CHAPTER 16

Initializing the Sensor

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

Understanding Initialization

Before configuring IDM, you must initialize the sensor.

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. With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, 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 IDM.

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

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 16-1 shows a sample System Configuration Dialog.

Example 16-1 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: Thu Mar  6 21:19:51 2008

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:
  No entries
Permit:
Permit:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    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
```

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.

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 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.

The following completed configuration appears:

```
The following configuration was entered.
service host
network-settings
host-ip 10.89.143.126/24,10.89.143.254
host-name sensor126
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
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 10.89.143.92 key-id 1
exit
```

```
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 8 Enter **2** to save the configuration (or **3** to continue with advanced setup using the CLI, IDM, or IME).

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

Step 9 Enter **yes** to reboot the sensor.

Step 10 After reboot, log in to the sensor, and 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 11 Write down the certificate fingerprints.

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

Step 12 Apply the most recent service pack and signature update.

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

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 18-1.

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

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

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.

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.

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

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

Step 5 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 6 Enter **yes** to modify the interface and virtual sensor configuration.

The current interface configuration appears:

```
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 7 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 8 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] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Step 9 Enter **1** to add an inline VLAN pair to GigabitEthernet0/0, for example:

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

Step 10 Enter a subinterface number and description:

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

Step 11 Enter numbers for VLAN 1 and 2:

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

Step 12 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, GigabitEthernet0/1, for inline VLAN pair.

Step 13 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 14 Enter **4** to add an inline interface pair.

The following options appear:

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

Step 15 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 16 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 17 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 18 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 19 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] 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 20 Enter **3** to add inline VLAN pair GigabitEthernet0/0:1.

Step 21 Enter **4** to add inline interface pair NewPair.

Step 22 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:
   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 23 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 24 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 25 Enter **yes** to disable automatic threat prevention on all virtual sensors.

Step 26 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 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 27 Enter **2** to save the configuration.

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

Step 28 Reboot the appliance:

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

Step 29 Enter **yes** to continue the reboot.

Step 30 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 18-1.

Advanced Setup for AIM-IPS

To continue with advanced setup for 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: ********
```

Step 2 Enter the **setup** command.

The System Configuration Dialog is displayed.

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 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 6 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 7 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 8 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 9 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 10 Press **Enter** to exit the interface and virtual sensor configuration menu.

The following option appears:

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

Step 11 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 12 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 aim-ips
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 13 Enter **2** to save the configuration.

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

Step 14 Reboot AIM-IPS.

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

Step 15 Enter **yes** to continue the reboot.

Step 16 Apply the most recent service pack and signature update.

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

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 18-1.

Advanced Setup for AIP-SSM

To continue with advanced setup for AIP-SSM, follow these steps:

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

```
asa# session 1
```

Step 2 Enter the **setup** command.

The System Configuration Dialog is displayed.

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 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://*idsm_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 6 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 7 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 8 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 9 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 10 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 11 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 running IPS 6.0 or later, 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 12 Press **Enter** to return to the main virtual sensor menu.

Step 13 Enter **3** to create a virtual sensor.

The following option appears:

```
Name[]:
```

Step 14 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 15 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 16 Enter **2** to create a signature-definition configuration file.

Step 17 Enter the signature-definition configuration name, **newSig**.

The following options appear:

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

Step 18 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 19 Press **Enter** to exit the interface and virtual sensor configuration menu.

The following option appears:

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

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

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

Step 23 Reboot AIP-SSM.

```
aip-ssm# 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 Apply the most recent service pack and signature update.

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

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 18-1.

Advanced Setup for IDSM-2

To continue with advanced setup for 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
```

Step 2 Enter the **setup** command.

The System Configuration Dialog is displayed.

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 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 6 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 7 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 8 Enter **3** to add promiscuous VLAN groups.

The list of available interfaces is displayed:

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

Step 9 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 10 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 11 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 12 Enter **2** to edit the virtual sensor configuration.

The following option appears:

```
  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

Step 13 Enter **2** to modify the virtual sensor vs0 configuration.

The following options appear:

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

No Interfaces to remove.

Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/7
```

Step 14 Enter **2** to add VLAN group GigabitEthernet0/8:10 to the virtual sensor vs0.

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

Step 15 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: sig0
  Promiscuous Vlan Groups:
   GigabitEthernet0/8:10  (Vlans: unassigned)
   GigabitEthernet0/8:9  (Vlans: 1-100)

  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

Step 16 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 17 Press **Enter** to exit the interface and virtual sensor configuration menu.

Step 18 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 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 19 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 20 Enter **2** to save the configuration.

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

Step 21 Reboot IDSM-2:

```
idsm-2# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

Step 22 Enter **yes** to continue the reboot.

Step 23 Apply the most recent service pack and signature update.

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

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 18-1.

Advanced Setup for NME-IPS

To continue with advanced setup for NME-IPS, follow these steps:

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

```
router# service-module ids-sensor 1/0 session
Trying 10.1.9.1, 2322 ... Open
```

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

Step 2 Enter the **setup** command.

The System Configuration Dialog is displayed.

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 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://*nme_ips_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 6 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 7 Enter **2** to modify the virtual sensor configuration.

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/1
 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 **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 9 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 10 Press **Enter** to exit the interface and virtual sensor configuration menu.

The following option appears:

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

Step 11 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 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 12 Enter **yes** if you want to disable automatic threat prevention on all virtual sensors; otherwise, press **Enter** to accept the default of no.

The following completed configuration appears:

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name nme-ips
telnet-option 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 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides
override-item-status Enabled
risk-rating-range 90-100
exit
exit

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

Step 13 Enter **2** to save the configuration.

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

Step 14 Reboot NME-IPS.

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

Step 15 Enter **yes** to continue the reboot.

Step 16 Apply the most recent service pack and signature update.

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

For More Information

For the procedure for obtaining the most recent IPS software, see Obtaining Cisco IPS Software, page 18-1.

Verifying Initialization

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 Fri Mar 28 19:24:58 2008
! ------------------------------
! Version 6.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S310.0   2007-12-05
!     Virus Update        V1.2     2005-11-24
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.24/25,10.89.147.126
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
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 17, "Logging In to the Sensor."