Basic Configuration Using the CLI

The command line interface (CLI) for IDS version 4.0 is the user interface that enables you to access the sensor through Telnet, SSH, and serial interface connections. Refer to the following topics for more information on using the CLI for version 4.0.

Introducing the CLI

This section contains these topics:

CLI Modes

The command line interface (CLI) for IDS version 4.0 supports the following command modes. Each mode provides access to a subset of commands.

Note In the following mode descriptions, where the prompt includes `sensor`, *sensor* is the name assigned to the device you are logging in to.

- **Privileged Exec**—Exec mode is the first level of the CLI. You enter Exec mode by logging in to the CLI. Exec mode is denoted by the prompt `sensor#`.
- **Global Configuration**—Configuration mode is the second level of the CLI. You enter Configuration mode by first logging in to the CLI and then typing **configure terminal**. Configuration mode is denoted by the prompt `sensor(config)#`.
- **Interface Command-Control Configuration**—Interface Command-Control Configuration mode is a third-level CLI mode. You enter Interface Command-Control Configuration mode by first entering Global Configuration mode and then typing **interface command-control**. Interface Command-Control Configuration mode is denoted by the prompt `sensor(config-if)#`.
- **Interface Group Configuration**—Interface Group Configuration is a third-level CLI mode. You enter Interface Group Configuration mode by first entering Global Configuration mode and then typing **interface group <number>**, where <*number*> is the group number. Config interface group mode is denoted by the prompt `sensor(config-ifg)#`.
- **Interface Sensing Configuration**—Interface Sensing Configuration is a third-level CLI mode. You enter Interface Sensing Configuration mode by first entering Global Configuration mode and then typing **interface sensing <name>**, where <*name*> is the logical interface name. Interface Sensing Configuration mode is denoted by the prompt `sensor(config-ifs)#`.
- **Service**—Service mode is a generic command mode. You enter Service mode by first entering Global Configuration mode and then typing **service <serviceName>**, where <*serviceName*> identifies the actual service you are trying to access, such as **Host**. Service mode is denoted by the prompt `sensor(config-<serviceName>)#`.

- **Virtual Sensor Configuration**—Virtual Sensor Configuration is a third-level CLI mode. You enter Virtual Sensor Configuration mode by typing **service virtual sensor-configuration** followed by the logical virtual sensor configuration name. Currently, the only allowed name is **virtualSensor**. Virtual Sensor Configuration mode is denoted by the prompt `sensor(config-vsc)#`.
- **Alarm Channel Configuration**—Alarm Channel Configuration is a third-level CLI mode. You enter Alarm Channel Configuration mode by typing **service alarm-channel-configuration** followed by the logical alarm channel configuration name. Currently, the only allowed name is **virtualAlarm**. Alarm Channel Configuration mode is denoted by the prompt `sensor(config-acc)#`.
- **Tune Micro Engines**—Tune Micro Engines is a fourth-level CLI mode. You enter Tune Micro Engines mode by first entering Virtual Sensor Configuration mode and then typing **tune-micro-engines**. Tune Micro Engines mode is denoted by the prompt `sensor(config-vsc-virtualSensor)#`.
- **Tune Alarm Channel**—Tune Alarm Channel is a fourth-level CLI mode. You enter Tune Alarm Channel mode by first entering Alarm Channel Configuration mode and then typing **tune-alarm-channel**. Tune Alarm Channel mode is denoted by the prompt `sensor(config-acc-virtualAlarm)#`.

Tips for Using the CLI

Refer to the following tips when using the CLI for IDS version 4.0.

Prompts

- You cannot change the prompt displayed for the CLI commands.
- User interactive prompts occur when the system displays a question and waits for user input. The default input is displayed inside brackets [ ]. To accept the default input, press **Enter**.

Help

- To display the help for a command, type **?** after the command. You can also type **?** after an incomplete token to view the valid tokens that will complete the command. Refer to the following examples to compare the two outputs.

```
sensor# configure ?
terminal Configure from the terminal
sensor# configure
```

```
sensor(config)# ip n?
name-server nat
sensor(config)# ip n
```

Note If you type a space between the incomplete token and the ?, as in **ip n ?**, the system returns the error `% Ambiguous command: ip n`.

- Only commands available in the current mode are displayed by help.

Tab Completion

- If you are unsure of the complete syntax for a command, you can type a portion of the command and press Tab to complete the command.
- If multiple commands match for tab completion, nothing is displayed, the terminal repeats the current line you entered.
- Only commands available in the current mode are displayed by tab complete and help.

Recall

- To recall the commands entered in a mode, use the Up Arrow or Down Arrow keys or press the Control key (Ctrl) simultaneously with the p key (**Ctrl-p**) or n key (**Ctrl-n**).

Note Help and tab complete requests are not reported in the recall list.

- A blank prompt indicates the end of the recall list.

Case Sensitivity

- The CLI is not case sensitive, but it does echo back the text in the same case you typed it. For example, if you type:

  `sensor# CONF` and press Tab, the sensor will display:
  `sensor# CONFigure`

Display Options

- `–More–` is an interactive prompt that indicates that the terminal output exceeds the allotted display space. To display the remaining output, press the Spacebar to display the next page of output or press the Enter to display the output one line at a time.
- To clear the current line contents and return to a blank command line, press the Control key (Ctrl) simultaneously with the c key (**Ctrl-c**) or press the **q** key.

Keywords

- In general, use the **no** form of a command to disable a feature or function. Use the command without the keyword no to enable a disabled feature or function. For example, the command **shutdown** disables an interface, the command **no shutdown** enables the interface. Refer to the individual commands for a complete description of what the **no** form of that command does.
- Configuration commands that specify a default value in the configuration files, such as service and tune-micro-engines, can have a **default** form. The default form of a command returns the command setting to the default value.

