Summary of Available Commands

IDS version 4.0 supports the following commands.

- C-E
  clear events, page 2-3
  clock set, page 2-4
  configure, page 2-5
  copy, page 2-6
  display-serial, page 2-9
  downgrade, page 2-10
  end, page 2-11
  erase, page 2-12
  exit, page 2-13
- H-M
  hostname, page 2-14
  interface, page 2-20
  ip address, page 2-15
  ip default-gateway, page 2-16
  iplog, page 2-17
  iplog-status, page 2-19
  more, page 2-22

- P-R

- S

clear events

Use the **clear events** command to clear the event store.

clear events

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

Use this command to clear all events from the event store.

This command is IDS specific; there is no related IOS command in versions 12.0 or earlier.

Example

The following command clears the event store.

```
sensor#clear events
Warning: Executing this command will remove all events currently
stored in the event store.
Continue with clear?
sensor#
```

clock set

Use the **clock set** command to manually set the system clock.

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

Syntax Description	
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).

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

Use the **clock set** command to set the time, relative to the configured time zone, if no other timing mechanisms are available. 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.

Example

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

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

configure

Use the **configure** command to enter Global Configuration mode. Global Configuration commands apply to features that affect the system as a whole rather than affecting just one protocol or interface.

configure terminal

Syntax Description

terminal—Executes configuration commands from the terminal.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **configure terminal** command places the user in Global Configuration mode.

Example

```
sensor#configure terminal
sensor(config)#
```

copy

Use the **copy** command to copy iplogs and configuration files.

copy [/erase]*source-url destination-url*

copy iplog *log-id destination-url*

Syntax Description	
/erase	(Optional) Erases the destination file before copying. This keyword only applies to local destinations. It is ignored for remote destinations.
source-url	The location of the source file to be copied. May be a URL or keyword.
destination-url	The location of the destination file to be copied. May be a URL or keyword.
log-id	Log id of file to copy. The log-id can be retrieved using the iplog-status command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator (Copy iplog only)
- Viewer (Copy iplog only)

Usage Guidelines

The exact format of the source and destination URLs varies according to the file. Valid formats are listed in the following table.

Prefix	Source or Destination
ftp:	Source 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:	Source or destination URL for the Secure Copy Protocol (SCP) network server. The syntax for this prefix is scp:[//[username@]location]/directory]/filename or scp:[//[username@]location]//absoluteDirectory]/filename

Keywords are used to designate the file location on the sensor. The following keywords are supported.

Keyword	Source or Destination
archive	A tar file containing the current configuration in XML file format. After copying the archived configuration, the sensor must be rebooted before the change will take effect.
current-config	The current running configuration. This configuration, unlike IOS version 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
backup-config	Storage location for configuration backup. The file format is CLI commands.
iplog	An iplog contained on the system. The IP logs are retrieved based on log-id. See the **iplog-status** command output. IP logs are stored in binary and will be displayed with a log viewer.

If ftp or scp is the selected protocol, the user will be prompted for a password. If no password is necessary for the ftp session, the user can return without entering anything.

The current-config and backup-config are stored as service commands where possible.

You can enter on the command line all necessary source and destination URL information and the username or you can enter **copy** and have the sensor prompt you for any missing information.

The IOS 12.0 **copy** command is more flexible and allows copying between different destinations.

Example

The following example would copy a file into the current configuration from the machine with the IP address 10.1.1.1, directory/filename /configuration/cfg.

```
sensor#copy scp://csidsuser@10.1.1.1/configuration/cfg current-config
password: *******
csiduser@10.1.1.1's password:
archive.tar 100%
|*************|64257
00:00

Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [Yes]:no
sensor#
```

Related Commands

iplog-status

more

display-serial

Use the **display-serial** command to direct all output to the serial connection. Use the **no display-serial** command to reset the output to the local terminal.

display-serial

no display-serial

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator

Usage Guidelines

The **display-serial** command allows the user to view system messages on a remote console (using the serial port) during the boot process. The local console will not be available as long as this option is enabled. Without this option set, a user connected to the serial port will not get any feedback until Linux has fully booted and enabled support for the serial connection. The default configuration is **no display-serial**.

Example

The following command will re-direct output to the serial port.

```
sensor(config)#display-serial
sensor(config)#
```

downgrade

Use the **downgrade** command to remove the most recent upgrade.

downgrade

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

None.

Example

The following command will remove the most recent upgrade from the system:

```
sensor#downgrade

Warning: Executing this command will reboot the system and downgrade
to IDS-K9-sp-4.0-2-S29.rpm. Configuration changes made since the last
upgrade will be lost and the system may be rebooted.
Continue with downgrade?:yes
sensor#
```

If the **downgrade** command is not available, for example, if no upgrades have been applied, the following is displayed:

```
sensor#downgrade
Error: No downgrade available
sensor#
```

end

Use the **end** command to exit a configuration mode or any submode.

end

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

All modes except the Generic Configuration Schema-Based Commands submodes.

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **end** command exits to the top-level Exec menu.

Example

```
sensor#configure terminal
sensor(config)#interface sensing0/0sensor(config-if)#end
sensor#
```

erase

Use the **erase** command to delete a logical file.

erase{ backup-config | current-config }

Syntax Description	
current-config	The current running configuration. This configuration, unlike IOS version 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
backup-config	Storage location for configuration backup. The file format is CLI commands.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator

Usage Guidelines

The IOS 12.0 version of the **erase** command allows the user to remove entire file systems. This concept is not supported in IDS.

Example

The following example erases the current configuration file and returns all settings to default. This command may need to reboot the sensor.

```
sensor#erase current-config

WARNING: Removing the current-config file will result in all
configuration being reset to default, including system information
such as IP address.
Continue?:Yes
sensor#
```

exit

Use the **exit** command to exit a configuration mode or close an active terminal session and terminate the Exec.

exit

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

All modes.

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **exit** command is used to return to the previous menu level.

Example

```
sensor#configure terminal
sensor(config)#interface command-control
sensor(config-if)#exit
sensor(config)#
```

hostname

Use the **hostname** command to set the hostname for a sensor.

hostname *name*

Syntax Description

Syntax Description	
name	Case-sensitive character string, up to 256 characters. Number, "_", and "-" are valid, spaces are not accepted.

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

None.

Example

```
sensor(config)#hostname bldg-3
sensor(config)#
```

ip address

Use the **ip address** command to set the IP address for the command and control interface.

ip address *ip-address mask*

Syntax Description	
ip-address	IP address. See the **setup** command for parameter details. Defaults to 10.1.9.201.
mask	Subnet mask. See the **setup** command for parameter details. Defaults to 255.255.255.0

Command Modes

Interface Command-Control Configuration

Supported User Roles

Administrator

Usage Guidelines

The **ip address** command is used to modify the command and control interface IP address.

IOS 12.0 allows for a secondary IP address to be configured on the interface and also allows the no form of this command to remove the IP address from the interface. IDS does not allow these options. All configuration except user accounts can be cleared using the **erase current-config** command.

Changing the IP address of the command and control interface may result in the sensor being rebooted.

Example

```
sensor(config-if)#ip address 10.1.2.1 255.255.255.0
sensor(config-if)#
```

ip default-gateway

Use the **ip default-gateway** command to define a default gateway for the command and control interface.

ip default-gateway *ip-address*

Syntax Description	
ip-address	Router IP address. Defaults to 10.1.9.1

Command Modes

Interface Command-control Configuration

Supported User Roles

Administrator

Usage Guidelines

Changing the default gateway of the command and control interface may result in the sensor being rebooted.

IOS 12.0 allows the no form of this command to remove the default-gateway configuration from the interface. IDS does not allow this option. All configuration except user accounts can be cleared using the **erase current-config** command.

Example

```
sensor(config-if)#ip default-gateway 10.1.1.1
sensor(config-if)#
```

iplog

Use the **iplog** command to start IP logging on an interface group. Use the no form of this command to disable one or all IP logging sessions.

iplog *group-id ip-address*[**duration** *minutes*][**packets** *numPackets*] [**bytes** *numBytes*]

no iplog*log-id* | *group-id*

no iplog

Syntax Description	
group-id	Group ID to begin/end logging on.
ip-address	Only log packets containing the specified IP address. See the **setup** command for parameter details.
minutes	Duration the logging should be active, in minutes. Defaults to 10 minutes.
numPackets	Total number of packets to log. Defaults to 1000 packets.

Syntax Description	
numBytes	Total 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.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator

Usage Guidelines

The **iplog** command does not exist in IOS 12.0.

If the no form of this command is specified without parameters, all logging will be stopped on the interface.

If duration, packets, and bytes are entered, logging will terminate whenever the first event occurs.

Example

The following example will begin logging all packets containing 10.2.3.1 in the source or destination address on interface group 0.

```
sensor#iplog 1 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#
```

Related Commands

iplog-status

iplog-status

Use the **iplog-status** command to display a description of the available IP log contents.

iplog-status

Syntax Description

There are no keywords or parameters associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **iplog-status** command does not exist in IOS 12.0.

