

## Initializing the Sensor

---

This chapter explains how to initialize the sensor using the **setup** command. It contains the following sections:

- [Overview, page 11-1](#)
- [System Configuration Dialog, page 11-1](#)
- [Initializing the Sensor, page 11-3](#)

### Overview

After you install the sensor on your network, you must use the **setup** command to initialize it. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, Telnet server, web server port, access control lists, and time settings, and you assign and enable virtual sensors and interfaces. After you initialize the sensor, you can communicate with it over the network. You are now ready to configure intrusion prevention.

### 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 11-1](#) shows a sample System Configuration Dialog.

### **Example 11-1 Example System Configuration Dialog**

```
--- 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 Configuration:
```

```
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
np 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 443
exit
service interface
physical-interfaces FastEthernet0/0
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 FastEthernet0/1
admin-state enabled
exit
physical-interfaces FastEthernet0/2
```

```
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 FastEthernet0/1
interface2 FastEthernet0/2
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 FastEthernet0/0 subinterface-number 1
logical-interface newPair
exit
exit

Current time: Wed May 5 10:25:35 2006
```

## Initializing the Sensor

This section describes how to initialize the various IPS sensors. It contains the following topics:

- [Initializing the Appliance, page 11-3](#)
- [Initializing IDSM-2, page 11-12](#)
- [Initializing AIM-IPS, page 11-19](#)
- [Initializing AIP-SSM, page 11-25](#)
- [Initializing NM-CIDS, page 11-32](#)
- [Verifying Initialization, page 11-37](#)

## Initializing the Appliance

**Note**

---

The interfaces change according to the appliance model, but the prompts are the same for all models.

---



**Note**

Setup supports multiple virtual sensors. In IPS 5.x, Setup added new subinterfaces to virtual sensor vs0. In IPS 6.0, 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.

To initialize the appliance, follow these steps:

**Step 1** Log in to the appliance using an account with administrator privileges using either a serial connection or a monitor and keyboard:



**Note**

You cannot use a monitor and keyboard with IDS-4215, IPS-4240, IPS-4255, IPS-4260, or IPS 4270-20.



**Note**

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

**Step 2** The first time you log in to the appliance 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, the `sensor#` prompt appears.

**Step 3** Enter the `setup` command.

The System Configuration Dialog is displayed.

**Step 4** Press the spacebar to get to the following question:

`Continue with configuration dialog?[yes]:`

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

**Step 5** Enter `yes` to continue.

**Step 6** 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 7** 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 8** Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

**Step 9** 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**

If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://appliance_ip_address:port` (for example, `https://10.1.9.201:1040`).



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

**Step 10** 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.

The IP network interface is in the form of IP Address/Netmask: *X.X.X.X/nn*, where *X.X.X.X* specifies the network IP address as a 32-bit address written as 4 octets separated by periods and *nn* specifies the number of bits in the netmask for that network.

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.

d. Press **Enter** at a blank permit line to proceed to the next step.

**Step 11** Enter **yes** to modify the system clock settings.

a. Enter **yes** if you want to use 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.

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



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

c. Choose recurring, date, or disable to specify how you want to configure summertime settings.

The default is recurring.

d. 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.

e. Specify the week you want to start summertime settings.

Valid entries are first, second, third, fourth, fifth, and last. The default is first.

f. Specify the day you want to start summertime settings.

Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

g. 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.

- h. 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.
- i. Specify the week you want the summertime settings to end.  
Valid entries are first, second, third, fourth, fifth, and last. The default is last.
- j. 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.
- k. Specify the time you want summertime settings to end.
- l. Specify the DST zone.  
The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+;,\_/-]+\$.
- m. 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 0.
- n. Enter **yes** to modify the system time zone.
- o. Specify the standard time zone name.  
The zone name is a character string up to 24 characters long.
- p. 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.

**Step 12** Enter **yes** to modify the interface and virtual sensor configuration.

The current interface configuration appears:

```
Current interface configuration
Command control: GigabitEthernet0/1
Unassigned:
Promiscuous:
FastEthernet0/0
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
GigabitEthernet0/0

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 13** 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.

The following options appear:

```
[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 14** Enter **2** to add inline VLAN pairs.