User Roles

The CLI for IDS version 4.0 supports three user roles: Administrator, Operator, and Viewer. The privilege levels for each role are different; therefore, the menus and available commands vary for each role.

- **Administrators**—This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
  - Add users and assign passwords.
  - Enable and disable control of physical interfaces and interface groups.
  - Assign physical sensing interfaces to interface groups.

  - Modify the list of hosts allowed to connect to the sensor as configuring or viewing agents.
  - Modify sensor address configuration.
  - Tune signatures.
  - Assign virtual sensor configuration to interface groups.
  - Manage routers.
- **Operators**—This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
  - Modify their passwords.
  - Tune signatures.
  - Manage routers.
- **Viewers**—This user role has the lowest level of privileges. Viewers can view configuration and event data and can perform the following function:
  - Modify their passwords.

Tip Monitoring applications, such as IDS Event Viewer, only require viewer access to the sensor. You can use the CLI to setup a user account with viewer privileges and then configure IDS Event Viewer to use this account to connect to the sensor.

- **Service**—This user role does not have direct access to the CLI. Service account users are logged directly into a bash shell. This account is intended to be used for support and troubleshooting purposes only. Unauthorized modifications are not supported and will require the device to be re-imaged to guarantee proper operation. You can create only one user with the service role.

Initial Configuration Tasks

You can use the CLI to perform the following basic tasks:

- Initializing the Sensor, page 4-7
- Creating the Service Account, page 4-13

Initializing the Sensor

After you have installed the sensors on your network, you can use the **setup** command to initially configure them.

Note If you have an IDS-4235 or IDS-4250, you must apply the BIOS upgrade before installing the version 4.0 software. See Upgrading the BIOS on the IDS-4235 and IDS-4250, page 1-10.

Note For support reasons, you must set up the service account after initializing the sensor. See the Creating the Service Account, page 4-13.

To initially configure the sensor, follow these steps:

Step 1 Log in to the CLI.

a. Session in to the IDS module by entering the **session** *module_number* command at the prompt.

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

Note The default username and password are both **cisco**.

Step 2 You are prompted to change the default password.

Note 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 re-image 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 his password. Or, if you have created the service account, you can have TAC create a password. See Creating the Service Account, page 4-13, for more information.

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.

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

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

Note Press the spacebar to show one page at a time.

Step 5 Enter **yes** to continue.

Step 6 Enter the following information:

- Host name

  The host name is a case-sensitive character string up to 256 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

- IP address

  An IP address is a 32-bit address written as four octets separated by periods, X.X.X.X, where X=0-255. The default is 10.1.9.201.

- Netmask

  The netmask is a 32-bit address written as four octets separated by periods, X.X.X.X, where X=0-255. The default for a Class C address is 255.255.255.0.

- Default gateway

  The default gateway is the default router IP address for the appliance. The default is 10.1.9.1.

- Telnet server status

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

- 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 IDS Device Manager in the format `https://`*sensor ip address*`:port` (for example, `https://10.1.9.201:1040`).

Step 7 Enter **yes** to save the configuration.

```
Use this configuration? [yes]: yes
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
```

Step 8 Enter **no** to avoid rebooting the sensor at this time.

If you modified the IP address, netmask, default gateway or web port, you are prompted for reboot.

```
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is
rebooted. Please use the reset command to complete the configuration.
```

See Step 18 for the **reset** command.

Step 9 Modify the network access lists to allow remote access:

a. Enter configure terminal mode:

```
sensor# configure terminal
```

b. Enter host configuration mode:

```
sensor(config)# service host
```

c. Enter network parameters configuration mode:

```
sensor(config-Host)# networkParams
```

d. View the current settings:

```
sensor(config-Host-net)# show settings
networkParams
 ————————————————————-
 ipAddress: 10.1.9.201
 netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.1.9.1
hostname: sensor
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 1)
————————————————————-
ipAddress: 10.0.0.0
netmask: 255.0.0.0 default: 255.255.255.255
```

e. Remove the 10.0.0.0 network from the access list:

```
sensor(config-Host-net)# no accessList ipAddress 10.0.0.0 netmask
255.0.0.0
```

Note The access list contains a default network address entry 10.0.0.0/255.0.0.0. You must remove this and modify the access list to suit your network.

f. To enter single host to the access list, use the following command:

```
sensor(config-Host-net)# accessList ipAddress 10.1.2.3
```

g. To add an entire network to the access list, use the following command:

```
sensor(config-Host-net)# accessList ipAddress 10.10.10.0 netmask
255.255.255.0
```

Note Enter the netmask if the IP address is a network address (as opposed to a host address).

h. Repeat Steps f and g for each address that you want to add to the access list.

i. View your changes:

```
sensor(config-Host-net)# show settings
networkParams
------------------------
ipAddress: 10.1.9.201
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.1.9.1
hostname: sensor
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 2)
------------------------
ipAddress: 10.1.2.3
netmask: 255.255.255.255 <defaulted>
------------------------
ipAddress: 10.10.10.0
netmask: 255.255.255.0 default: 255.255.255.255
```

j. Exit network parameters configuration mode:

```
sensor(config-Host-net)# exit
```

Step 10 Configure the time:

Caution Make sure that the Catalyst supervisor engine's clock and timezone are set correctly (unless the IDS module is configured to use NTP) before you set the time on the module. The module obtains the current UTC time from the supervisor engine and applies the timezone settings that are configured in the IDS configuration to calculate the local time. If the supervisor engine's time in incorrect, the module's local time will also be incorrect.

a. Enter time parameter configuration mode:

```
sensor(config-Host)# timeParams
```

b. Specify the standard time offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian):

```
sensor(config-Host-tim)# offset -360
```

c. Specify the standard time zone:

```
sensor(config-Host-tim)# standardTimeZoneName CST
```

d. Enter summertime parameter configuration mode:

```
sensor(config-Host-tim)# summerTimeParams
```

e. Specify that summertime parameters recur at the same time each year:

```
sensor(config-Host-tim-sum)# active-selection recurringParams
```

f. Enter recurring summertime parameter configuration mode:

```
sensor(config-Host-tim-sum)# recurringParams
```

g. Specify the summertime time zone name:

```
sensor(config-Host-tim-sum-rec)# summerTimeZoneName CDT
```

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. Exit time parameter configuration mode:

```
sensor(config-Host-tim-sum-rec)# exit
sensor(config-Host-tim-sum)# exit
sensor(config-Host-tim)# exit
```

Step 11 Exit configure host mode:

```
sensor(config-Host)# exit
```

Step 12 Enter **yes** to apply the changes.