Example

```
sensor#iplog-status

Group:0
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:0
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#
```

Related Commands

iplog

interface

Use the **interface** command to enter the appropriate interface configuration mode for an interface.

interface command-control

interface sensing *name*

interface group *number*

Syntax Description	
name	Sensing interface name. The interface name is a logical name ‘int’ followed by a number (0–7). For example, int0, int1.
number	Logical number for interface group. Valid values are 0–7.

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator

Note The Operator user role is supported for the interface group command.

Usage Guidelines

There is only one command and control port. Use the **command-control** command to enter configuration mode for the command and control interface.

Use the **sensing** command to enter configuration mode for a sniffing interface.

An interface group provides a way to group sensing interfaces into one logical virtual sensor. Currently, only one interface group, 0, is supported. The sensing interfaces are auto-detected and, by default, the most reasonable interface is assigned to the interface group as the sensing interface. Only one interface may be assigned to the interface group at any given time. Use the **group** command to enter configuration mode for the interface group.

Example

The following command enters the Interface Command-Control Configuration submode:

```
sensor(config)#interface command-control
sensor(config-if)#
```

The following command enters the interface group configuration submode:

```
sensor(config)#interface group 0
sensor(config-ifg)#
```

The following command enters the interface sensing configuration submode:

```
sensor(config)#interface sensing int0
sensor(config-ifs)#
```

more

Use the **more** command to display the contents of a logical file.

more *keyword*

Syntax Description	
current-config	The current running configuration. This configuration, unlike IOS version 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
backup-config	Storage location for configuration backup. The file format is CLI commands.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator (current-config only)
- Viewer (current-config only)

Usage Guidelines

The IOS 12.0 version of the **more** command allows the user to display the contents of files stored on various partitions in the device. The IDS **more** command only allows display of logical files.

The current-config and backup-config are stored as token value pairs as read from the .xml file. The output is the same as the commands that would be entered in the Generic Configuration Schema-Based Commands modes.

Example

```
sensor#more current-config

!
!Current Configuration last modified Mon Sep 18 10:23:29 2000
!
service host
general
default-gateway 172.21.172.1
hostname sensor
ip-address 172.21.172.25
netmask 255.255.255.0
exit
exit
```

password

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

password

password[*name*[*newPassword*]]

Syntax Description	
name	Specifies the username. A valid username is 1-32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).
password	The password is requested when the user enters this command. A password can be any printable character, including spaces. A valid password is 6-32 characters long.

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator
- Viewer

Note The Operator and Viewer roles can modify the password for the current user.

Usage Guidelines

Use the **password** command to update the login password for the current user. The administrator may also use this command to modify the password for an existing user. The administrator will not be prompted for the current password in this case.

The IOS 12.0 password command allows the user to enter the new password in the clear on the password line. This command has been modified for IDS so that the password is protected.

Example

The following example shows how to modify the password for the current user:

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

The following example modifies the password for the user “tester”. This command may only be executed by an administrator:

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

ping

Use the **ping** command to diagnose basic network connectivity.

ping*address*[*count*]

Syntax Description	
address	IP address of system to ping.
count	Number of echo requests to send. If no value is entered, 4 requests will be sent. Valid range is 1-10000.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

No command interrupt is available for the **ping** command. The command must run to completion.

This command is implemented using the ping command provided by the operating system. The output from the command varies slightly between operating systems.

Example

```
sensor#ping 10.1.1.2

PING 10.1.1.1 from 10.1.1.2: 32(60) bytes of data.
40 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=0.2 ms
40 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.2 ms

--10.1.1.1 ping statistics--
```

```
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms

sensor#
```

The following example shows the output for an unreachable address:

```
sensor#ping 172.21.172.1
PING 172.21.172.1 (172.21.172.1) from 10.89.175.50 : 56(84) bytes of
data.

--172.21.172.1 ping statistics--
5 packets transmitted, 0 packets received, 100% packet loss

sensor#
```

privilege

Use the **privilege** command to modify the privilege level for an existing user. The privilege may also be specified during user creation with the username command.

privilege user*name*[administrator | operator | viewer]

Syntax Description	
name	Specifies the username. A valid username is 1-32 characters long. Acceptable characters are alphanumerical, dash (-), and underscore (_).

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

Use the **privilege** command to modify the privilege for a user. There is no similar command in IOS version 12.0.

Example

The following example changes the privilege for user “tester” to operator.

```
sensor(config)#privilege user tester operator
Warning: The privilege change does not apply to current CLI sessions.
It will be applied to subsequent logins.
sensor(config)#
```

recover

The **recover** command reimages the application partition with the application image stored on the recovery partition. The sensor is rebooted multiple times and all configuration except for network parameters is reset to default.

recover application-partition Example sensor(config)#

Syntax Description	
application-partition	Reimages the application partition.

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

Valid answers to the continue with recover question are **yes** or **no**. **Y** or **N** are not valid responses.

Shutdown begins immediately after the command is executed. Because shutdown may take a little time, the user may continue to access CLI commands (access is not denied) but will be terminated without warning. If necessary, a period (.) will be displayed on the screen once a second to indicate progress while the applications are shutting down.

There is no related IOS command in versions 12.0 or earlier.

Example

```
sensor(config)#recover application-partition

Warning: Executing this command will stop all applications and
re-image the node to version 4.0(1)S29. All configuration changes
except for network settings will be reset to default.

Continue with recovery?:yes

Request Succeeded

sensor(config)#
```

remove-xl

Use the **remove-xl** command to indicate that the hardware accelerator card has been removed from the device.

remove-xl

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

The **remove-xl** command is IDS specific; there is no related IOS command in versions 12.0 or earlier.

Example

The following example specifies that the hardware accelerator card has been removed from the system.

```
sensor#remove-xl
sensor#
```

reset

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

reset [powerdown]

Syntax Description	
powerdown	This option causes the sensor to power off after the applications are shutdown.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

Valid answers to the continue with reset question are **yes** or **no**. **Y** or **N** are not valid responses.

Shutdown begins immediately after the command is executed. Because shutdown may take a little time, the user may continue to access CLI commands (access is not denied) but will be terminated without warning. If necessary, a period (.) will be displayed on the screen once a second to indicate progress while the applications are shutting down.

There is no similar command in IOS 12.0 or earlier.

Example

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

reset-signatures

Use the **reset-signatures** command to reset standard signature settings back to the default configuration. If no arguments are entered, all signatures for all engines will be reset to the default values. This command does not modify custom signatures. To reset a configuration completely back to default, create a virtual sensor configuration file using the **virtual-sensor-configuration** command and use the **virtual-sensor** command to assign it to the interface group.

reset-signatures{*ATOMIC.ARP* | *ATOMIC.ICMP* | *ATOMIC.IPOPTIONS* | *ATOMIC.L3.IP* | *ATOMIC.TCP* | *ATOMIC.UDP* | *FLOOD.HOST.ICMP* | *FLOOD.HOST.UDP* | *FLOOD.NET* | *OTHER* | *SERVICE.CISCOLOGIN* | *SERVICE.DNS* | *SERVIC.FTP* | *SERVICE.GENERIC* | *SERVICE.HTTP* | *SERVICE.IDENT* | *SERVICE.NTP* | *SERVICE.RPC* | *SERVICE.SMB* | *SERVICE.SMTP* | *SERVICE.SNMP* | *SERVICE.SSH* | *SERVICE.SYSLOG* | *STATE.STRING.LPRFORMATSTRING* | *STRING.ICMP* | *STRING.TCP* | *STRING.UDP* | *SWEEP.HOST.ICMP* | *SWEEP.HOST.TCP* | *SWEEP.MULTI* | *SWEEP.OTHER.TCP* | *SWEEP.PORT.UDP* | *TRAFFIC.ICMP* | *TROJAN.BO2K* | *TROJAN.TFN2K* | *TROJAN.UDP*} {**all** |*comma-separated-signature-list*}]

Syntax Description	
all	Resets all signatures for the specified micro engine back to default settings.
comma-separated-signature-list	Resets specified signatures back to default settings. The list may include ranges and wildcards. If a signature has sub-sig Ids, all sub-sigs for the signature will be reset to default also. This only applies to standard signatures, 0–19999.

Command Modes

Virtual Sensor Configuration

Supported User Roles

- Administrator
- Operator

Usage Guidelines

Non-existent signatures within an entered range are ignored. The request will still succeed for all existing signatures.

This command is IDS specific; there is no related IOS command in versions 12.0 or earlier.