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

The list of available interfaces is displayed:

```
Available Interfaces
[1] FastEthernet0/0
[2] FastEthernet0/1
[3] FastEthernet0/2
[4] FastEthernet0/3
[5] GigabitEthernet0/0
```

Option:

**Step 15** Enter **1** to add an inline VLAN pair to FastEthernet0/0, for example:

```
Inline Vlan Pairs for FastEthernet0/0
None
```

**Step 16** Enter a subinterface number and description:

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

**Step 17** Enter numbers for VLAN 1 and 2:

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

**Step 18** 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] FastEthernet0/0
[2] FastEthernet0/1
[3] FastEthernet0/2
[4] FastEthernet0/3
[5] GigabitEthernet0/0
```

Option:



**Note** At this point, you can configure another interface, for example, FastEthernet0/1, for inline VLAN pair.

**Step 19** Press **Enter** to return to the top-level interface editing menu.

The following options appear:

- [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 20** Enter **4** to add an inline interface pair.

The following options appear:

```
Available Interfaces
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
GigabitEthernet0/0
```

**Step 21** Enter the pair name, description, and which interfaces you want to pair:

```
Pair name: newPair
Description[Created via setup by user asmith:
Interface1[]: FastEthernet0/1
Interface2[]: FastEthernet0/2
Pair name:
```

**Step 22** Press **Enter** to return to the top-level interface editing menu.

The following options appear:

- [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 23** Press **Enter** to return to the top-level editing menu.

The following options appear:

- [1] Edit Interface Configuration
- [2] Edit Virtual Sensor Configuration
- [3] Display configuration

Option:

**Step 24** Enter **2** to edit the virtual sensor configuration.

The following options appear:

- [1] Remove virtual sensor.
- [2] Modify "vs0" virtual sensor configuration.
- [3] Create new virtual sensor.

Option:

**Step 25** Enter **2** to modify the virtual sensor configuration, vs0.

The following options appear:

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

No Interfaces to remove.

Unassigned:
Promiscuous:
  [1] FastEthernet0/3
  [2] GigabitEthernet0/0
Inline Vlan Pair:
  [3] FastEthernet0/0:1 (Vlans: 200, 300)
Inline Interface Pair:
  [4] newPair (FastEthernet0/1, FastEthernet0/2)
Add Interface:
```

**Step 26** Enter **3** to add inline VLAN pair FastEthernet0/0:1.

**Step 27** Enter **4** to add inline interface pair NewPair.

**Step 28** Press **Enter** to return to the top-level virtual sensor menu.

The following options appear:

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
  FastEthernet0/0:1 (Vlans: 200, 300)
  Inline Interface Pair:
  newPair (FastEthernet0/1, FastEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option: FastEthernet0/1, FastEthernet0/2)
Add Interface:
```

**Step 29** Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

The following options appear:

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

**Step 30** 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.

The following appears:

```
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 31** Enter **yes** to disable automatic threat prevention on all virtual sensors.

**Step 32** Press **Enter** to exit the interface and virtual sensor configuration.

The following completed configuration appears:

```
The following configuration was entered.
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
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 FastEthernet0/0
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 FastEthernet0/1
admin-state enabled
exit
physical-interfaces FastEthernet0/2
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 FastEthernet0/1
interface2 FastEthernet0/2
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 FastEthernet0/0 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 33** Enter **2** to save the configuration.

```

Enter your selection[2]: 2
Configuration Saved.

```

**Step 34** Enter **yes** to modify the system date and time.




---

**Note** This option is not available when NTP has been configured. The appliances get their time from the configured NTP server.

---

- a. Enter the local date (yyyy-mm-dd).
- b. Enter the local time (hh:mm:ss).

**Step 35** Reboot the appliance:

```

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

```

**Step 36** Enter **yes** to continue the reboot.

**Step 37** 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 38** Write down the certificate fingerprints.

You need the fingerprints to check the authenticity of the certificate when connecting to this appliance with a web browser.

**Step 39** Apply the most recent service pack and signature update.

The Readme explains how to apply the most recent software update.

You are now ready to configure your appliance for intrusion prevention.

---

**For More Information**

- For more information on the System Configuration Dialog, see [System Configuration Dialog](#), page 11-1.
- For the procedure for configuring NTP, refer to [Configuring the Sensor to Use an NTP Time Source](#).
- For information on how to obtain the most recent software, see [Obtaining Cisco IPS Software](#), page 13-1.
- For the procedure for using HTTPS to log in to IDM, refer to [Logging In to IDM](#).
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - [Installing and Using Cisco Intrusion Prevention System Device Manager 6.0](#)
  - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0](#)

## Initializing IDSM-2

To initialize IDSM-2, follow these steps:

---

**Step 1** Session in to IDSM-2 using an account with administrator privileges:

- For Catalyst software:
 

