



## CHAPTER 3

# Initializing the Sensor

---

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

- [Overview, page 3-1](#)
- [System Configuration Dialog, page 3-1](#)
- [Initializing the Sensor, page 3-2](#)
- [Verifying Initialization, page 3-7](#)

## Overview

After you have installed 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, time settings, and assign and enable interfaces. After you have initialized the sensor, you can communicate with it over the network. You are then ready to configure intrusion prevention using either the CLI, IDM, or ASDM.

## System Configuration Dialog

When you type 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, press the question mark (?) key 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 type **yes**, the configuration is saved. If you type **no**, the configuration is not saved and the process begins again. There is no default for this prompt; you must type either **yes** or **no**.

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

You can edit the default virtual sensor, vs0, through the System Configuration Dialog. You can assign promiscuous and/or inline-pairs to the virtual sensor. This also enables the assigned interfaces. After setup is complete, the virtual sensor is configured to monitor traffic.

**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.

## Initializing the Sensor

To initialize the sensor, follow these steps:

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

- Log in to the appliance by using a serial connection or with a monitor and keyboard.

**Note**

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

- Session to IDSM-2:

- For Catalyst software:

```
cat6k> enable
cat6k> (enable) session module_number
```

- For Cisco IOS software:

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

- Session to NM-CIDS:

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

- Session to AIP-SSM:

```
asa# session 1
```

**Note**

The default username and password are both **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.

**Caution**

If you forget your password, you may have to reimage your sensor (see [Chapter 17, “Upgrading, Downgrading, and Installing System Images”](#)), unless there is another user with Administrator privileges. The other Administrator can log in and assign a new password to the user who forgot the password. Or, if you have created the service account for support purposes, you can have TAC create a password. For more information, see [Creating the Service Account, page 4-13](#).

After you change the password, the `sensor#` prompt appears.

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

The System Configuration Dialog is displayed.



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

```
--- 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
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
```

```
Current time: Wed May 5 10:25:35 2004
```

**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** Type **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 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://sensor_ip_address:port` (for example, `https://10.1.9.201:1040`).



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

**Step 10** Type **yes** to modify the network access list.

- a. If you want to delete an entry, type the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.
- b. Type the IP address and netmask of the network you want to add to the access list.  
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 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.
- 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** Type **yes** to modify the system clock settings.

- a. Type **yes** if you want to use NTP.

You will 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. For the procedure, see [Configuring the Sensor to Use an NTP Time Source](#), page 4-29.

- b. Type **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 april.
- 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 first Sunday in April, and a stop time of 2 a.m. on the fourth Sunday in October. 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 october.
- 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. Type **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 offset.  
The default is 0.  
Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian).

**Step 12** Type **yes** to modify the virtual sensor configuration (vs0).

The current interface configuration appears:

```
Current interface configuration
Command control: GigabitEthernet0/1
Unused:
  GigabitEthernet2/1
  GigabitEthernet2/0
Promiscuous:
  GigabitEthernet0/0
Inline:
  None
```

**Step 13** Type **yes** to add a promiscuous or monitoring interface.

**Step 14** Type the interface you want to add, for example, **GigabitEthernet0/1**.

**Step 15** Type **yes** to add inline pairs (appears only if your platform supports inline pairs).

a. Type the inline pair name.

b. Type the inline pair description.

The default is Created via setup by user <yourusername>.

c. Type the name of the first interface in the inline pair, **interface1**.

d. Type the name of the second interface in the inline pair, **interface2**.

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 16** Type **2** to save the configuration.

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

**Step 17** Type **yes** to modify the system date and time.



**Note** This option is not available on modules or when NTP has been configured. The modules get their time from the router or switch in which they are installed, or from the configured NTP server.

a. Type the local date (yyyy-mm-dd).

b. Type the local time (hh:mm:ss).

**Step 18** Reboot the sensor:

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

**Step 19** Type **yes** to continue the reboot.

**Step 20** 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 21** Write down the certificate fingerprints.

You will need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

**Step 22** Apply the most recent service pack and signature update.

See [Chapter 18, “Obtaining Cisco IPS Software,”](#) for information on how to obtain the most recent software. The Readme explains how to apply the most recent software update.

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

## 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.

For the procedure, see [Chapter 2, “Logging In to the Sensor.”](#)

**Step 2** View your configuration:

```

sensor# show configuration
generating current config:
! -----
! Version 5.0(1)
! Current configuration last modified Thu Aug 12 16:55:33 2004
! -----
service analysis-engine
global-parameters
ip-logging
max-open-iplog-files 30
exit
exit
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
exit
! -----
service authentication
exit
! -----
service host
network-settings
host-ip 10.89.146.110/24,10.89.146.254
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 10.89.0.0/16
access-list 64.101.0.0/16
access-list 10.89.149.31/32
access-list 64.102.0.0/16
ftp-timeout 150
exit
exit
time-zone-settings
offset -360

```

```

standard-time-zone-name CST
exit
summertime-option recurring
summertime-zone-name CST
start-summertime
month april
week-of-month first
day-of-week sunday
exit
exit
! -----
service interface
physical-interfaces GigabitEthernet0/1
description Something
alt-tcp-reset-interface none
exit
bypass-mode off
interface-notifications
missed-percentage-threshold 2
exit
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 will need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

---