Example

The following example resets all signatures on sensing 1 back to default settings.

```
sensor(config)#service virtual-sensor-configuration virtualSensor
sensor(config-vsc)#reset-signatures all
sensor(config-vsc)#
```

The following example resets signatures 1101 through 1103 and all 2* level signatures back to default settings.

```
sensor(config-vsc)#reset-signatures atomic-icmp 1101-1103,2*
```

The following example resets all 21* level signatures back to default settings. (2100, 2101, 2102, 2150, and so on).

```
sensor(config-vsc)#reset-signatures atomic-icmp 21*
sensor(config-vsc)#
```

ssh authorized-key

Use the **ssh authorized-key** command to add a public key to the current user for a client allowed to use RSA authentication to log in to the local SSH server. Use the no form of this command to remove an authorized key from the system.

ssh authorized-key *id key-modulus-length public-exponent public-modulus*

no ssh authorized-key *id*

Syntax Description	
id	1–256 character string uniquely identifying the authorized key. Numbers, dash (-), and underscore (_) are valid. Spaces and question marks (?) are not accepted.
key-modulus-length	ASCII decimal integer in the range [511, 2048]

Syntax Description	
public-exponent	ASCII decimal integer in the range [3, 2^32]
public-modulus	ASCII decimal integer, x, such that (2^key-modulus-length) < x< (2^(key-modulus-length +1))

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **ssh authorized-key** command adds an entry to the known hosts table for the current user. To modify a key, first remove the entry and then add the modified key back to the table.

There is no related command in IOS versions 12.0 and earlier.

Example

```
sensor(config)#ssh authorized-key system1 1023 37
66039468023948509328450928345902459O
sensor(config)#
```

ssh generate-key

Use the **ssh generate-key** command to change the server host key used by the secure shell server on the sensor.

ssh generate-key

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

The sensor must be rebooted for the changes to take effect. If the remote client is using the Secure Shell Protocol version 1.5, the displayed key fingerprint will match that displayed in the remote secure shell client in future connections with this sensor.

There is no related command in IOS versions 12.0 or earlier.

Example

```
sensor#ssh generate-key
Warning: Executing this command will cause other hosts SSH clients to
stop trusting this host and require approximately 20 seconds to
complete.
Continue? [no]
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble:
xebiz-vykyk-fekuh-ruhuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
sensor#
```

service

Use the **service** command to access the configuration menus for specific node services.

service {alarm-channel-configuration | Authentication | Host | Logger | Network Access | SshKnownHosts | TrustedCertificate | virtual-sensor-configuration | WebServer}

Syntax Description	
alarm-channel-configuration	Refer to the **service alarm-channel-configuration** command for more information.
Authentication	Configure the order of methods that should be used to authenticate users.
Host	Refer to the **service Host** command for more information.
Logger	Refer to the **service Logger** command for more information.
NetworkAccess	Refer to the **service NetworkAccess**command for more information.
SshKnownHosts	Refer to the **service SshKnownHosts**command for more information.
TrustedCertificate	Refer to the **service TrustedCertificate** command for more information.
virtual-sensor-configuration	Refer to the **service virtual-sensor-configuration** command for more information.
WebServer	Refer to the **service WebServer** command for more information.

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator (read only)
- Viewer (ready only)

Usage Guidelines

The **service** command allows the user to configure service-specific parameters. The items and menus in this configuration are service dependent and are built dynamically based on the configuration retrieved from the service when the command is executed. The modifications made in this mode and any submodes are applied to the service when the user exits the service mode.

The command mode is indicated by the command prompt. For example, service host mode is indicated by the prompt `sensor(config-Host)#`.

There is no related command in IOS versions 12.0 or earlier.

Example

The following example demonstrates how to access the service configuration mode for host services:

```
sensor(config)#service host
sensor(config-Host)#?
exit Exit service configuration mode
show Display system settings and/or history information
```

service alarm-channel-configuration

Use the **service alarm-channel-configuration** command to enter Alarm Channel Configuration mode for a logically named alarm channel configuration. Currently, the only logically named configuration allowed is *virtualAlarm*.

service alarm-channel-configuration *name*

Syntax Description	
name	Logical name of the configuration. Currently, only allowed name is *virtualAlarm*.
exit	Exits the current mode or submode.

- **systemVariables**—User modifiable system variables

  IN <VALUE>: Defines the protected network space (Should include ALL protected addresses)
  default IN

  DMZ1 <VALUE>: Defines the DMZ1 network space
  default DMZ1

  DMZ2 <VALUE>: Defines the DMZ2 network space
  default DMZ2

  DMZ3 <VALUE>: Defines the DMZ3 network space
  default DMZ3

  USER-ADDRS1 <VALUE>: User-defined network space
  default USER-ADDRS1

  USER-ADDRS2 <VALUE>: User-defined network space
  default USER-ADDRS2

  USER-ADDRS3 <VALUE>: User-defined network space
  default USER-ADDRS3

  USER-ADDRS4 <VALUE>: User-defined network space
  default USER-ADDRS4

  USER-ADDRS5 <VALUE>: User-defined network space
  default USER-ADDRS5

  SIG1 SIG1: User-defined Signature set
  default SIG1

  SIG2 SIG2: User-defined Signature set
  default SIG2

SIG3 SIG3: User-defined Signature set
default SIG3

SIG4 SIG4: User-defined Signature set
default SIG4

SIG5 SIG5: User-defined Signature set
default SIG5

- **EventFilter**—Configuration for the event filters.

  Filters DestAddrs <VALUE> (default: *) Exception <False,True> (default: False) SIGID <0-2147483647> (default: *) SourceAddrs <VALUE> (default: *) SubSig <0-2147483647> (default: *)
  Filters: Defines the filter rules [
  DestAddrs: Source Addresses of events to which this filter should be applied.
  Exception: Does this filter describe an exception to an event filter? This allows creating 'General Case' exclusions and then adding more specific inclusions.
  SIGID: Signature IDs of events to which this filter should be applied.
  SourceAddrs: Source addresses of events to which this filter should be applied.
  SubSig: SubSigID's of events to which this filter should be applied.

  no Filters DestAddrs <VALUE> (default: *) Exception <False,True> (default: False) SIGID <0-2147483647> (default: *) SourceAddrs <VALUE> (default: *) SubSig <0-2147483647> (default: *): Removes a filter rule entry or selection setting
  DestAddrs: Source addresses of events to which this filter should be applied.
  Exception: Does this filter describe an exception to an event filter? This allows creating 'General Case' exclusions and then adding more specific inclusions.
  SIGID: Signature IDs of events to which this filter should be applied.
  SourceAddrs: Source addresses of events to which this filter should be applied.
  SubSig: SubSigIDs of events to which this filter should be applied.

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **service alarm-channel-configuration** command places the user into Alarm Channel Configuration mode. The items and menus in this mode are service dependent and are built dynamically based on the configuration retrieved from the service when the command is executed. The modifications made in this mode are applied to the analysis engine when the user exits the configuration mode. A configuration can only be deleted if it is not currently associated with an interface group. There is no related command in IOS versions 12.0 or earlier.

Example

The following command enters the basic alarm-channel configuration menu.

```
sensor(config)#service alarm-channel-configuration virtualAlarm
sensor(config-acc)#
```

service Host

Use the **service Host** command to configure the host parameters, such as system clock settings, upgrades, and IP access list.

service Host

Syntax Description	
exit	Exits the current mode or submode.
show settings	**show**: Displays current mode settings. **settings**: Displays configuration contents for the current and children submodes.

- **networkParams**—Network configuration parameters. Valid parameters include the following:

  default ipAddress: Sets the Command and Control interface IP address back to the system default setting.

  networkParams netmask <value>: Command and Control interface netmask (default is 255.255.255.255)

  default netmask: Sets the netmask for the Command and Control interface back to the system default setting.

  networkParams defaultGateway <value>: Command and Control interface default gateway

  default defaultGateway: Sets the default gateway for the Command and Control interface back to the system default setting.

  networkParams telnetOption <enable,disable>: Option for disabling or enabling Telnet service

  default telnetOption: Sets the Telnet service option back to the system default setting.

  networkParams hostname <value>: Sensor hostname.

  default hostname: Sets the sensor hostname back to the system default setting.

  networkParams accessList ipAddress <value> netmask <value>: List of trusted hosts.

  no accessList ipAddress <value> netmask <value>: Removes an entry from accessList table.

- **timeParams**—Time configuration parameters. Valid parameters include the following:

  standardTimeZoneName <standardTimeZoneName> : Descriptive name for standard time.

  recurringParams: Recurring timezone parameters.

  nonRecurringParams: Non-recurring timezone parameters.

summerTimeParams: Summertime parameters.
summerTimeZoneName <summerTimeZoneName> : Descriptive name for summer time.
startSummerTime: Start of summer time.
monthOfYear <jan,feb,mar,apr,may,jun,jul,aug,sep,oct,nov,dec> : Month of year.
weekOfMonth <first,second,third,fourth,fifth,last> : Week of month.
dayOfWeek <sun,mon,tue,wed,thu,fri,sat> : Day of week.
timeOfDay hh:mm[:ss]: Time of day.

no summerTimeParams: Removes summerTimeParams contents.

endSummerTime: Sets the monthOfYear, weekOfMonth, dayOfWeek, and timeOfDay to end summer time.

summerTimeZoneName <summerTimeZoneName>: Descriptive name for summer time.
startSummerTime: Start of summer time.
date YYYY-MM-DD: date
time hh:mm[:ss]: Time of day.