```
console> enable
console> (enable) session module_number
```
- For Cisco IOS software:
 

```
router# session slot slot_number processor 1
```




---

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

---

**Step 2** The first time you log in to IDSM-2 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, the `sensor#` prompt appears.

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

**Step 4** Press the spacebar to get to the following question:  
`Continue with configuration dialog?[yes]:`

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

**Step 5** Enter `yes` to continue.

**Step 6** 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 7** 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 IDSM-2 IP address as a 32-bit address written as 4 octets separated by periods where  $X = 0-255$ ,  $nn$  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 where  $Y = 0-255$ .

**Step 8** Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

**Step 9** 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** If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://idsm2_ip_address:port` (for example, `https://10.1.1.9.201:1040`).



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

**Step 10** 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.
 

The IP network interface is in the form of IP Address/Netmask:  $X.X.X.X/nn$ , where  $X.X.X.X$  specifies the network IP address as a 32-bit address written as 4 octets separated by periods where  $X = 0-255$ ,  $nn$  specifies the number of bits in the netmask for that network.

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.
- d. Press **Enter** at a blank permit line to proceed to the next step.

**Step 11** Enter **yes** to modify the system clock settings.

- a. Enter **yes** if you want to use 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.

- b. Enter **yes** to modify summertime settings.



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

- c. Choose recurring, date, or disable to specify how you want to configure summertime settings.
 

The default is recurring.

- d. 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.
- e. Specify the week you want to start summertime settings.  
Valid entries are first, second, third, fourth, fifth, and last. The default is first.
- f. Specify the day you want to start summertime settings.  
Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.
- g. 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.

---

- h. 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.
- i. Specify the week you want the summertime settings to end.  
Valid entries are first, second, third, fourth, fifth, and last. The default is last.
- j. 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.
- k. Specify the time you want summertime settings to end.
- l. Specify the DST zone.  
The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:;\_/-]+\$.
- m. 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 0.
- n. Enter **yes** to modify the system time zone.
- o. Specify the standard time zone name.  
The zone name is a character string up to 24 characters long.
- p. 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.

**Step 12** Enter **yes** to modify the interface and virtual sensor configuration.

The current interface configuration appears:

```
Current interface configuration
Command control: GigabitEthernet0/2
Unassigned:
Promiscuous:
```

```
GigabitEthernet0/7
GigabitEthernet0/8

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 13** 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.



**Note** The IDSM-2 does not support the Add/Modify Inline Interface Pair Vlan Groups option. When running an inline interface pair the two IDSM-2 data ports are configured as access ports or a trunk port carrying only the native VLAN. The packets do not have 802.1q headers and cannot be separated by VLAN. To monitor multiple VLANs inline, use Inline VLAN Pairs.

The following options appear:

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

**Step 14** Enter **3** to add promiscuous VLAN groups.

The list of available interfaces is displayed:

```
Available Interfaces
[1] GigabitEthernet0/7
[2] GigabitEthernet0/8
Option:
```

**Step 15** Enter **2** to add VLAN groups to GigabitEthernet0/8.

```
Promiscuous Vlan Groups for GigabitEthernet0/8
None
Subinterface Number:
```

**a.** Enter **10** to add subinterface 10.

```
Subinterface Number: 10
Description[Created via setup by user asmith]:
Select vlans:
[1] All unassigned vlans.
[2] Enter vlans range.
Option:
```

**b.** Enter **1** to assign all unassigned VLANs to subinterface 10.

```
Subinterface Number:
```

- c. Enter **9** to add subinterface 9.

```
Subinterface Number: 9
Description[Created via setup by user asmith]:
Vlans[]:
```

- d. Enter **1-100** to assign VLANs 1-100 to subinterface 9.




---

**Note** This removes VLANs 1-100 from the unassigned VLANs contained in subinterface 10.

---

- e. Repeat Steps c and d until you have added all VLAN groups.

- f. Press **Enter** at a blank subinterface line to return to list of interfaces available for VLAN groups.