Step 13 Enter **no** to avoid rebooting the sensor at this time.

```
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is
rebooted. Please use the reset command to complete the configuration.
```

See Step 18 for the **reset** command.

Step 14 Exit configure terminal mode:

```
sensor(config)# exit
```

Step 15 Set the clock:

clock set *hh:mm month day year*

Note This step does not apply to the IDS module. You can only manually set the clock on the IDS appliance.

Step 16 Generate the self-signed X.509 certificate (needed by TLS) by entering the following command:

```
sensor# tls generate-key
MD5 fingerprint is 47:B4:C9:36:B1:E7:D2:5E:D1:3E:F6:B7:83:F4:68:60
SHA1 fingerprint is
8B:26:BB:EB:04:D4:9F:27:02:0E:25:F7:BE:0E:91:4F:B8:0A:CF:7B
```

Step 17 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 18 Reboot the sensor:

```
sensor# reset
```

Step 19 Enter **yes** to continue rebooting the sensor.

```
Warning: Executing this command will stop all applications and reboot
the node.
Continue with reset? : yes
Request Succeeded.
```

Creating the Service Account

You should create a service account for TAC to use during troubleshooting. Although more then one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

Caution Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. We do not support the addition and/or running of an additional service to the operating system through the service account, because it affects the proper performance and proper functioning of the other IDS services. TAC does not support a sensor on which additional services have been added.

To create the service account, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter configure terminal mode:

```
sensor# configure terminal
```

Step 3 Create the service account:

```
sensor(config)# username user privilege service
```

Step 4 Enter the password when prompted.

Step 5 Exit configure terminal mode:

```
sensor(config)# exit
```

When you enter the service account, you receive the following warning:

```
********************** WARNING ********************** UNAUTHORIZED
ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. This account is intended
to be used for support and troubleshooting purposes only. Unauthorized
modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*****************************************************
```

Manually Setting the System Clock

You can manually set the system clock of the IDS appliance. Use the **clock set** command to set the time, relative to the configured time zone, if no other timing mechanisms are available.

Note If you are using an NTP or VINES clock source, or if you have a router with calendar capability, you do not need to use the **clock set** command to set the system clock.

Note The IDS module obtains its time configuration from the Catalyst 6500 family switch.

To manually set the system clock, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command:

clock set *hh:mm:[:ss] month day year*

- hh:mm [:ss]—Current time in hours (military format), minutes, and seconds.
- day—Current day (by date) in the month.
- month—Current month (by name, no abbreviation).
- year—Current year (no abbreviation).

The following example manually sets the system clock to 1:32 p.m., July 29, 2002:

```
sensor# clock set 13:32 July 29 2002
sensor#
```

Logging in to the Sensor

To log in to the sensor, SSH to the IDS appliance or telnet to the IDM module in the Catalyst 6500 series switch.

To log in to the sensor, follow these steps:

Step 1 Do one of the following:

a. SSH to the IDS appliance:

ssh *user@ip-address*

b. Telnet to the Catalyst 6500 series switch:

telnet *ip address*
session *slot_number*

Step 2 Enter your username and password at the login prompt:

Note The default is cisco.

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

If you are logging in for the first time, you are prompted to change your password.

Changing a Password

The **password** command updates the password on the local sensor. You can also use this command to change the password for an existing user.

To change the password for a user, follow these steps:

Step 1 Type the following command to enter configuration mode:

```
configure terminal
```

The `sensor(config)#` prompt is displayed.

Step 2 Enter the following commands to change the password for the user:

```
sensor(config)# password
Enter Old Login Password: ************
Enter New Login Password: ************
```

```
Re-enter New Login Password: ************
sensor(config)#
```

Step 3 With administrator privileges, you can change the password of another user by entering these commands:

Note This example modifies the password for the user "tester."

```
sensor(config)# password tester
Enter New Login Password: ******
Re-enter New Login Password: ******
sensor(config)#
```

Adding a User

You can add a new user, set the privilege level—administrator, operator, viewer, or service account—and set the password for the new user. Use the **username** command to create users on the local system. Use the **no** form of this command to remove a user from the system.

The **username** command provides username and password authentication for login purposes only. You cannot use this command to remove a user who is logged in to the system. If you do not specify a password, the system prompts you for one. Use the **password** command to change the password for existing users. Use the **privilege** command to change the privilege for existing users. You cannot use the **privilege** command to change a user to the service role. To change user privileges, you must remove that user and then use the **username** command to create a user.

To add a user, follow these steps:

Step 1 Enter the following command to enter configuration mode:

```
configure terminal
```

The `sensor(config)#` prompt is displayed.

Step 2 Enter the following command to specify the parameters for the user:

username *name* **password** *password* **privilege** *administrator/operator/viewer/service*

The following example adds the user "tester" with a privilege level of viewer and the password "testpassword."

```
sensor(config)# username tester
Enter Login Password: *****
Re-enter Login Password: *****
```

Step 3 Verify that the user has been added:

a. Type **exit** to exit configuration mode.

b. Enter the following command:

```
show users all
```

A list of users is displayed.

Adding Trusted Hosts

You can identify hosts (trusted hosts) that are allowed to connect to the sensor.