- Default time commands:
  default monthOfYear: Sets the month of year back to the system default setting.
  default weekOfMonth: Sets the week of month back to the system default setting.
  default dayOfWeek: Sets the day of week back to the system default setting.
  default timeOfDay: Sets the time of day back to the system default setting.
  default offset: Sets the offset back to the system default setting.
  default summerTimeZoneName: Sets the descriptive name for summer time back to the system default setting.
  default date: Sets the date back to the system default setting.
  default time: Sets the time of day back to the system default setting.
  default keyId: Sets the NTP server key id back to the system default setting.
  default keyValue: Sets the NTP server key value back to the system default setting.
  default standardTimeZoneName: Sets the descriptive name for standard time back to the system default setting.

- **ntpServers ipAddress <value>**—Defines NTP servers. If no NTP server is defined, the system clock will be used.

  keyId <keyId>: NTP server key id.

  keyValue <keyValue>: NTP server key value.

  no ntpServers ipAddress <value>: Removes an entry from ntpServers table.
- **active-selection <recurringParams,nonRecurringParams,none>**—Indicates active selection for the current mode.

service Logger

Configure debug levels. Valid parameters include:

- **exit**—Exit service configuration mode.
- **show settings**—**show**: Display current mode settings.

  settings: Display configuration contents for the current and children submodes.
- **masterControl**—Allows overall control of logApp.
- **enable-debug <false,true>**—Enables debug logging, for all zones, to the log file.
- **default enable-debug**—Set the debug logging setting back to the system default setting.

service NetworkAccess

Configure parameters relating to network access controller. Valid parameters include:

- **exit**—Exit service configuration mode.
- **show settings**—**show**: Display current mode settings.

  settings: Display configuration contents for the current and children submodes.
- **general**—General NAC configuration.

- **enable-acl-logging <false,true>**—Flag indicating if ACL logging should be enabled.

  default enable-acl-logging: Sets enable-acl-logging back to the system default setting.

- **allow-sensor-shun <false,true>**—Flag indicating if CIDS IP can be shunned.

  default allow-sensor-shun: Sets the sensor shun parameter back to the system default setting.

- **shun-enable <false,true>**—Flag indicating if shunning should be enabled.

  default shun-enable [default: Set the value back to the system default setting] [shun-enable: Flag indicating if shunning should be enabled.]

- **shun-max-entries <value>**—Maximum number of active shuns.

  default shun-max-entries [default: Set the value back to the system default setting] [shun-max-entries: Maximum number of active shuns.]

- **master-blocking-sensors mbs-ipaddress <value>**—**master-blocking-sensors**: List containing sensors for forwarding shuns.

  mbs-ipaddress: IP address of CIDS for forward shun requests.

  no master-blocking-sensors mbs-ipaddress <value>: Remove an IP address from master-blocking-sensors table.

- **mbs-password**—Account password of CIDS for forward shun requests.

  default mbs-password: Sets the account password back to the system default setting.

- **mbs-port <mbs-port>**—Port of CIDS for forward shun requests.

  default mbs-port: Sets the port back to the system default setting.

- **mbs-tls <false,true>**—IP address of CIDS for forward shun requests.

  default mbs-tls: Sets the IP address back to the system default setting.

- **mbs-username <mbs-username>**—Account name of CIDS for forward shun requests.

  default mbs-username: Sets the account name back to the system default setting.

- **never-shun-hosts ip-address <value>—never-shun-hosts**: List specifying never shun host parameters.

  ip-address: IP address of device that should never be shunned.

  no never-shun-hosts ip-address A.B.C.D: Removes an entry from never-shun-hosts table.

- **never-shun-networks ip-address <value> netmask <value>—never-shun-networks**: List specifying never shun network parameters.

  ip-address: IP address of network that should never be shunned.

  netmask: Netmask of network that should never be shunned.

  no never-shun-networks ip-address <value> netmask <value>: Removes an entry from never-shun-networks table.

- **shun-hosts ip-address <value>—shun-hosts**: List specifying shunned hosts.

  ip-address: Source IP address of device to shun.

  no shun-hosts ip-address <value> : Removes an entry from shun-hosts table.

- **dest-ip-address <value>**—Destination IP address to shun.

  default dest-ip-address: Sets the destination IP address back to the system default setting.

- **dest-port <value>**—Destination port of device to shun. The dest-ip-address must be present.

  default dest-port: Sets the destination port back to the system default setting.

- **protocol <tcp,udp>**—Specify IP protocol. The dest-ip-address must be present.

  default protocol: Sets the protocol back to the system default setting.

- **source-port <value>**—Source port of device to shun. The dest-ip-address must be present.

  default source-port: Sets the source port back to the system default setting.

- **shun-networks ip-address <value> netmask <value>—shun-networks**: List specifying shunned networks.
  ip-address: IP address of network to shun.
  netmask: Netmask of network to shun.

no shun-networks ip-address <value> netmask <value>: Removes an entry from shun-networks table.

- **shun-device-cfg name <name>—shun-device-cfg**: Settings for device access.
  name: Logical name of general device configuration to use for this device.

  enable-password : Enable password for device.

  default enable-password: Sets the enable password back to the system default setting.

  password: Password for the initial router login.

  default password: Sets the password for the initial router login back to the system default setting.

  username <username>: TACACS+ username for account on device.

  default username: Sets the username back to the system default setting.

- **cat6k-devices ip-address <value>—cat6k-devices**: Settings for CAT 6K routers controlled by NAC.
  ip-address: IP address of the managed device.

  no cat6k-devices ip-address <value>: Removes an entry from cat6k-devices table.

  communication <ssh-des,ssh-3des,telnet>: Indicates the method used to access the box. If unspecified, SSH 3DES will be used.

  default communication: Sets the access method back to the system default setting.

  nat-address <value>: CIDS NAT address.

  default nat-address: Sets the NAT address back to the system default setting.

  shun-device-cfg <shun-device-cfg>: Logical name of general device configuration to use for this device.

  default shun-device-cfg: Sets the general device configuration back to the system default setting.

  post-vacl-name <post-vacl-name>: Name of VACL manually programmed on the device.

  default post-vacl-name: Sets the post VACL name back to the system default setting.

pre-vacl-name <pre-vacl-name>: Name of VACL manually programmed on the device.

default pre-vacl-name: Sets the pre-VACL name back to the system default setting.

shun-interfaces vlan <1-65535>
shun-interfaces: List containing interface names.
vlan: VLAN number used by the device.

no shun-interfaces vlan <1-65535>: Removes an entry from shun-interfaces table.

- **router-devices ip-address <value>—router-devices**: Settings for routers controlled by NAC.
  ip-address: IP address of the managed device.

  no router-devices ip-address <value>: Removes an entry from router-devices table.

  communication <ssh-des,ssh-3des,telnet> : Indicates the method used to access the box. If unspecified, SSH 3DES will be used.

  default communication: Sets the access method back to the system default setting.

  nat-address <value>: CIDS NAT address.

  default nat-address: Sets the NAT address back to the system default setting.

  shun-device-cfg <shun-device-cfg>: Logical name of general device configuration to use for this device.

  default shun-device-cfg: Sets the general device configuration back to the system default setting.

  shun-interfaces direction <out,in> interface-name <interface-name>
  shun-interfaces: List containing interface names and directions.
  direction: Direction to shun.
  interface-name: Interface name used by the router.

  no shun-interfaces direction <out,in> interface-name <interface-name>: Removes an entry from shun-interfaces table.

  post-acl-name <post-acl-name>: Name of ACL manually programmed on the device.

  default post-acl-name: Sets the post ACL name back to the system default setting.

pre-acl-name <pre-acl-name>: Name of ACL manually programmed on the device.

default pre-acl-name: Sets the pre-ACL name back to the system default setting.

- **pix-devices ip-address <value>—pix-devices**: Settings for the PIX Firewalls controlled by NAC
  ip-address: IP address of the managed device.

  no pix-devices ip-address <value>: Removes an entry from pix-devices table.

  communication <ssh-des,ssh-3des,telnet>: Indicates the method used to access the box. If unspecified, SSH 3DES will be used.

  default communication: Sets the access method back to the system default setting.

  nat-address <value>: CIDS NAT address.

  default nat-address: Sets the NAT address back to the system default setting.

  shun-device-cfg <shun-device-cfg>: Logical name of general device configuration to use for this device.

  default shun-device-cfg: Sets the general device configuration back to the system default setting.

  no shun-device-cfg name <name>: Removes an entry from shun-device-cfg table.

service SshKnownHosts

Configure the known-hosts keys for the system.

- **exit**—Exit service configuration mode.
- **show settings—show**: Display current mode settings.

  settings: Display configuration contents for current and children submodes.
- **rsa1Keys id <value>—rsa1Keys**: The list of known hosts with which this sensor will connect using SSH protocol version 1.5.
  id: IP address of the remote host.

  no rsa1Keys id <value>: Removes an entry from rsa1Keys table.

- **exponent exponent [exponent: Remote host's SSH protocol version 1.5 RSA public key exponent]**—

  default exponent [default: Set the value back to the system default setting] [exponent: Remote host's SSH protocol version 1.5 RSA public key exponent]

- **length <length>**—Remote host's SSH protocol version 1.5 RSA public key modulus length.

  default length: Sets the key modulus length back to the system default setting.