The following options appear:

```
[1] GigabitEthernet0/7
[2] GigabitEthernet0/8
Option:
```

- Step 16** Press **Enter** to return to the top-level interface configuration menu.

The following options appear:

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

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

The following options appear:

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

- Step 18** Enter **2** to edit the virtual sensor configuration.

The following option appears:

```
[1] Modify "vs0" virtual sensor configuration.
Option:
```

- Step 19** Enter **1** to modify the virtual sensor vs0 configuration.

The following options appear:

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

Anomaly Detection Configuration
[1] ad0
[2] Create a new anomaly detection configuration
Option[1]:
```

- Step 20** Enter **1** to use the existing anomaly-detection configuration, ad0.

The following options appear:

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

**Step 21** Enter **1** to use the existing event-action-rules configuration. rules0.

The following options appear:

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
```

No Interfaces to remove.

```
Unassigned:
  Promiscuous:
    [1] GigabitEthernet0/7
  Promiscuous Vlan Groups:
    [2] GigabitEthernet0/8:10 (Vlans: unassigned)
    [3] GigabitEthernet0/8:9 (Vlans: 1-100)
Add Interface:
```

**Step 22** Enter **2** to add VLAN group GigabitEthernet0/8:9 to the virtual sensor vs0.

Your configuration appears with the following options:

```
[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** Press **Enter** to return to the top-level virtual sensor configuration menu.

The following options appear:

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Promiscuous Vlan Groups:
    GigabitEthernet0/8:10 (Vlans: unassigned)
    GigabitEthernet0/8:9 (Vlans: 1-100)

  [1] Modify "vs0" virtual sensor configuration.
Option:
```

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

The following options appear:

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

**Step 25** Press **Enter** to exit the interface and virtual sensor configuration menu.

**Step 26** 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.

The following appears:

```
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 27** Enter **yes** to disable automatic threat prevention on all virtual sensors.

The following completed configuration appears:

```
The following configuration was entered.
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name idsm-2
telnet-option disabled
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 GigabitEthernet0/8
admin-state enabled
subinterface-type vlan-group
subinterface 9
description Created via setup by user asmith
vlans range 1-100
exit
subinterface 10
description Created via setup by user asmith
vlans unassigned
exit
exit
exit
exit
service analysis-engine
virtual-sensor vs0
description Created via setup by user cisco
signature-definition sig0
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/8 subinterface-number 9
physical-interface GigabitEthernet0/8 subinterface-number 10
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
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 IDSM-2:

```
idsm-2# 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** Display the self-signed X.509 certificate (needed by TLS):

```
idsm-2# 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 32** Write down the certificate fingerprints.

You need the fingerprints to check the authenticity of the certificate when connecting to this IDSM-2 with a web browser.

**Step 33** Apply the most recent service pack and signature update.

The Readme explains how to apply the most recent software update.

You are now ready to configure your IDSM-2 for intrusion prevention.

#### For More Information

- For more information on the System Configuration Dialog, see [System Configuration Dialog, page 11-1](#).
- For the procedure for configuring NTP, refer to [Configuring the Sensor to Use an NTP Time Source](#).
- For information on how to obtain the most recent software, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for using HTTPS to log in to IDM, refer to [Logging In to IDM](#).
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - [Installing and Using Cisco Intrusion Prevention System Device Manager 6.0](#)
  - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0](#)

## Initializing AIM-IPS

To initialize AIM-IPS, follow these steps:

**Step 1** Session in to AIM-IPS using an account with administrator privileges:

```
router# service-module ids-sensor 0/0 session
Trying 10.1.9.1, 2322 ... Open
```

```
sensor login: cisco
Password:
```




---

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

---

**Step 2** The first time you log in to AIM-IPS 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, the `sensor#` prompt appears.

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

**Step 4** Press the spacebar to get to the following question:

```
Continue with configuration dialog?[yes]:
```

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

**Step 5** Enter `yes` to continue.

**Step 6** 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 7** Specify the IP interface.

The IP interface is in the form of IP Address/Netmask, Gateway: `X.X.X.X/mn, Y.Y.Y.Y`, where `X.X.X.X` specifies the AIM-IPS IP address as a 32-bit address written as 4 octets separated by periods where `X = 0-255`, `mn` 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 where `Y = 0-255`.




---

**Note** The `Y.Y.Y.Y` gateway address is either the IP address from the IDS-Sensor interface of the router, or if you configured the IDS-Sensor interface of the router using the `ip unnumbered` command, then it is the IP address of the other interface of the router that is being shared with the IDS-Sensor interface.

