7.1(5) and later], IPS 4270-20 [IPS 7.1(3) and later], IPS 4345 and IPS 4360 [IPS 7.1(3) and later], and IPS 4510 and IPS 4520 [IPS 7.1(4) and later].

Note Adding new subinterfaces is a two-step process. You first organize the interfaces when you edit the virtual sensor configuration. You then choose which interfaces and subinterfaces are assigned to which virtual sensors.

The interfaces change according to the appliance model, but the prompts are the same for all models. To continue with advanced setup for the appliance, follow these steps:

Step 1 Log in to the appliance using an account with administrator privileges.

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is enabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter **yes** to modify the interface and virtual sensor configuration and to see the current interface configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Promiscuous:
   GigabitEthernet0/0
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs1
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs2
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **1** to edit the interface configuration.

Note The following options let you create and delete interfaces. You assign the interfaces to virtual sensors in the virtual sensor configuration. If you are using promiscuous mode for your interfaces and are not subdividing them by VLAN, no additional configuration is necessary.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 9 Enter **2** to add inline VLAN pairs and display the list of available interfaces.

Caution The new VLAN pair is not automatically added to a virtual sensor.

```
Available Interfaces
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Step 10 Enter **1** to add an inline VLAN pair to GigabitEthernet 0/0, for example.

```
Inline Vlan Pairs for GigabitEthernet0/0
   None
```

Step 11 Enter a subinterface number and description.

```
Subinterface Number:
Description[Created via setup by user asmith]:
```

Step 12 Enter numbers for VLAN 1 and 2.

```
Vlan1[]: 200
Vlan2[]: 300
```

Step 13 Press **Enter** to return to the available interfaces menu.

Note Entering a carriage return at a prompt without a value returns you to the previous menu.

```
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Note At this point, you can configure another interface, for example, GigabitEthernet 0/1, for inline VLAN pair.

Step 14 Press **Enter** to return to the top-level interface editing menu.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
```

```
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 15 Enter **4** to add an inline interface pair and see these options.

```
Available Interfaces
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3
```

Step 16 Enter the pair name, description, and which interfaces you want to pair.

```
Pair name: newPair
Description[Created via setup by user asmith:
Interface1[]: GigabitEthernet0/1
Interface2[]: GigabitEthernet0/2
Pair name:
```

Step 17 Press **Enter** to return to the top-level interface editing menu.

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 18 Press **Enter** to return to the top-level editing menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 19 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 20 Enter **2** to modify the virtual sensor configuration, vs0.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/3
   [2] GigabitEthernet0/0
  Inline Vlan Pair:
   [3] GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   [4] newPair (GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 21 Enter **3** to add inline VLAN pair GigabitEthernet0/0:1.

Step 22 Enter **4** to add inline interface pair NewPair.

Step 23 Press **Enter** to return to the top-level virtual sensor menu.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
   GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   newPair (GigabitEthernet0/1, GigabitEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option: GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 24 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 25 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 26 Enter **yes** to disable automatic threat prevention on all virtual sensors.

Step 27 Press **Enter** to exit the interface and virtual sensor configuration.

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option disabled
sshv1-fallback enabled
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service interface
physical-interfaces GigabitEthernet0/0
```

```
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user asmith
vlan1 200
vlan2 300
exit
exit
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 GigabitEthernet0/1
interface2 GigabitEthernet0/2
exit
exit
service analysis-engine
virtual-sensor newVs
description Created via setup by user cisco
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/0
exit
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 1
logical-interface newPair
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 28 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 29 Reboot the appliance.

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 30 Enter **yes** to continue the reboot.

Step 31 Apply the most recent service pack and signature update. You are now ready to configure your appliance for intrusion prevention.

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 21-1.

Advanced Setup for the ASA 5500 AIP SSM

To continue with advanced setup for the ASA 5500 AIP SSM, follow these steps:

Step 1 Session in to the ASA 5500 AIP SSM using an account with administrator privileges.

```
asa# session 1
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is enabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5500 AIP SSM. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5500 AIP SSM than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 9 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 11 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

Step 12 Enter **1** to add GigabitEthernet 0/1 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign GigabitEthernet 0/1. We recommend that you assign GigabitEthernet 0/1 to vs0, but you can assign it to another virtual sensor if you want to.

Step 13 Press **Enter** to return to the main virtual sensor menu.

Step 14 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 15 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

Step 16 Enter **1** to use the existing anomaly detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 17 Enter **2** to create a signature-definition configuration file.

Step 18 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 19 Enter **1** to use the existing event-action-rules configuration, rules0.

Note If GigabitEthernet 0/1 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   GigabitEthernet0/1

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 20 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 21 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 22 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name aip-ssm
telnet-option disabled
sshv1-fallback enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
```

```
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 23 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 24 Reboot the ASA 5500 AIP SSM.