To add a trusted host, follow these steps:

Step 1 Enter the following command to enter configuration mode:

```
configure terminal
```

The `sensor(config)#` prompt is displayed.

Step 2 Enter the following command to enter service host mode:

```
service host
```

Step 3 Enter the following command to enter network parameters submode:

```
networkParams
```

Step 4 Enter the following command and parameter to specify the allowed host:

accessList ipAddress *ipaddress*

The IP address is now in the list of trusted hosts.

Step 5 You can enter an optional netmask to specify allowed networks.

accessList ipAddress *ipaddress* **netmask** *netmask*

Step 6 Exit service mode to apply changes.

Removing a User

You can delete a user and thus prevent access to the sensor.

To remove a user, follow these steps:

Step 1 Type the following command to enter configuration mode:

configure terminal

The `sensor(config)#` prompt is displayed.

Step 2 Enter the following command to remove the user:

no username *name*

The username is now removed from the sensor.

Step 3 Verify that the user has been removed:

a. Type **exit** to exit configuration mode.

b. Enter the following command:

show users all

A list of users is displayed. The user you removed no longer appears in the list.

Adding Known Hosts to the SSH Known Hosts Lists

You must add hosts to the SSH known hosts list so that the sensor can recognize hosts that it can communicate with through SSH.

To add a host to the list of SSH known hosts, follow these steps:

Step 1 Enter configuration terminal mode:

```
sensor# configure terminal
```

Step 2 Enter the IP address of the host you want to add:

```
sensor(config)# ssh host-key 10.89.147.195

MD5 fingerprint is 0E:C0:E3:36:E3:DF:B1:70:2D:E8:8C:5C:28:0E:27:00
Bubble Babble is
xifik-ladom-lugyz-kyciz-hikib-rivip-tizaf-metan-cyvyb-cubah-tuxix
```

Step 3 Enter **yes** to have the fingerprint added to the known hosts list.

```
Would you like to add this to the known hosts table for this
host?[yes] yes
```

Step 4 To see the list of SSH known hosts, enter these commands:

```
sensor(config)# service SshKnownHosts
sensor(config-SshKnownHosts)# show settings
```

The following output appears:

```
rsa1Keys (min: 0, max: 500, current: 1)
-----------------------------
id: 10.89.147.195
exponent: 35
length: 1024
modulus:
151936152815071142258918316164087378281570933465405127461564938127898 3
286041312612481177367123522013025197338658324618560204597093850118250 4
305227602781635186037007504076117930686028701278264811264429766754467 3
638988707417212418007114846697947098702479401735835566226681045310693 7
837868583043330248263314526 37
-----------------------------
```

Step 5 To remove an entry, enter these commands:

```
sensor(config-SshKnownHosts)# no rsa1Keys id 10.89.147.195
sensor(config-SshKnownHosts)# show settings
rsa1Keys (min: 0, max: 500, current: 0)
 ---------------------------
```

Step 6 Exit configuration terminal mode:

```
sensor(config-SshKnownHosts)# exit
Apply Changes:?[yes]: yes
sensor(config)# exit
```

Administrative Tasks

This section contains procedures for administrative tasks on the sensor:

Displaying the Current Version and Configuration

You can display the IDS software version and sensor configuration. Use the **show version** command to display version information for all installed operating system (OS) packages, signature packages, and IDS processes running on the system. To view the configuration for the entire system, use the **more current-config** command.

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter **show version**:

The following output appears:

```
sensor31# show version
Application Partition:

Cisco Systems Intrusion Detection Sensor, Version 4.0(1)S45

OS Version 2.4.18-5smpbigphys
Platform: IDS-4250-XL
Sensor up-time is 6 days.
Using 406511616 out of 1846276096 bytes of available memory (22%
usage)
Using 544M out of 15G bytes of available disk space (4% usage)

MainApp 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
AnalysisEngine 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running
Authentication 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running
Logger 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
NetworkAccess 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running
TransactionSource 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600
Running
WebServer 2003_Jan_23_02.00 (Release) 2003-01-23T02:00:25-0600 Running
CLI 2003_Jan_17_18.33 (Release) 2003-01-17T18:33:18-0600

Upgrade History:

IDS-maj-4.0-1-S45.rpm.pkg 20:43:18 UTC Mon Feb 03 2003

Recovery Partition Version 1.1 - 4.0(1)S45
```

Note If the –MORE– prompt is displayed, press **Ctrl-C** to get back to the CLI prompt.

Step 3 Enter **more current-config**.

The following output appears:

```
sensor# more current-config
! ------------------
service Authentication
general
attemptLimit 0
methods method Local
exit
exit
exit
! ------------------
service Host
networkParams
ipAddress 10.89.147.31
netmask 255.255.255.128
defaultGateway 10.89.147.126
hostname sensor31
telnetOption disabled
accessList ipAddress 10.0.0.0 netmask 255.0.0.0
accessList ipAddress 64.101.0.0 netmask 255.255.0.0
exit
optionalAutoUpgrade
active-selection
autoUpgradeParams autoUpgradeParams
schedule
active-selection calendarUpgrade
calendarUpgrade
timesOfDay time 14:40:00
daysOfWeek day wed
exit
exit
ipAddress 10.89.149.10
directory var/relupdates
username netrangr
password 12345
fileCopyProtocol ftp
exit
exit
timeParams
offset -360
standardTimeZoneName CST
summerTimeParams
active-selection none
exit
```

```
exit
exit
```

Backing up and Restoring the Current Configuration File

You can do the following tasks to protect your configuration:

- Back up your current configuration.
- Display the backup of the current configuration.
- Merge the backup configuration file with the current configuration.
- Overwrite the current configuration file with the backup configuration file.

To back up your current configuration, follow these steps:

Step 1 Enter the following command at the prompt.

```
copy current-config backup-config
```

The current configuration is saved in a backup file.