---

**Step 8** Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

**Step 9** 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** If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://aip-ssm_ip_address:port` (for example, `https://10.1.9.201:1040`).

---




---

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

---

**Step 10** 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.  
 The IP network interface is in the form of IP Address/Netmask: *X.X.X.X/nm*, where *X.X.X.X* specifies the network IP address as a 32-bit address written as 4 octets separated by periods where *X* = 0-255, *nm* specifies the number of bits in the netmask for that network.  
 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.
- d. Press Enter at a blank permit line to proceed to the next step.

**Step 11** Enter **yes** to modify the system clock settings.

- a. Enter **yes** if you want to use 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.
- b. Enter **yes** to modify summertime settings.




---

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

---

- c. Choose recurring, date, or disable to specify how you want to configure summertime settings.  
 The default is recurring.
- d. 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.
- e. Specify the week you want to start summertime settings.  
 Valid entries are first, second, third, fourth, fifth, and last. The default is first.
- f. Specify the day you want to start summertime settings.  
 Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.
- g. 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 a.m. on the second Sunday in March, and a stop time of 2 a.m. on the first Sunday in November. The default summertime offset is 60 minutes.

---

- h. 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.

- i. Specify the week you want the summertime settings to end.  
Valid entries are first, second, third, fourth, fifth, and last. The default is last.
- j. 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.
- k. Specify the time you want summertime settings to end.
- l. Specify the DST zone.  
The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+;,\_/-]+\$.
- m. 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 0.
- n. Enter **yes** to modify the system time zone.
- o. Specify the standard time zone name.  
The zone name is a character string up to 24 characters long.
- p. 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.

**Step 12** Enter **yes** to modify the interface and virtual sensor configuration.

You may receive a warning that Analysis Engine is initializing and you cannot modify the virtual sensor configuration at this time. Press the space bar to receive the following menu:

```
[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.
```

Enter your selection[2]:

If you receive the warning that Analysis Engine is initializing, enter **2** to save your configuration thus far and exit setup. You can then reenter setup and press **Enter** until you are back to the interface and virtual sensor menu.

**Step 13** Enter **2** to modify the virtual sensor configuration.

```
Modify interface/virtual sensor configuration?[no]: yes
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 14** Enter **2** to edit the virtual sensor vs0 configuration.

The following appears:

```
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 15** Enter **1** to add GigabitEthernet0/1 to virtual sensor vs0.

```
Add Interface: 1
```

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
    GigabitEthernet0/1

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

**Step 16** Press **Enter** to exit the interface and virtual sensor configuration menu.

The following option appears:

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

**Step 17** 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.

The following appears:

```
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 18** Enter **yes** to disable automatic threat prevention on all virtual sensors.

The following completed configuration appears:

The following configuration was entered.

```
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name aimips
telnet-option disabled
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 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface 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 19** Enter **2** to save the configuration.

```

Enter your selection[2]: 2
Configuration Saved.

```

**Step 20** Reboot AIM-IPS.

```

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

```

**Step 21** Enter **yes** to continue the reboot.

**Step 22** Log in to AIM-IPS, and display the self-signed X.509 certificate (needed by TLS):

```

aim-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 23** Write down the certificate fingerprints.

You need the fingerprints to check the authenticity of the certificate when connecting to this AIM-IPS with a web browser.

**Step 24** Apply the most recent service pack and signature update.

The Readme explains how to apply the most recent software update.

You are now ready to configure your AIM-IPS for intrusion prevention.

#### For More Information

- For more information on the System Configuration Dialog, see [System Configuration Dialog](#), page 11-1.
- For the procedure for configuring NTP, refer to [Configuring the Sensor to Use an NTP Time Source](#).

- For the procedure for configuring an unnumbered IP address interface, refer to [Using an Unnumbered IP Address Interface](#).
- For information on how to obtain the most recent software, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for using HTTPS to log in to IDM, refer to [Logging In to IDM](#).
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - [Installing and Using Cisco Intrusion Prevention System Device Manager 6.0](#)
  - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0](#)

## Initializing AIP-SSM

To initialize AIP-SSM, follow these steps:

**Step 1** Session in to AIP-SSM using an account with administrator privileges:

```
asa# session 1
```



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

**Step 2** The first time you log in to AIP-SSM 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, the `sensor#` prompt appears.

**Step 3** Enter the `setup` command.

The System Configuration Dialog is displayed.

**Step 4** Press the spacebar to get to the following question:

```
Continue with configuration dialog?[yes]:
```

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

**Step 5** Enter **yes** to continue.

**Step 6** 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 7** 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 IDSM-2 IP address as a 32-bit address written as 4 octets separated by periods where `X = 0-255`, `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 where `Y = 0-255`.

**Step 8** Specify the Telnet server status.

You can disable or enable Telnet services. The default is disabled.

**Step 9** 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** If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://aip-ssm_ip_address:port` (for example, `https://10.1.9.201:1040`).



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

**Step 10** 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.

The IP network interface is in the form of IP Address/Netmask: *X.X.X.X/nn*, where *X.X.X.X* specifies the network IP address as a 32-bit address written as 4 octets separated by periods where *X* = 0-255, *nn* specifies the number of bits in the netmask for that network.

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.
- d. Press Enter at a blank permit line to proceed to the next step.

**Step 11** Enter **yes** to modify the system clock settings.

- a. Enter **yes** if you want to use 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.

- b. Enter **yes** to modify summertime settings.



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

- c. Choose recurring, date, or disable to specify how you want to configure summertime settings.

The default is recurring.

- d. 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.

- e. Specify the week you want to start summertime settings.

Valid entries are first, second, third, fourth, fifth, and last. The default is first.

- f. Specify the day you want to start summertime settings.

Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

- g. 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.

- h. 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.

- i. Specify the week you want the summertime settings to end.

Valid entries are first, second, third, fourth, fifth, and last. The default is last.

- j. 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.

- k. Specify the time you want summertime settings to end.

- l. Specify the DST zone.

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

- m. 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 0.

- n. Enter **yes** to modify the system time zone.

- o. Specify the standard time zone name.

The zone name is a character string up to 24 characters long.

- p. 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.

- Step 12** Enter **yes** to modify the interface and virtual sensor configuration.

The current interface configuration appears:

```
Current interface configuration
Command control: GigabitEthernet0/0
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 13** Enter **1** to edit the interface configuration.



**Note** You do not need to configure interfaces on AIP-SSM. You should ignore the Modify interface default-vlan setting. The separation of traffic across virtual sensors is configured differently for AIP-SSM than for other sensors.

The following option appears:

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

**Step 14** Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

The following options appear:

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

**Step 15** 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 16** Enter **2** to modify the virtual sensor vs0 configuration.

The following appears:

```
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 17** Enter **1** to add GigabitEthernet0/1 to virtual sensor vs0.



**Note** With ASA 7.2 and earlier, one virtual sensor is supported. The virtual sensor to which GigabitEthernet0/1 is assigned is used for monitoring packets coming from the adaptive security appliance. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.



**Note** With ASA 7.2.3 and later with IPS 6.0, multiple virtual sensors are supported. The ASA 7.2.3 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 GigabitEthernet0/1. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.

**Step 18** Press **Enter** to return to the main virtual sensor menu.

**Step 19** Enter **3** to create a virtual sensor.

The following options appear:

Name[]:

**Step 20** 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 21** Enter **1** to use the existing anomaly-detection configuration, ad0.

The following options appear:

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

**Step 22** Enter **2** to create a signature-definition configuration file.

Name[]:

**Step 23** Enter the signature-definition configuration name, **newSig**.

The following options appear:

```
Event Action Rules Configuration
  [1] rules0
  [2] newRules
  [3] Create a new event action rules configuration
Option[3]:
```

**Step 24** Enter **1** to use the existing event-action-rules configuration, rules0.



**Note** If GigabitEthernet0/1 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.



**Note** With ASA 7.2 and earlier, one virtual sensor is supported. The virtual sensor to which GigabitEthernet0/1 is assigned is used for monitoring packets coming from the adaptive security appliance. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.



**Note** With ASA 7.2.3 and later with IPS 6.0, multiple virtual sensors are supported. The ASA 7.2.3 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 GigabitEthernet0/1. We recommend that you assign GigabitEthernet0/1 to vs0, but you can assign it to another virtual sensor if you want to.

The following options appear:

```
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 25** Press **Enter** to exit the interface and virtual sensor configuration menu.