```
aip-ssm# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 25 Enter **yes** to continue the reboot.

Step 26 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
aip-ssm# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 27 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5500 AIP SSM with a web browser.

Step 28 Apply the most recent service pack and signature update. You are now ready to configure your ASA 5500 AIP SSM for intrusion prevention.

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 21-1.

Advanced Setup for the ASA 5500-X IPS SSP

To continue with advanced setup for the ASA 5500-X IPS SSP, follow these steps:

Step 1 Session in to the IPS using an account with administrator privileges.

```
asa# session ips
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is enabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel 0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5500-X IPS SSP. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5500-X IPS SSP than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 9 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 11 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel 0/0
Add Interface:
```

Step 12 Enter **1** to add PortChannel 0/0 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign PortChannel 0/0. We recommend that you assign PortChannel 0/0 to vs0, but you can assign it to another virtual sensor if you want to.

Step 13 Press **Enter** to return to the main virtual sensor menu.

Step 14 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 15 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

Step 16 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 17 Enter **2** to create a signature-definition configuration file.

Step 18 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 19 Enter **1** to use the existing event-action-rules configuration, rules0.

Note If PortChannel 0/0 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 20 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 21 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 22 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name asa-ips
telnet-option disabled
sshv1-fallback enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
```

```
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 23 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 24 Reboot the ASA 5500-X IPS SSP.

```
asa-ips# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 25 Enter **yes** to continue the reboot.

Step 26 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
asa-ips# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 27 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5500-X IPS SSP with a web browser.

Step 28 Apply the most recent service pack and signature update. You are now ready to configure the ASA 5500-X IPS SSP for intrusion prevention.

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 21-1.

Advanced Setup for the ASA 5585-X IPS SSP

To continue with advanced setup for the ASA 5585-X IPS SSP, follow these steps:

Step 1 Session in to the ASA 5585-X IPS SSP using an account with administrator privileges.

```
asa# session 1
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the SSHv1 fallback setting. The default is enabled.

Step 6 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 7 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 8 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5585-X IPS SSP. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5585-X IPS SSP than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 9 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 10 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 11 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.
```

```
 Unassigned:
  Monitored:
   [1] PortChannel0/0
Add Interface:
```

Step 12 Enter **1** to add PortChannel 0/0 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign PortChannel 0/0. We recommend that you assign PortChannel 0/0 to vs0, but you can assign it to another virtual sensor if you want to.

Step 13 Press **Enter** to return to the main virtual sensor menu.

Step 14 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 15 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

Step 16 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 17 Enter **2** to create a signature-definition configuration file.

Step 18 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 19 Enter **1** to use the existing event action rules configuration, rules0.

Note If PortChannel 0/0 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
```

```
  [4] Create new virtual sensor.
Option:
```

Step 20 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 21 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 22 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name ips-ssm
telnet-option disabled
sshv1-fallback enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
```

```
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 23 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 24 Reboot the ASA 5585-X IPS SSP.

```
ips-ssp# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 25 Enter **yes** to continue the reboot.

Step 26 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 27 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5585-X IPS SSP with a web browser.

Step 28 Apply the most recent service pack and signature update. You are now ready to configure your ASA 5585-X IPS SSP for intrusion prevention.

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 21-1.

Verifying Initialization

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS 7.1 version you have installed.

To verify that you initialized your sensor, follow these steps:

Step 1 Log in to the sensor.

Step 2 View your configuration.

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Tue Nov 01 10:40:39 2011
! ------------------------------
! Version 7.1(3)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S581.0   2011-07-11
! ------------------------------
service interface
exit
! ------------------------------
```

```
service authentication
permit-packet-logging true
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option enabled
sshv1-fallback enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -360
standard-time-zone-name GMT-06:00
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
exit
exit
signatures 2004 0
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
exit
exit
exit
! ------------------------------
service ssh-known-hosts
rsa1-keys 10.89.146.1
length 1024
exponent 35
modulus 12783094292288326767015615132168773328115097561020607196221632570955980269998149478748431202060218539250569954487820368372742332963486465122675278103455023820741470819765804773674487613727040180067491475301153544560864727358878607802092320356564916540239189319280544503100030493898641274232894037971186901542 7
exit
exit
```

```
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

Note You can also use the **more current-config** command to view your configuration.

Step 3 Display the self-signed X.509 certificate (needed by TLS).

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 4 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when connecting to this sensor with a web browser.

For More Information

For the procedure for logging in to the sensor, see Chapter 2, "Logging In to the Sensor."