CHAPTER 10

Initializing the Sensor

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

- Overview, page 10-1
- System Configuration Dialog, page 10-1
- Initializing the Sensor, page 10-2
- Verifying Initialization, page 10-8

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.

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, 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 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 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:

    ```
    switch# 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 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.

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

Step 3 Enter 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 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 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/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 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.

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 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. 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 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 Enter **`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
  Inline VLAN Pair:
    None
```

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

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

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

a. Enter the inline interface pair name.

b. Enter the inline interface pair description.

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

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

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

e. Repeat Steps a through d to add another inline interface pair, or press **Enter** for the next option.

Step 16 Enter **`yes`** to add inline VLAN pairs (appears only if your platform supports inline VLAN pairs).

A list of interfaces available for inline VLAN pairs appears:

```
Available Interfaces:
 [1] GigabitEthernet0/0
 [2] GigabitEthernet2/0
 [3] GigabitEthernet2/1
```

Step 17 Enter the number of the interface you want to subdivide into inline VLAN pairs.

The current inline VLAN pair configuration for that interface appears:

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

a. Enter the subinterface number to add.

b. Enter the inline VLAN pair description.

c. Enter the first VLAN number (vlan1).

d. Enter the second VLAN number (vlan2).

e. Repeat Steps a through d to add another inline VLAN pair on this interface or press **Enter** for the next option.

Step 18 Enter **yes** to subdivide another interface. Enter **no** or press **Enter** to complete the addition of the inline VLAN pairs.

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

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

Step 20 Enter **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. Enter the local date (yyyy-mm-dd).

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

Step 21 Reboot the sensor:

```
sensor# 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 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 24 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 25 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 sensor for intrusion prevention.

For More Information

- For the procedure for using HTTPS to log in to IDM, refer to Logging In to IDM.
- For information on how to obtain the most recent software, see Obtaining Cisco IPS Software, page 11-1.
- For the procedures for reimaging sensors, refer to Upgrading, Downgrading, and Installing System Images.
- For the procedure for creating the Service account, refer to Creating the Service Account.
- For the procedure for configuring NTP, refer to Configuring the Sensor to Use an NTP Time Source.

- For the procedures for configuring intrusion prevention on your sensor, refer to the following documents:
  - *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*
  - *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*

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
generating current config:
! ------------------------------
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
```

```
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
```

```
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTAlVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMDUwNjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESM
BAGA1UECxMJU1NNLUlQUzEwMRYwFAYDVQQDEw0xMC44OS4xNDkuMjI3MIGfMA0GCSqGSIb3DQEBAQUAA
4GNADCBiQKBgQCoOobDuZOEPudw63Rlt8K1YsymzR/D9Rlcnad/U0gjAQGfcUh3sG3TXPQewon1fH0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANMf4zPcPCAORJ6DMQHFj44A+3tMZWsC
yaod23S1oYOxx7v5puPDYn3IQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVwHji12vBLo+biULJG95hbTFlqO+ba3R6nPD3tepgx5zTdOr2onnlFHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ1lAQDiogskdCs4ax1tB4SbEU5y1tktKgcwWEdJpbbNJhzpoRsRICfM3HlOEwN
exit
! ------------------------------
service web-server
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 these 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 various sensors, refer to Logging In to the Sensor.