Step 2 Enter the following command to display the backed up configuration file:

```
more backup-config
```

The backed up configuration file is displayed.

Step 3 Choose one of the following:

a. Enter the following command to merge the backup configuration into the current configuration:

```
copy backup-config current-config
```

b. Enter the following command to overwrite the current configuration with the back-up configuration:

```
copy/erase backup-config current-config
```

Displaying Events

Use the **show events** command to display the local event log. You can display new events, events from a specific time or of a specific severity, and delete all events.

The **show events** command displays the requested event types beginning at the requested start time. If no start time is entered, the selected events are displayed beginning at the current time. If no event types are entered, all events are displayed. Events are displayed as a live feed. You can cancel the live feed by the pressing Ctrl-C.

To display events, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command at the CLI prompt:

```
show events
```

New alarm events are displayed as they occur.

Step 3 Enter the following command to display alarm events from a specific time:

show events *hh:mm month day year*

For example, **show events 10:00 September 22 2002** displays all events since 10:00 am September 22. 2002.

Events from the specified time are displayed.

Step 4 Enter the following command to display alarm events since a specified time for a specified alert level:

show events alert *level hh:mm month day year*

For example, **show events alert high 10:00 September 22 2002** displays all high severity events since 10:00 am September 22, 2002.

Events from the specified time are displayed.

Step 5 Enter the following command to delete events from the event store:

```
clear events
```

The following shows the entire syntax for the show events commands. See *Cisco Intrusion Detection System Command Reference Version 4.0* for more information.

show events [{ [**alert** [*informational*] [*low*] [*medium*] [*high*]] | **error** [*warning* | *error* | *fatal*] | **log | NAC | status**}] [*hh:mm:ss*[*month day* [*year*]]]

Starting and Stopping the Sensor

The **reset** command shuts down the applications running on the sensor and reboots it. If the powerdown option is included, the sensor will be powered off if possible or left in a state where the power can be turned off.

Shutdown begins immediately after the command is executed. Because shutdown may take a little time, you can continue to access CLI commands (access is not denied) but access can be terminated without warning.

To start and stop the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command at the CLI prompt:

```
reset
```

You are asked if you want to continue with reset.

Step 3 Enter **yes**.

The sensor reboots.

Step 4 Enter the following command at the CLI prompt:

```
reset powerdown
```

You are prompted to turn off the power switch on the sensor.

Example output:

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

Displaying Tech Support Information

You can display system information and have it sent to a specific URL for use with troubleshooting with TAC.

You can specify the following destination types:

- **ftp:**—Destination URL for File Transfer Protocol (FTP) network server. The syntax for this prefix is `ftp:[[//username@location]/relativeDirectory]/filename` or `ftp:[[//username@location]//absoluteDirectory]/filename`.
- **scp:**—Destination URL for the Secure Copy Protocol (SCP) network server. The syntax for this prefix is `scp:[[//username@]location]/relativeDirectory]/filename` or `scp:[[//username@]location]//absoluteDirectory]/filename`.

To display tech support information, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter the following command at the prompt:

`show tech-support page password destination-url` *destination-url*

The following variables are optional:

- page—Causes the output to display a page of information at a time.
- password—Leaves passwords and other security information in the output.
- destination—Indicates the information should be formatted as HTML and sent to the destination following this tag.
- destination-url—Identifies the destination for the report file.

Note Press Ctrl-C to get back to the prompt.

The following example places the tech-support output into the file `~csidsuser/reports/sensor1Report.html`. The path is relative to csidsuser's home account:

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2/reports/sensor1Report.html
password:*******
```

The following example places the tech support output into the file `/absolute/reports/sensor1Report.html`:

```
show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
password:*******
```

Configuration Tasks

The following section lists the configuration tasks:

Configuring Alarm Channel System Variables

The **tune-alarm-channel** command allows you to configure system variables for the aggregation process. The items and menus in this configuration depend on the contents of the configuration file and are built dynamically based on the configuration retrieved when the command is executed. The modifications made in this mode and any submodes contained within it are applied when you exit tune-alarm-channel mode.

You can change the value of an alarm channel system variable, but you cannot add variables or delete variables. You also cannot change the name, type, or constraints of a variable.

You use system variables when configuring alarm channel event filters. When you want to use the same value within multiple filters, use a variable. When you change the value of a variable, the variables in all the filters are updated. This saves you from having to change the variable over and over again as you configure alarm filters. See Configuring Alarm Channel Event Filters, page 4-30 for more information.

For example, if you had an IP address space that applied to your engineering group and there were no Windows systems in that group, and you were not worried about any Windows-based attacks, you could set up a USER-ADDR1 to be the engineering group's IP address space. You could then use this variable on the Event Filters page to set up the filter to ignore all Windows-based attacks for USER-ADDR1.

To configure alarm channel system variables, follow these steps:

Step 1 Enter alarm channel system variables submode:

```
configure terminal
service alarm-channel-configuration virtualAlarm
tune-alarm-channel
systemVariables
```

You are in the alarm channel system variables submode:

```
sensor(config-acc-virtualAlarm-sys)#
```

Step 2 View the alarm channel system variables:

```
show settings
```

Look through the list of system variables for the alarm channel and choose the system variable that you want to configure.

Step 3 Enter the system variable you want to configure and its value:

```
SIG1 2001-2006
```

Step 4 View your changes:

```
show settings
```

Step 5 Enter **exit** two times.

Step 6 Enter **yes** to apply the changes.

Configuring Alarm Channel Event Filters

The **tune-alarm-channel** command allows you to configure event filters for the aggregation process. The items and menus in this configuration depend on the contents of the configuration file and are built dynamically based on the configuration retrieved when the command is executed. The modifications made in this mode and any submodes contained within it are applied when you exit tune-alarm-channel mode.

You can configure event filters that are based on source and destination addresses for specified signatures. You can use the alarm channel system variables that you have defined to group addresses for your filters. See Configuring Alarm Channel System Variables, page 4-29, for more information.

To configure alarm channel event filters, follow these steps:

Step 1 Enter alarm channel submode:

```
configure terminal
service alarm-channel-configuration virtualAlarm
tune-alarm-channel
EventFilter
```

You are in the alarm channel event filter submode:

```
sensor(config-acc-virtualAlarm-Eve)#
```

Step 2 To set up a filter:

`Filters SIGID` *signature-id* **`SubSig`** *sub-id* **`SourceAddrs`** *ipaddress* **`DestAddrs`** *ipaddress* **`Exception`** `true | false`

- SIGID—You can use a list (2001, 2004), or a range (2001–2004), an asterisk (*) for all signatures, or one of the SIG variables if you defined them. See Configuring Alarm Channel System Variables, page 4-29, for more information.
- SubSig—Enter the subsignature IDs of the events to which this filter should be applied.
- Exception—Enter the exception (True, False) to the event filter.
- SourceAddrs—Enter the source addresses of events to which this filter should be applied. You can use one of the DMZ or USER-ADDR variables if you defined them. See Configuring Alarm Channel System Variables, page 4-29, for more information.
- DestAddrs—Enter the destination addresses of events to which this filter should be applied. You can use one of the DMZ or USER-ADDR variables if you defined them. See Configuring Alarm Channel System Variables, page 4-29, for more information.

Step 3 View your changes:

`show settings`

Step 4 Enter **exit** two times.

Step 5 Enter **yes** to apply the changes.

Viewing Signature Engines

You can display settings for individual signature engines.

To view signature engine settings, follow these steps:

Step 1 Enter the following command to enter configuration mode:

`configure terminal`

The `sensor(config)#` prompt is displayed.

Step 2 Enter the following command to enter service virtual sensor configuration mode:

```
service virtual-sensor-configuration virtualSensor
```

The `sensor(config-vsc)#` prompt is displayed.

Step 3 Enter the following command to enter tuning mode:

```
tune-micro-engines
```

The `sensor(config-vsc-virtualSensor)#` prompt is displayed.

Step 4 Enter **?** to display a list of signature engine names.

A list of all signature engine names and a description of each is displayed.

Step 5 Enter the engine name whose settings you want to see.

The prompt changes to indicate which signature engine mode you are in.

Step 6 Enter **show settings** to see the signature engine parameters.

Step 7 Press the spacebar to page through all of the settings. Press **Ctrl-C** to return to the prompt.

Configuring Virtual Sensor System Variables

You can change the value of a system variable but you cannot add or delete variables. You cannot change the name or type of a variable. You cannot select the virtual sensor, because there is only one virtual sensor in version 4.0.

Use these virtual sensor system variables when you are tuning signatures. See Tuning Signature Engines, page 4-33, for more information.

To configure virtual sensor system variables, follow these steps:

Step 1 Enter signature engine submode:

```
configure terminal
service virtual-sensor-configuration virtualSensor
tune-micro-engines
systemVariables
```

You are in the virtual sensor system variables submode:

```
sensor(config-vsc-virtualSensor-sys)#
```

Step 2 Enter **?** to see a list of possible virtual sensor system variables.

Step 3 Enter the system variable you want to configure and its value:

- WEBPORTS

  WEBPORTS has a predefined set of ports where web servers are running, but you can edit the value. This variable affects all signatures that have web ports. The default is 80, 3128, 8000, 8010, 8080, 8888, 24326.

- Ports1, Ports2, Ports3, Ports4

  You can set up a list of ports to apply to particular signatures.

- ADDRS1, ADDRS2, ADDRS3, ADDRS4

  You can set up this variable with a list of addresses to use anywhere you can use IP addresses.

- IPReassemblMaxFrags

  You can define the total number of fragments you want the system to queue. You can define a number between 1000 and 50,000. The default is 10,000.

Step 4 Enter **exit** two times.

Step 5 Enter **yes** to apply the changes.

Step 6 View your changes:

```
show settings
```

The value you added now appears in the list of virtual sensor system variables.

Tuning Signature Engines

To tune parameters in a signature engine, follow the procedure for viewing signature engines (see Viewing Signature Engines, page 4-31). When you have chosen a signature engine to tune and are in its mode, you can choose the parameters you want to change.

The **tune-micro-engines** command allows you to configure standard signatures and create custom signatures for the sensor micro-engines. The items and menus in this configuration depend upon the contents of the configuration file and are built dynamically based on the configuration retrieved when the command is executed. The modifications made in this mode and any submodes contained within it are applied to the system when you exit tune-micro-engines mode.

To tune parameters in signature engines, follow these steps:

Step 1 Enter signature engine submode:

```
configure terminal
service virtual-sensor-configuration virtualSensor
tune-micro-engines engine name
```

You are in the signature engine submode:

```
sensor(config-vsc-virtualSensor-ATO)#
```

This example shows the ATOMIC.ARP signature engine.

Step 2 View the signature settings:

```
show settings
```

Look through the list of settings for that signature engine and chose the signature ID that you want to tune.

Step 3 Configure the parameters:

```
signature SIGID signature ID
```

The prompt now displays the signature mode:

```
sensor(config-vsc-virtualSensor-ATO-sig)#
```

Step 4 Enter **?** at the prompt to see a list of configurable parameters.

Step 5 Enter the parameter that you want to configure and add or change the values.

Step 6 View your changes:

```
show settings
```

Step 7 Enter **exit** three times to save your changes.

Step 8 Enter **yes** to apply the changes.

Generating IP Logs

You can configure the sensor to catch all IP traffic associated with the hosts you specify by IP address.

To generate logs files for specific IP addresses, follow these steps:

Step 1 Log in to the CLI.

Step 2 Set up IP logging:

iplog *group-idip-address* **duration** *minutes* **packets** *numPackets* **bytes** *numBytes*

- *group-id*—Group ID to begin/end logging on. This is the interface group. For 4.0, there is only one interface group. Use 0 as the value.
- *ip-address*—Only log packets containing the specified IP address.
- *minutes*—Duration the logging should be active, in minutes. The default is 10 minutes.
- *numPackets*—Number of packets to log. The default is 1000 packets.
- *numBytes*—Number of bytes to log.
- *log-id*—Log ID of logging session to stop. The log-id can be retrieved using the **iplog-status** command.

Here is example output:

```
sensor# iplog 0 10.2.3.1
Logging started for group 0, IP address 10.2.3.1, Log ID 2342
Warning: IP Logging will affect system performance.
sensor#
```

Step 3 Check the log file output:

iplog-status

Here is the example output:

```
sensor# iplog-status

Group:1
IPAddress: 10.1.1.2
Start Time: 10:02:34 8/24/2001
End Time: In progress
```

```
Remaining: 5 minutes or 48 packets
Trigger Alert: Device: deviceName

Group:1
IPAddress: 10.2.3.1
Start Time: 23:34:02 7/1/2001
End Time: 23:44:02 7/1/2001
Remaining:
Trigger Alert: EventId: 209348

sensor#
```

IDS Module Configuration Tasks

This section contains these topics:

Verifying the Installation

Verify that the switch acknowledges the new IDS module and has brought it online.

To verify the installation, follow these steps:

Step 1 Log in to the console.

Step 2 Enter the following command:

`show module show port` *module_number/port_number*

This example shows the output of the **show module** command:

```
cat6k> (enable) show mod
Mod Slot Ports Module-Type Model Sub Status
--- ---- ----- ------------------- ---------- --- ------
1 1 2 1000BaseX Supervisor WS-X6K-SUP2-2GE yes ok
15 1 1 Multilayer Switch Feature WS-F6K-MSFC2 no ok
2 2 8 1000BaseX Ethernet WS-X6408-GBIC no ok
3 3 48 10/100BaseTX Ethernet WS-X6548-RJ-45 no ok
4 4 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
5 5 0 Switch Fabric Module 2 WS-X6500-SFM2 no ok
6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
7 7 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok
Mod Module-Name Serial-Num
--- ---------- ------
1 SAD044409HJ 15 SAD044509KZ
2 JAB04040859
3 SAD0612021X
4 SAD063803LR
5 SAD060705HA
6 SAD05380608
7 SAD0538060L
Mod MAC-Address(es) Hw Fw Sw
--- ---------- ---- ------ ---------
1 00-01-63-d0-73-20 to 00-01-63-d0-73-21 1.1 6.1(3) 7.5(1)
00-01-63-d0-73-1e to 00-01-63-d0-73-1f 00-09-44-89-90-00 to
00-09-44-89-93-ff
15 00-04-9a-12-3b-40 to 00-04-9a-12-3b-7f 1.1 12.1(13)E3 12.1(13)E3
2 00-30-a3-38-9a-30 to 00-30-a3-38-9a-37 2.3 4.2(0.24)V 7.5(1)
3 00-01-63-d7-5a-ca to 00-01-63-d7-5a-f9 4.2 6.3(1) 7.5(1)
4 00-03-fe-aa-c0-08 to 00-03-fe-aa-c0-0f 0.102 7.2(1) 1.3(0.9)m
5 00-01-00-02-00-03 1.1 6.1(3) 7.5(1)
6 00-00-0b-ff-00-00 to 00-00-0b-ff-00-07 0.102 7.2(1) 4.0(1)S37
7 00-40-0b-ff-00-00 to 00-40-0b-ff-00-07 0.101 7.2(1) 4.0(1)S37
e Sub-Model Sub-Serial Sub-Hw
--- ---------- ---------- ------ ---
1 L3 Switching Engine II WS-F6K-PFC2 SAD044302BP 1.0
4 IDS 2 accelerator board WS-SVC-IDSUPG 0347e5fc7e 2.0
6 IDS 2 accelerator board WS-SVC-IDSUPG 0347e5fd02 2.0
7 IDS 2 accelerator board WS-SVC-IDSUPG 0347e5fc6f 2.0
cat6k (enable)
```

Note It is normal for the status to read “other” when the IDS module is first installed. After the IDS module completes the diagnostics routines and comes online, the status reads “ok.” Allow up to 5 minutes for the IDS module to come online.

See Enabling a Full Memory Test, page 4-38, for information on enabling a full memory test after verifying the IDS module installation.

Enabling a Full Memory Test

When the IDS module initially boots, by default it runs a partial memory test. For Catalyst software, you can enable a full memory test when you use the **set boot device bootseq** *mod_number* **mem-test-full** command. This command is specific to Catalyst software. The long memory test takes about 12 minutes.

To enable a full memory test, follow these steps:

Step 1 Log in to the console.

Step 2 Enter the following commands:

```
Console> set boot device cf:1 4 mem-test-full
Console> show boot device 4
```

Step 3 The following output appears:

```
Device BOOT variable = cf:1
FAST BOOT Enabled
```

Step 4 Reset the IDS module by entering the **reset** command.

The full memory test runs.

Note A full memory test takes more time to complete than a partial memory test.

Configuring VACLS

You can set VACLs to capture traffic for IDS from a single VLAN or from multiple VLANs. Ports 7 and 8 monitor traffic from all VLANs on which a security ACL has been applied with the capture feature. If you want to monitor traffic from specific VLANs only, you need to clear the VLANs that you do not want to monitor from the capture feature.

Note By default, port 1 is set as the TCP reset port. Port 2 is the command and control port. Ports 7 and 8 are the monitoring ports and can be configured as security ACL capture ports.

To set VACLs to capture IDS traffic on VLANs, follow these steps:

Step 1 Log into the console.

Step 2 Enter privileged mode.