The following option appears:

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

**Step 26** 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.

---

The following appears:

```
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 27** Enter **yes** to disable automatic threat prevention on all virtual sensors.

The following completed configuration appears:

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

```

Enter your selection[2]: 2
Configuration Saved.

```

**Step 29** Reboot AIP-SSM.

```

aip-ssm# 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** 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 32** Write down the certificate fingerprints.

You need the fingerprints to check the authenticity of the certificate when connecting to this AIP-SSM with a web browser.

**Step 33** Apply the most recent service pack and signature update.

The Readme explains how to apply the most recent software update.

You are now ready to configure your AIP-SSM for intrusion prevention.

### For More Information

- For more information on the System Configuration Dialog, see [System Configuration Dialog, page 11-1](#).
- For the procedure for configuring NTP, refer to [Configuring the Sensor to Use an NTP Time Source](#).
- For more information on how to configure virtual sensors, refer to [Configuring AIP-SSM](#).
- For information on how to obtain the most recent software, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for using HTTPS to log in to IDM and ASDM, refer to [Logging In to IDM](#).
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - [Installing and Using Cisco Intrusion Prevention System Device Manager 6.0](#)
  - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0](#)

# Initializing NM-CIDS



**Note** NM-CIDS does not support inline interface pairs or VLAN pairs. Nor does it support virtualization.

To initialize NM-CIDS, follow these steps:

**Step 1** Session to NM-CIDS using an account with administrator privileges:

```
router# service-module IDS-Sensor slot_number/port_number session
```



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

**Step 2** The first time you log in to NM-CIDS 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, the `sensor#` prompt appears.

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

**Step 4** Press the spacebar to get to the following question:  
Continue with configuration dialog?[yes]:

Press the spacebar to show one page at a time. Press **Enter** to show one line at a time.

**Step 5** Enter **yes** to continue.

**Step 6** 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 7** Specify the IP interface. The IP interface is in the form of IP Address/Netmask, Gateway: *X.X.X.X/nm,Y.Y.Y.Y*, where *X.X.X.X* specifies the NM-CIDS IP address as a 32-bit address written as 4 octets separated by periods where *X* = 0-255, *nm* 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 where *Y* = 0-255.

**Step 8** Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

**Step 9** 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** If you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format `https://nm-cids_ip_address:port` (for example, `https://10.1.9.201:1040`).



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

**Step 10** 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.

The IP network interface is in the form of IP Address/Netmask: *X.X.X.X/nm*, where *X.X.X.X* specifies the network IP address as a 32-bit address written as 4 octets separated by periods where *X* = 0-255, *nm* specifies the number of bits in the netmask for that network.

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.
- d. Press **Enter** at a blank permit line to proceed to the next step.

**Step 11** Enter **yes** to modify the system clock settings.

- a. Enter **yes** if you want to use 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.

- b. Enter **yes** to modify summertime settings.




---

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

---

- c. Choose recurring, date, or disable to specify how you want to configure summertime settings.

The default is recurring.

- d. 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.

- e. Specify the week you want to start summertime settings.

Valid entries are first, second, third, fourth, fifth, and last. The default is first.

- f. Specify the day you want to start summertime settings.

Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

- g. 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.

---

- h. 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.

- i. Specify the week you want the summertime settings to end.  
Valid entries are first, second, third, fourth, fifth, and last. The default is last.
- j. 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.
- k. Specify the time you want summertime settings to end.
- l. Specify the DST zone.  
The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+;,\_/-]+\$.
- m. 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 0.
- n. Enter **yes** to modify the system time zone.
- o. Specify the standard time zone name.  
The zone name is a character string up to 24 characters long.
- p. 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.

**Step 12** Enter **yes** to modify the interface and virtual sensor configuration.

The current interface configuration appears:

```
Current interface configuration
Command control: FastEthernet0/0
Unassigned:
Promiscuous:
FastEthernet0/1

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 13** 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.

---

The following option appears:

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

**Step 14** Enter **1** to modify the default VLAN setting:

```
FastEthernet0/1 default-vlan[0]: 45
[1] Modify interface default-vlan.
```

Option:

**Step 15** Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

The following options appear:

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

Option:

**Step 16** Enter **2** to edit the virtual sensor configuration.

The following option appears:

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

No Interfaces to remove.