- **modulus <modulus>**—: Remote host's SSH protocol version 1.5 RSA public key modulus.

  default modulus: Sets the public key modulus back to the system default setting.

service TrustedCertificates

Configure list of X.509 certificates for trusted certificate authorities.

- **exit**—Exit service configuration mode.
- **show settings**—**show**: Display current mode settings.

  settings: Display configuration contents for current and children submodes.

- **trustedCertificates commonName <commonName>**—**trustedCertificates**: The list of X.509 host certificates that this sensor will trust when it connects using TLS or SSL.
  commonName: The certificate subject's common name. For host certificates, this field should contain the hostname or dotted-decimal IP address of the trusted host. This field is never accessed by the sensor software. It is provided to aid the user in identifying the certificate with which it is associated.

no trustedCertificates commonName <commonName>: Removes an entry from trustedCertificates table.

- **certificate <certificate>**—Base64 encoded ASN.1 DER representation of the X.509 host certificate.

  default certificate: Sets the value back to the system default setting.

service virtual-sensor-configuration

Use the **service virtual-sensor-configuration** command to enter the configuration mode for a logically named virtual sensor. Currently, the only logically named configuration allowed is *virtualSensor.*

service virtual-sensor-configuration*name*

Syntax Description	
name	Logical name of the configuration. The only allowed name is *virtualSensor.*
exit	Exits the current mode or submode.
show settings	**show**: Displays current mode settings. **settings**: Displays configuration contents for current and children submodes.

- **systemVariables**—User modifiable system variables.

  WEBPORTS WEBPORTS: Defines the ports associated with the web service.

  default WEBPORTS: Sets the ports associated with the web service back to the system default setting.

  Ports1 Ports1: User defined.

  default Ports1: Sets the value back to the system default setting.

Ports2 Ports2: User defined.

default Ports2: Sets the value back to the system default setting.

Ports3 Ports3: User defined.

default Ports3: Sets the value back to the system default setting.

Ports4 Ports4: User defined.

default Ports4: Sets the value back to the system default setting.

ADDRS1 <VALUE>: Defines a set of IpAddress Ranges.

default ADDRS1: Sets the IpAddress Range back to the system default setting.

ADDRS2 <VALUE>: Defines a set of IpAddress Ranges.

default ADDRS2: Sets the IpAddress Range back to the system default setting.

ADDRS3 <VALUE>: Defines a set of IpAddress Ranges.

default ADDRS3: Sets the IpAddress Range back to the system default setting.

ADDRS4 <VALUE>: Defines a set of IpAddress Ranges.

default ADDRS4: Sets the IpAddress Range back to the system default setting.

- **FragmentReassembly**—Fragment Reassembly configuration tokens.

  IPReassembleMode <NT,Solaris,Linux,BSD>: How to reassemble fragments.

  default IPReassembleMode: Sets the fragment reassembly method back to the system default setting.

  IPReassembleTimeout IPReassembleTimeout: Caching time for incomplete fragments.

  default IPReassembleTimeout: Sets the caching time back to the system default setting.

- **StreamReassembly**—Stream Reassembly configuration tokens.

  TCP3WayHandshakeRequired <False,True>: Tracks the TCP 3-way handshake before allowing a stream to be opened.

default TCP3WayHandshakeRequired: Sets the option back to the system default setting.

TCPReassemblyMode <strict,loose>: What method of reassembly to use.

default TCPReassemblyMode: Sets the option back to the system default setting.

TCPOpenEstablishedTimeout TCPOpenEstablishedTimeout: Caching time for quiescent established TCP connections.

default TCPOpenEstablishedTimeout: Sets the caching time back to the system default setting.

TCPEmbryonicTimeout TCPEmbryonicTimeout: Caching time for embryonic TCP connections.

default TCPEmbryonicTimeout: Sets the caching time back to the system default setting.

- **IPLog**—Virtual Sensor IP log configuration tokens.

  NumberOfIPLogFiles NumberOfIPLogFiles: Total number of IP logfiles to maintain on the system.

  default NumberOfIPLogFiles: Sets the total number of IP logfiles to maintain on the system back to the system default.

  MaxOpenIPLogFiles MaxOpenIPLogFiles: The maximum number of concurrently open log files.

  default MaxOpenIPLogFiles: Set the maximum number of concurrently open log files back to the system default setting.

  MaxIPLogFileSize MaxIPLogFileSize: The maximum size of an IP log file in bytes.

  default MaxIPLogFileSize: Sets the maximum size of an IP log file in bytes back to the system default setting.

  IPLogPackets IPLogPackets: The maximum number of packets in a log event (0 implies no limit).

  default IPLogPackets: Sets the maximum number of packets in a log event back to the system default setting.

  IPLogTime IPLogTime: The time duration of the log event in seconds.

  default IPLogTime: Sets the time duration of the log event in seconds back to the system default setting.

IPLogBytes IPLogBytes: The maximum number of bytes in a log event (0 implies no limit).

default IPLogBytes: Sets the maximum number of bytes in a log event back to the system default setting.

- **ShunEvent**—Shun Event configuration tokens.

  ShunTime ShunTime: The time duration of the shun event in minutes.

  default ShunTime: Sets the time duration of the shun event (in minutes) back to the system default setting.

- **ATOMIC.ARP**—

  Layer 2 ARP signatures

  signatures SIGID <994-50000> SubSig <0-2147483647> (default: 0)
  signatures: Layer 2 ARP signatures.
  SIGID: Signature Identifier. 994-19999 valid for default signatures. 20000-50000 valid for user signatures.
  SubSig: Sub-Signature ID. Denotes a specific variant of a signature.

  AlarmInterval AlarmInterval: Special Handling for timed events. Use AlarmInterval Y with MinHits X for X alarms in Y second interval.
  default AlarmInterval

  AlarmSeverity <high,informational,low,medium>: The severity of this alert reported in the alarm.
  default AlarmSeverity

  AlarmThrottle <FireAll,FireOnce,GlobalSummarize,Summarize>: Technique used to limit alarm firings. FireAll sends all alarms. FireOnce sends the firstalarm then deletes the inspector. Summarize sends an IntervalSummary alarm. GlobalSummarize sends a GlobalSummary alarm.
  default AlarmThrottle

  AlarmTraits AlarmTraits: User-defined traits further describing this signature.
  default AlarmTraits

  ArpOperation ArpOperation: What arp op code is this signature interested in?
  default ArpOperation

ChokeThreshold ChokeThreshold: Threshold value of alarms-per-interval to auto-switch AlarmThrottle modes. If ChokeThreshold is defined, the sensor will automatically switch AlarmThrottle modes when a large volume of alarms is seen in the ThrottleInterval.
default ChokeThreshold

Enabled <True,False>: True to Enable the Sig. False to Disable the Sig.
default Enabled

EventAction <log,reset,shunHost,shunConnection,ZERO>: What action(s) to perform when the alarm is fired.
default EventAction

FlipAddr <True,False>: True if address (and ports) Source and Destination are swapped in the alarm message. False for no swap (normal).
default FlipAddr

MacFlip MacFlip: Fire when the MAC address changes more than this many times for the IP address?
default MacFlip

MaxInspectLength MaxInspectLength: Maximum number of bytes to inspect.
default MaxInspectLength

MaxTTL MaxTTL: Maximum number of seconds to inspect a logical stream. The inspector is deleted after X seconds of being active.
default MaxTTL

MinHits MinHits: Minimum number of signature hits before the alarm message is sent. This a limiter for firing the alarm only after X times of seeing the signature on the address key.
default MinHits

Protocol <FRAG,IP,TCP,UDP,ICMP,ARP,CROSS,CUSTOM,ZERO>: Protocol of interest for this inspector.
default Protocol

RequestInbalance RequestInbalance: Fire when you have this many more requests than replies on the IP address.
default RequestInbalance

ResetAfterIdle ResetAfterIdle: Number of seconds to wait to reset signature counters after the host(s) were idle.
default ResetAfterIdle

SigComment: USER NOTES - miscellaneous information about this signature.
default SigComment

SigName: Official name of the signature.
default SigName

SigStringInfo: Extra information included in the alarm message.
default SigStringInfo

StorageKey <xxxx,Axxx,xxBx,AxBx,AaBb,Axxb,STREAM,DOUBLE,ZERO>: Type of Address Key used to store persistent data.
default StorageKey

SummaryKey <AaBb,AxBx,Axxb,Axxx,xxBx>: The Storage Type on which to summarize this signature.
default SummaryKey

ThrottleInterval ThrottleInterval: Number of seconds defining an Alarm Throttle interval. This is used with the AlarmThrottle parameter to tune special alarm limiters.
default ThrottleInterval

WantFrag <ANY,False,True>: True if a fragment is desired. False if a fragment is not desired. Any for either.
default WantFrag

wantDstBroadcast <True,False>: Does this signature fire when it sees an ARP dst address of 255.255.255.255 ?]
default wantDstBroadcast

wantSrcBroadcast<True,False>: Does this signature fire when it sees an ARP src address of 255.255.255.255 ?]
default wantSrcBroadcast

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **service virtual-sensor-configuration** command allows the user to access the Virtual Sensor Configuration mode. A configuration can only be deleted if it is not associated with an interface group.