```
Console> enable
```

Step 3 Enter the following command to set the VACL to capture traffic:

```
Console> (enable) set security acl ip acl name permit (...) capture
```

Step 4 Enter the following command to commit the VACL:

```
Console> (enable) commit security acl
```

Step 5 Enter the following command to map the VACL to the VLANs:

```
Console> (enable) set security acl map acl name [vlans]
```

Step 6 Enter the following command to add the IDS module sniffing port (port 7 or 8) to the VACL capture list:

```
Console> (enable) set security acl capture idsm_mod/port_number
```

This example shows how to capture Cisco IOS traffic on VLANs:

```
Console> (enable) show security acl info all
set security acl ip webacl2
------------------------------
permit tcp any host 10.1.6.1 eq 21 capture
permit tcp host 10.1.6.1 eq 21 any capture
permit tcp any host 10.1.6.1 eq 20
```

```
permit tcp any host 10.1.6.1 eq 80 capture
permit tcp any host 10.1.6.2 eq 80 capture
deny ip any host 10.1.6.1
deny ip any host 10.1.6.2
permit ip any any
```

Note Refer to *Catalyst 6500 Family Command Reference* for more information on trunk ports and ACLs.

Using the mls Command

When you are running the Cisco IOS Firewall on the Multilayer Switch Feature Card (MSFC), you cannot use VACLs to capture traffic for the IDS module, because you cannot apply VACLs to a VLAN in which you have applied an IP inspect rule for the Cisco IOS Firewall. However, you can use the **mls ip ids** command to designate which packets are captured. Packets that are permitted by the ACL are captured. Those denied by the ACL are not captured. The permit/deny parameter does not affect whether a packet is forwarded to destination ports. Packets coming in to that router interface are checked against the IDS ACL to determine if they should be captured.

Note The **mls ip ids** command only captures incoming traffic.

To use the mls ip ids command to capture IDS traffic, follow these steps:

Step 1 Log in to the console.

Step 2 Enter privileged mode.

Step 3 Configure an ACL to designate which packets will be captured:

```
Router (config)# ip access-list extended word
```

Step 4 Select the VLAN interface.

```
Router (config)# interface vlan vlan_number
```

Step 5 On the MSFC, apply the IDS ACL to a router interface.

```
Router (config-if)# mls ip ids word
```

Step 6 On the supervisor engine, add the IDS module sniffing port (port 7 or 8) to the VACL capture list.

```
Console> (enable) set security acl capture idsm_module_port_number
```

Caution For the IDS module to capture all packets marked by the **mls ip ids** command, port 3 of the IDS module must be a member of all VLANs to which those packets are routed.

Configuring SPAN

To use the SPAN source port as a traffic source for the IDS module, set port 1 on the IDS module as the SPAN destination port. You cannot set port 2 on the IDS module as a SPAN source port.

The IDS module can analyze Ethernet VLAN traffic from Ethernet or Fast Ethernet SPAN source ports, or you can specify an Ethernet VLAN as the SPAN source.

To enable SPAN on the IDS module, follow these steps:

Step 1 Enter the following command to enable SPAN to the IDS module from a source port:

set span *[source_module/source_port]* **idsm_module/1** *[rx | tx | both] [filter vlans...]*

Note Use the filter keyword and variable to monitor traffic on specific VLANs on source trunk ports.

Step 2 Enter the following command to enable SPAN to the IDS module from a VLAN:

set span *[vlan]* **idsm_module/1** *[rx | tx | both]*

Step 3 Enter the following command to disable all SPAN traffic to the IDS module:

```
set span disable idsm_module/1
```

Note Refer to *Catalyst 6500 Series Command Reference* for more information on SPAN.

Catalyst Software Supervisor Engine Commands

The IDS module also supports these supervisor engine CLI commands, which are described in more detail in *Catalyst 6500 Series Command Reference*.

- **clear config** *module_number*

  Clears the configuration on the supervisor engine that is associated with the specified IDS module.

- **clear log** *module_number*

  Deletes all entries in the error log for the specified IDS module.

- **session** *slot_number*

  Logs in to the console of the IDS module from the switch console.

- **set module** commands (all other **set module** commands return an error message):
  - **set module name** *module_number*

    Sets the name of the module.
  - **set module power** *module_number* **up | down**

    Enables or disables the power to the specified IDS module.

- **set port name** module_number

  Configures the name for the specified IDS module port.

- **set span**

  Configures port 1 as a SPAN destination port. You cannot use port 1 on the IDS module as a SPAN source port.

- **set trunk**

  Configures trunk ports.

- **set vlan**

  Configures VLAN capture ports.

- **show config**

  Displays the supervisor engine NVRAM configurations.

- **show log**

  Displays the error logs for the specified IDS module.

- **show mac** *module_number*

  Displays the MAC counters for the specified IDS module.

- **show module** *module_number*

  With an IDS module installed, displays "Intrusion Detection System Module" under Module-Type.

- **show port** *module_number*

  Displays the port status for the specified IDS module.

- **show port capabilities** *[module | module_number]*

  Displays the capabilities of the module and ports.

- **show test**

  Displays the errors reported from the diagnostic tests for both the SPAN port (port 1) and the management port (port 2) and the BIOS and CMOS boot results.

Unsupported Supervisor Engine Commands

These supervisor engine CLI commands are not supported by the IDS module:

- **set module {enable|disable}** *module_number*
- **set port broadcast**
- **set port channel**
- **set port cops**
- **set port disable**

- **set port enable**
- **set port flowcontrol**
- **set port gmrp**
- **set port gvrp**
- **set port host**
- **set port inlinepower**
- **set port jumbo**
- **set port membership**
- **set port negotiation**
- **set port protocol**
- **set port qos**
- **set port rsvp**
- **set port security**
- **set port speed**
- **set port trap**
- **set protocolfilter**
- **set rgmp**
- **set snmp**
- **set spantree**
- **set udld**
- **set vtp**