```
Unassigned:
Monitored:
  [1] FastEthernet0/1
```

Add Interface:

**Step 17** Enter **1** to add FastEthernet0/1 to virtual sensor vs0.

**Step 18** Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

The following options appear:

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
    FastEthernet0/1

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

Option:

**Step 19** Press **Enter** to exit the interface and virtual sensor configuration menu.

**Step 20** 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.

---

The following appears:

```
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 21** Enter **yes** to disable automatic threat prevention on all virtual sensors.

The following completed configuration appears:

The following configuration was entered.

```

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name nm-cids
telnet-option disabled
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 FastEthernet0/0
default-vlan 45
exit
exit
service analysis-engine
virtual-sensor vs0
description Created via setup by user cisco
signature-definition sig0
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface FastEthernet0/1
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 22** Enter **2** to save the configuration.

```

Enter your selection[2]: 2
Configuration Saved.

```

**Step 23** Reboot NM-CIDS:

```

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

```

**Step 24** Enter **yes** to continue the reboot.

**Step 25** Display the self-signed X.509 certificate (needed by TLS):

```

nm-cids# 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 26** Write down the certificate fingerprints.

You need the fingerprints to check the authenticity of the certificate when connecting to this NM-CIDS with a web browser.

**Step 27** Apply the most recent service pack and signature update.

The Readme explains how to apply the most recent software update.

You are now ready to configure your NM-CIDS for intrusion prevention.

#### For More Information

- For more information on the System Configuration Dialog, see [System Configuration Dialog, page 11-1](#).
- For the procedure for configuring NTP, refer to [Configuring the Sensor to Use an NTP Time Source](#).
- For information on how to obtain the most recent software, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for using HTTPS to log in to IDM, refer to [Logging In to IDM](#).
- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - [Installing and Using Cisco Intrusion Prevention System Device Manager 6.0](#)
  - [Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0](#)

## Verifying Initialization

After you have run the **setup** command, you should verify that your sensor has been initialized correctly.

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 Wed Nov 16 11:23:21 2006
! -----
! Version 6.0(0.2)
! Host:
!   Realm Keys          key1.0
! Signature Definition:
!   Signature Update    S184.0   2005-11-09

! -----
service interface
exit
! -----
service analysis-engine
global-parameters
ip-logging
max-open-iplog-files 50
exit
exit
virtual-sensor vs0
description default virtual sensor

```

```

signature-definition sig0
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode learn
exit
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
overrides deny-attacker-inline
override-item-status Enabled
risk-rating-range 0-100
exit
exit
! -----
service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 150
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
password-recovery allowed
exit
! -----
service logger
exit
! -----
service network-access
general
enable-acl-logging true
master-blocking-sensors 1.1.1.1
password bar
port 443
tls true
username foo
exit
never-block-hosts 1.1.1.1
exit
user-profiles test
exit
cat6k-devices 2.2.2.2
communication ssh-3des
profile-name test
block-vlans 12
exit
exit
router-devices 1.1.1.1
communication ssh-3des
profile-name test
block-interfaces 2.2.2.2 in
exit
response-capabilities block

```

```
exit
router-devices 3.3.3.3
communication ssh-3des
profile-name test
response-capabilities block|rate-limit
exit
exit
! -----
service notification
trap-destinations 1.1.1.1
trap-community-name something1
trap-port 166
exit
enable-notifications true
enable-set-get true
exit
! -----
service signature-definition sig0
signatures 2002 0
status
enabled true
exit
exit
signatures 2200 0
engine service-generic
specify-payload-source no
exit
exit
signatures 2202 0
engine atomic-ip
specify-ip-total-length yes
ip-total-length 12
exit
exit
exit
! -----
service ssh-known-hosts
rsa1-keys 10.89.130.72
length 1024
exponent 35
modulus 123015580885566039934287351002587653918192484054259603815920527749611655
42176138623148347589841831265831897841200949075192510730433429613298427164703821
15018377013402532698957593057061259778152893255492349859332687387121067704990725
87538411757554422994558230630572671733280051457220642360910995447890862728013
exit
exit
! -----
service trusted-certificates
exit
! -----
service web-server
exit
! -----
service anomaly-detection ad0
learning-accept-mode auto
action rotate
schedule periodic-schedule
start-time 10:00:00
interval 90
exit
exit
illegal-zone
other
```

```
default-thresholds
threshold-histogram low num-source-ips 19
exit
exit
exit
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, see [Chapter 12, “Logging In to the Sensor.”](#)