There is no related command in IOS versions 12.0 or earlier.

Example

The following example accesses the configuration menus for the basic virtual sensor configuration.

```
sensor(config)#service virtual-sensor-configuration virtualSensor
sensor(config-vsc)#
```

service WebServer

Configure parameters relating to the web server. Valid parameters include:

- **exit**—Exit Service configuration mode (when in service Webserver submode) or exit general configuration mode (when in configuration mode).
- **show settings**—show: Display current mode settings.

  settings: Display configuration contents for current and children submodes.
- **general**—General cidwebserver configuration.
- **enable-tls**—Determines whether encryption (TLSv1 and SSLv3) is enabled.
- **ports**—List of ports on which the web server listens for connections.
- **server-id**—The value the web server returns in the HTTP Server header.

- **Default commands—default enable-tls**: Sets the encryption (TLSv1 and SSLv3) back to the system default setting.

  default ports: Sets the list of ports on which the web server listens for connections back to the system default setting.

  default server-id: Sets the value the web server returns in the HTTP Server header back to the system default setting.

setup

The **setup** command allows the user to configure the basic sensor settings, including the host name, IP address, netmask, default gateway, Telnet server, and web server port.

setup

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

When you enter the setup command facility, 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 using the setup command facility.

You must run through the entire System Configuration Dialog until you come to the item 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 running through the entire System Configuration Dialog, press **Ctrl-C**.

The facility also provides help text for each prompt. To access help text, enter **?** at a prompt. When you complete your changes, the setup command facility shows you the configuration that was created during the setup session. It also asks you if you want to use this configuration. If you answer Yes, the configuration is saved to disk. If you answer No, the configuration is not saved and the process begins again. There is no default for this prompt; you must answer either Yes or No.

Valid ranges for configurable parameters are as follows:

- **IP Address**—32-bit address written as 4 octets separated by periods. X.X.X.X where X = 0-255.
- **Netmask**—Same boundaries as the IP address definition above. The netmask strips the network ID from the IP address, leaving only the host ID. Each netmask consists of binary ones (decimal 255) to mask the network ID and binary zeroes (decimal 0) to retain the host ID of the IP address. For example, the default netmask setting for a Class B address is 255.255.0.0.
- **Host Name**—Case-sensitive character string, up to 256 characters. Numbers, "_", and "-" are valid; spaces are not accepted.

Example

```
sensor#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 Configuration:
service host
networkParams
hostname sensor
 ipAddress 172.21.172.25
netmask 255.255.255.0
defaultGateway 172.21.172.1
telnetOption enabled
 exit
 exit
!
```

```
service webServer
general
 ports 8080
exit
exit

Current time: Thu Aug 8 09:55:38 2002
 Setup Configuration last modified: Thu Aug 8 09:53:41 2002
Continue with configuration dialog?[yes]:
Enter host name[sensor]:
Enter IP address[172.21.172.25]:
 Enter netmask[255.255.255.0]:
Enter default gateway[172.21.172.1]:
Enter telnet-server status[enabled]:
 Enter web-server port[8080]:80

The following configuration was entered.
 service host
 networkParams
hostname sensor
ipAddress 172.21.172.25
netmask 255.255.255.0
 defaultGateway 172.21.172.1
 telnetOption enabled
exit
exit
 !
 service webServer
 general
ports 80
 exit
exit

Use this configuration?[yes]:
Configuration Saved.
sensor#
```

show clock

Use the **show clock** command to display the system clock.

show clock[detail]

Syntax Description

detail—(Optional) Indicates the clock source (NTP or system) and the current summer-time setting (if any).

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The system clock keeps an authoritative flag that indicates whether the time is authoritative, or believed to be accurate. If the system clock has been set by a timing source such as NTP, the flag is set.

The following symbols describe the flag:

- *****—Time is not authoritative.
- **(blank)**—Time is authoritative.
- **.**—Time is authoritative, but NTP is not synchronized.

Example

```
sensor#show clock
12:30:02 EST Tues Dec 19 2000
Time source is authoritative
sensor#

sensor#show clock
*12:30:02 EST Tues Dec 19 2000
 Time source is not authoritative
sensor#
```

If NTP is configured and synchronized:

```
sensor#show clock detail
12:30:02 CST Tues Dec 19 2000
Time source is NTP
Summer time starts 03:00:00 CDT Sun Apr 7 2003
Summer time ends 01:00:00 CST Sun Oct 27 2003sensor#
```

show events

Use the **show events** command to display the local event log contents.

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

Syntax Description	
alert	Display alerts. Provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis-engine whenever an IDS signature is triggered by network activity. If no level is selected (informational, low, medium, high), all alert events will be displayed.
error	Display error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events will be displayed.

Syntax Description	
log	Display log events. These events are generated whenever a transaction is received and responded to by an application. Contains information about the request, response, and success or failure of the transaction.
NAC	Display Network Access Control requests (shun requests).
status	Display status events.
hh:mm:ss	Start time in hours (military format), minutes and seconds.
day	Start day (by date) in the month.
month	Start month (by name).
year	Start year (no abbreviation).

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

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.

There is no related command in IOS versions 12.0 and earlier.

Example

The following example displays shun requests beginning at 10:00 on December 25, 2000:

```
sensor#show events NAC time 10:00:00 Dec 25 2000
```

The following request displays fatal error messages beginning at the current time:

```
sensor#show events error fatal
```

The following request displays all events beginning at 10:00 on December 25, 2000:

```
sensor#show events 10:00:00 Dec 25 2000
```

The following output is taken from the XML content:

```
evAlert: eventId=1025376040313262350 severity=high
originator:
deviceName: sensor1
appName: sensorApp
time: 2002/07/30 18:24:18 2002/07/30 12:24:18 CST
signature: sigId=4500 subSigId=0 version=1.0 IOS Embedded SNMP
Community Names
 participants:
attack:
attacker: proxy=false
addr: 132.206.27.3

port: 61476
victim:
addr: 132.202.9.254
port: 161
protocol: udp
```

show history

Use the **show history** command to list the commands you have entered in the current menu.

show history

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

All modes

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **show history** command provides a record of the commands you have entered in the current menu. The number of commands that the history buffer will record is 50.

Example

```
sensor#show history
show users
show events
sensor#
```

show interfaces

Use the **show interfaces** command to display statistics for all system interfaces. This command displays **show interfaces command-control**, **show interfaces sensing** and **show interfaces group**.

show interfaces [clear]

Syntax Description	
clear	Clear the diagnostics.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

This command displays statistics for the command-control, sensing interfaces and interface groups. The clear option will also clear statistics that may be reset.

Example

```
sensor# show int
command-control is up
 Internet address is 10.89.147.31, subnet mask is 255.255.255.128,
telnet is disabled.
 Hardware is eth1, tx
 Network Statistics
 eth1 Link encap:Ethernet HWaddr 00:06:5B:0F:0E:53
 inet addr:10.89.147.31 Bcast:10.89.147.127 Mask:255.255.255.128
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:49703 errors:5454 dropped:0 overruns:0 frame:5454
TX packets:22928 errors:0 dropped:0 overruns:0 carrier:0
collisions:1913 txqueuelen:100
RX bytes:17140400 (16.3 Mb) TX bytes:11013743 (10.5 Mb)
Interrupt:16 Base address:0xdcc0 Memory:feb20000-feb40000
Group 0 is up
Sensing ports int1
Logical virtual sensor configuration: virtualSensor
Logical alarm channel configuration: virtualAlarm
VirtualSensor0
General Statistics for this Virtual Sensor
 Number of seconds since a reset of the statistics = 8259
Total number of packets processed since reset = 72599
 Total number of IP packets processed since reset = 65659
Total number of packets that were not IP processed since reset = 6940
 Total number of TCP packets processed since reset = 62176
 Total number of UDP packets processed since reset = 3364
Total number of ICMP packets processed since reset = 119
```

```
Total number of packets that were not TCP, UDP, or ICMP processed
since reset = 0
 Total number of ARP packets processed since reset = 331
Total number of ISL encapsulated packets processed since reset = 275
Total number of 802.1q encapsulated packets processed since reset = 0
 Total number of packets with bad IP checksums processed since reset =
0
Total number of packets with bad layer 4 checksums processed since
reset = 0
 Total number of bytes processed since reset = 27794157
 The rate of packets per second since reset = 8
The rate of bytes per second since reset = 3365
The average bytes per packet since reset = 382
 Statistics for the TCP Stream Reassembly Unit
The current number of established TCP steams. (can not be reset) = 1
 The current number of embryonic TCP steams. (can not be reset) = 0
The current number of closing TCP steams. (can not be reset) = 0
TCP streams that have been tracked since last reset = 293
TCP packets that arrived out of order for their stream. = 0
TCP Packets that caused a stream to jump over a gap in sequence. = 0
 TCP Packet currently queued for reassembly = 0
The rate of TCP connections tracked per second since reset = 0
 The Signature Database Statistics.
The Number of each type of node active in the system (can not be
reset)
Total nodes active = 58
TCP nodes keyed on both IP addresses and both ports = 2
UDP nodes keyed on both IP addresses and both ports = 1
IP nodes keyed on both IP addresses = 11
The number of each type of node inserted since reset Total nodes
inserted = 3053
TCP nodes keyed on both IP addresses and both ports = 269
UDP nodes keyed on both IP addresses and both ports = 251
IP nodes keyed on both IP addresses = 445
The rate of nodes per second for each time since reset Nodes per
second = 0
TCP nodes keyed on both IP addresses and both ports per second = 0
 UDP nodes keyed on both IP addresses and both ports per second = 0
IP nodes keyed on both IP addresses per second = 0
Sensing int0 is up
Hardware is eth0, TX
Reset port
 Sensing int1 is up
Hardware is eth1, TX
Reset port
Command control port
 MAC statistics from the IntelPro interface Link = up
 Speed = 100
```

```
 Duplex = Half
 State = up
Rx_Packets = 49703
Tx_Packets = 22928
 Rx_Bytes = 17140400
Tx_Bytes = 11013743
 Rx_Errors = 5454
 Tx_Errors = 0
 Rx_Dropped = 0
Tx_Dropped = 0
Multicast = 4957
Collisions = 1913
 Rx_Length_Errors = 5454
Rx_Over_Errors = 0
 Rx_CRC_Errors = 0
 Rx_Frame_Errors = 0
 Rx_FIFO_Errors = 0
Rx_Missed_Errors = 0
Tx_Aborted_Errors = 0
Tx_Carrier_Errors = 0
 Tx_FIFO_Errors = 0
 Tx_Heartbeat_Errors = 0
 Tx_Window_Errors = 0
 Tx_Abort_Late_Coll = 0
Tx_Deferred_Ok = 76 Tx_Single_Coll_Ok = 1261 Tx_Multi_Coll_Ok = 285
 Rx_Long_Length_Errors = 0
Rx_Short_Length_Errors = 0
 Rx_Align_Errors = 0
 Rx_Flow_Control_XON = 0
Rx_Flow_Control_XOFF = 0
 Tx_Flow_Control_XON = 0
Tx_Flow_Control_XOFF = 0
 Rx_CSum_Offload_Good = 41864
Rx_CSum_Offload_Errors = 0
PHY_Media_Type = Copper
 Packets dropped by PCAP ring = 0
Sensing int2 is down
 Hardware is falcon1, XL
```

show interfaces command-control

Use the **show interfaces command-control** command to display information about the command and control interface.

show interfaces command-control

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **show interfaces command-control** command contains information about the command and control interface and the system in general. The first line indicates if the interface is up or down. For IDS, the command and control interface will always be up.

IOS 12.0 includes a more detailed selection of slot/port, unit, port-adapter, and so on. This information is not necessary for IDS.

Example

```
sensor#show interfaces command-control

command-control is up

Internet address is 10.89.147.31, subnet mask is 255.255.255.128,
telnet is disabled.
Hardware is eth1, tx
Network Statistics
eth1 Link encap:Ethernet HWaddr 00:06:5B:0F:0E:53
```

```
 inet addr:10.89.147.31 Bcast:10.89.147.127 Mask:255.255.255.128
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:49703 errors:5454 dropped:0 overruns:0 frame:289
TX packets:22928 errors:0 dropped:0 overruns:0 carrier:0
 collisions:1913
RX bytes: 17140400 (16.3mb) TX bytes: 11013743 (10.5mb) txqueuelen:100
Interrupt:16 Base address:0xddc0 Memory: feb20000-feb40000

sensor#
```

show interfaces group

Use the **show interfaces group** command to display information about the logical group.

show interfaces group *[number]*

Syntax Description	
number	Logical number for interface group. Valid values are 0–7. If no group number is provided, the command displays information about all interface groups.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

If the interface number is not specified, the **show interfaces group** command displays statistics for all interface groups.

Example

```
sensor#show interface group 0

Group 0 is up
Sensing ports int1
Logical virtual sensor configuration: virtualSensor
Logical alarm channel configuration: virtualAlarm

Statistics for Virtual Sensor

VirtualSensor0
General Statistics for this Virtual Sensor
 Number of seconds since a reset of the statistics = 8259
Total number of packets processed since reset = 72599
 Total number of IP packets processed since reset = 65659
Total number of packets that were not IP processed since reset = 6940
 Total number of TCP packets processed since reset = 62176
 Total number of UDP packets processed since reset = 3364
Total number of ICMP packets processed since reset = 119
Total number of packets that were not TCP, UDP, or ICMP processed
since reset = 0
 Total number of ARP packets processed since reset = 331
Total number of ISL encapsulated packets processed since reset = 275
Total number of 802.1q encapsulated packets processed since reset = 0
 Total number of packets with bad IP checksums processed since reset =
0
Total number of packets with bad layer 4 checksums processed since
reset = 0
 Total number of bytes processed since reset = 27794157
 The rate of packets per second since reset = 8
The rate of bytes per second since reset = 3365
The average bytes per packet since reset = 382
 Statistics for the TCP Stream Reassembly Unit
The current number of established TCP steams. (can not be reset) = 1
 The current number of embryonic TCP steams. (can not be reset) = 0
The current number of closing TCP steams. (can not be reset) = 0
TCP streams that have been tracked since last reset = 293
TCP packets that arrived out of order for thier stream. = 0
TCP Packets that caused a stream to jump over a gap in sequence. = 0
 TCP Packet currently queued for reassembly = 0
The rate of TCP connections tracked per second since reset = 0
 The Signature Database Statistics.
The Number of each type of node active in the system (can not be
reset)
Total nodes active = 58
TCP nodes keyed on both IP addresses and both ports = 2
UDP nodes keyed on both IP addresses and both ports = 1
```

```
IP nodes keyed on both IP addresses = 11
The number of each type of node inserted since reset Total nodes
inserted = 3053
TCP nodes keyed on both IP addresses and both ports = 269
UDP nodes keyed on both IP addresses and both ports = 251
IP nodes keyed on both IP addresses = 445
The rate of nodes per second for each time since reset Nodes per
second = 0
TCP nodes keyed on both IP addresses and both ports per second = 0
 UDP nodes keyed on both IP addresses and both ports per second = 0
IP nodes keyed on both IP addresses per second = 0sensor#
```

show interfaces sensing

Use the **show interfaces sensing** command to display information about the sensing interfaces.

show interfaces sensing *name*

Syntax Description	
name	Logical interface name (int0, int1, and so on)

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

If no logical name is specified, the **show interfaces sensing** command displays information about all sensing ports.

There is no related command in IOS versions 12.0 and earlier.

Example

```
sensor#show interfaces sensing

Sensing int0 is up
Hardware is eth0, Tx
Reset port
Sensing int1 is up
Hardware is eth1, TX
Reset port
Command control port
 MAC statistics from the IntelPro interface Link = up
 Speed = 100
 Duplex = Half
 State = up
Rx_Packets = 49703
Tx_Packets = 22928
 Rx_Bytes = 17140400
Tx_Bytes = 11013743
 Rx_Errors = 5454
 Tx_Errors = 0
 Rx_Dropped = 0
Tx_Dropped = 0
Multicast = 4957
Collisions = 1913
 Rx_Length_Errors = 5454
Rx_Over_Errors = 0
 Rx_CRC_Errors = 0
 Rx_Frame_Errors = 0
 Rx_FIFO_Errors = 0
Rx_Missed_Errors = 0
Tx_Aborted_Errors = 0
Tx_Carrier_Errors = 0
 Tx_FIFO_Errors = 0
 Tx_Heartbeat_Errors = 0
 Tx_Window_Errors = 0
 Tx_Abort_Late_Coll = 0
Tx_Deferred_Ok = 76 Tx_Single_Coll_Ok = 1261 Tx_Multi_Coll_Ok = 285
 Rx_Long_Length_Errors = 0
Rx_Short_Length_Errors = 0
 Rx_Align_Errors = 0
 Rx_Flow_Control_XON = 0
Rx_Flow_Control_XOFF = 0
 Tx_Flow_Control_XON = 0
Tx_Flow_Control_XOFF = 0
 Rx_CSum_Offload_Good = 41864
Rx_CSum_Offload_Errors = 0
PHY_Media_Type = Copper
```

```
 Packets dropped by PCAP ring = 0
Sensing int2 is down
 Hardware is falcon1, XL

sensor#
```

show privilege

Use the **show privilege** command to show your current level of privilege.

show privilege

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

A privilege level can only be modified by the administrator. See the **username** command for more information.

Example

```
sensor#show privilege
Current privilege level is viewer
sensor#
```

Related Commands

username

show ssh authorized-keys

Use the **show ssh authorized-keys** command to display the RSA keys for the current user.

show ssh authorized-keys *[id]*

Syntax Description	
id	1–256 character string that uniquely identifies the authorized key. Numbers, underscore (_), and dash (-) are valid. Spaces and question mark (?) are not valid.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

If no ID is specified, the **show ssh authorized-keys** command displays a list of configured IDs in the system.

Example

```
sensor#show ssh authorized-keys
system1
system2
```

```
system3
system4

sensor#show ssh authorized-keys system 1
1023 37

660222729556609833380897067163729433570828686860008172017802434921804 2
142078130359208295091017013584805250399939321125031474527683786209111 8
998665371608981314792208604473991134136964287068231936192814852186409 4
557416306138786468335115835910404940213136954353396163449793497050167 9
258314654862214646742199705 7
sensor#
```

ssh host-key

Use the **ssh host-key** command to add an entry to the known hosts table. If the modulus, exponent, and length are not provided, the system displays the MD5 fingerprint for the requested IP address and allows you to select to add the key to the table. Use the no form of this command to remove an entry from the known hosts table.

ssh host-key *ipaddress [key-modulus-length public-exponent public-modulus]*

no ssh host-key *ipaddress*

Syntax Description	
ipaddress	32-bit address written as 4 octets separated by periods. X.X.X.X where X=0–255.
key-modulus-length (optional)	ascii decimal integer in the range [511, 2048]
public-exponent (optional)	ascii decimal integer in the range [3, 2^32]
public-modulus (optional)	ascii decimal integer, x, such that (2 ^ key-modulus-length) < x < (2 ^ (key-modulus-length + 1))

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator

Usage Guidelines

The **ssh host-key** command adds an entry to the known hosts table. If the modulus, exponent and length are not provided, the secure shell sever at the specified IP address is contacted to obtain the required key. This information is sent over the network, therefore, the specified host must be accessible at the moment the command is issued.
To modify a key for an IP address, you must remove the entry from the table and then add the modified key back to the table.
There is no related command in IOS versions 12.0 and earlier.

Example

The following command adds an entry to the known host table for 10.1.2.3.

```
sensor(config)#ssh host-key 10.1.2.3 1024
139306213541835240385332922253968814685684523520064131997839905113640120217816869696708721704631322844292073851730565044879082670677555415793705848520399557211463129660455216130971260106861481274996959351374059833139315488498830230218292235333515265386058916365194499784287458362788327746013850608404341586192 7sensor(config)#
```

The following command adds an entry to the known host table for 10.1.2.3.

```
sensor(config)#ssh host-key 10.1.2.3
MD5 fingerprint is
49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7Bsensor(config)#
Would you like to add this to the known hosts table for this host?
[yes]
sensor(config)#
```

show ssh server-key

Use the **show ssh server-key** command to display the host key and host key fingerprint for the SSH server.

show ssh server-key

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **show ssh server-key** command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

```
sensor#show ssh server-key
1024 35
139306213541835240385332922253968814685684523520064131997839905113640l
202178168696967087217046313228442920738517305650448790826706775541579 3
705848520399557211463129660455216130971260106861481274996959351374059 8
331393154884988302302182922353335152653860589163651944997842874583627 8
832774601385060840434158619 27
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
sensor#
```

show settings

Use the **show settings** command to display the contents of the configuration contained in the current submode.

show settings

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

All service, tune-micro-engine, and alarm-channel-configuration submodes.

Supported User Roles

- Administrator
- Operator
- Viewer (with access to top-level command tree only)

Usage Guidelines

The **show settings** command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

The following example shows the output for NAC configuration mode:

```
sensor(config)#service netw
sensor(config-NetworkAccess)#show settings
cat6k-devices (min: 0, max: 100, current: 1)

communication:
ip-address: 172.21.172.151
nat-address: shun-device-cfg: groupa
shun-interfaces (min: 0, max: 100, current: 2)
```

```
post-vacl-name: testPostACL
pre-vacl-name: testPreACL
vlan: 1 units: none

post-vacl-name:
pre-vacl-name:
vlan: 5 units: none

general
————————————————————————
allow-sensor-shun: false
enable-acl-logging: false
master-blocking-sensors (min: 0, max: 100, current: 0)

never-shun-hosts (min: 0, max: 100, current: 0)
————————————————————————
————————————————————————- never-shun-networks (min: 0, max: 100,
current: 0)
————————————————————————
————————————————————————
shun-enable: true
shun-hosts (min: 0, max: 100, current: 0)

shun-max-entries: 100 units: none
shun-networks (min: 0, max: 100, current: 0)
————————————————————————
————————————————————————
————————————————————————
 pix-devices (min: 0, max: 100, current: 1)
————————————————————————
communication: telnet
 enable-acl-logging: false ip-address: 172.21.172.151
nat-address:
shun-device-cfg:

router-devices (min: 0, max: 100, current: 1)
————————————————————————
communication:
ip-address: 172.21.172.100
nat-address:
shun-device-cfg: groupa
shun-interfaces (min: 0, max: 100, current: 2)

direction: in
interface-name: fa1/0
post-acl-name: testPostACL
pre-acl-name: testPreACL
 ————————————————————————
```

```
direction: out
interface-name: FastEthernet1/0
post-acl-name:
 pre-acl-name:

shun-device-cfg (min: 0, max: 100, current: 1)

enable-password: <hidden>
name: groupa
password: <hidden>
tacacs-password:
username: managed

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

show statistics

Use the **show statistics** command to display the requested statistics.

show statistics { Authentication | EventServer | EventStore | Host | Logger | NetworkAccess | TransactionServer | TransactionSource | WebServer } [clear]

Syntax Description	
clear	Clear the statistics after they are retrieved. This option is not available for Host or NetworkAccess statistics.
Authentication	Display authorizations-authentication statistics.
EventServer	Display event server statistics.
EventStore	Display event store statistics.
Host	Display host (main) statistic.s
Logger	Display logger statistics.

Syntax Description	
Network Access	Display network-access-controller statistics.
TransactionServer	Display transaction server statistics.
TransactionSource	Display transaction source statistics.
WebServer	Display web-server statistics.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

There is no related command in IOS versions 12.0 and earlier.

show tls fingerprint

Use the **show tls fingerprint** command to display the TLS certificate fingerprint.

show tls fingerprint

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **show tls fingerprint** command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

```
sensor#show tls fingerprint
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB SHA1:
16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

show tls trusted-hosts

Use the **show tls trusted-hosts** command to display the trusted hosts for this sensor.

show tls trusted-hosts *[id]*

Syntax Description	
id	1–32 character string uniquely identifying the authorized key. Numbers, dash (-), and underscore (_) are valid. Spaces and question marks (?) are not accepted.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

Use the **show tls trusted-hosts** command without the ID to display a list of configured IDs. Use this command with a specific ID to view the fingerprint of the certificate associated with that ID.

This command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

```
sensor#show tls trusted-hosts
172.21.172.1
10.2.1.4
10.1.1.1

sensor#show tls trusted-hosts 10.1.1.1
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

show tech-support

Use the **show tech-support** command to display the current system status.

show tech-support [page][password][**destination** *destination-url*]

Syntax Description	
page	(Optional) Causes the output to display one page of information at a time. Use the Enter key to display the next line of output or use the Spacebar to display the next page of information. If **page** is not used, the output is displayed without page breaks
password	(Optional) Leaves passwords and other security information in the output. If **password** is not used, passwords and other security sensitive information in the output are replaced with the label <removed> by default.
destination	(Optional) Tag indicating the information should be formatted as HTML and sent to the destination following this tag.
destination-url	(Optional) The destination for the report file. If a url is provided, the output will be formatted into an HTML file and sent to the specified destination; otherwise the output is displayed on the screen.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

IOS version 12.0 does not support the destination portion of this command.

The exact format of the destination URL varies according to the file. The user can select a filename, but it must be terminated by .html.

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

The report contains HTML-linked output from the following commands:

- **more current-config**
- **show version**
- **getHostSupportInfo** (control transaction response)
- Debug Logs

Example

The following example will place 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.htmlpassword:*******
```

The following example will place the tech-support output into the file /absolute/reports/sensor1Report.html:

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

show users

Use the **show users** command to display information about users logged in to the CLI.

show users [all]

Syntax Description	
all	(Optional) Lists all user accounts configured on the system, regardless of login status.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **show users** command displays an ID, username, and privilege. An asterisk (*) next to the description indicates the current user.

A maximum of 10 users can be logged in to the sensor at a time.

The output for this command differs from the IOS command.

Example

```
sensor#show users

CLI ID     User           Privilege
1234       notheruser     viewer
*9802      curuser        operator
5824       tester         administrator

sensor#show users all

CLI ID     User           Privilege
1234       notheruser     viewer
*9802      curuser        operator
5824       tester         administrator
           tester2        viewer
           foobar         operator
```

show version

Use the **show version** command to display the version information for all installed operating system (OS) packages, signature packages, and IDS process running on the system.

show version

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The output for the **show version** command is IDS specific and differs from the output for the IOS command.

Example

```
sensor#show version

Application Partition:
 Cisco Systems Intrusion Detection Sensor, Version 4.0(2)S30
OS Version 2.4.18-5
Platform: 4210
Sensor up-time is 24 hours, 34 minutes
Using 150728704 out of 200593408 bytes of available memory (75% usage)
Using 3800498176 out of 4293263360 bytes of available disk space (89%
usage)
MainApp v122 (Release) 2002-09-27T14:25-0500 Running
AnalysisEngine v122 (Release) Running
Authentication v122 (Release) Running
WebServer v122 (Release) Running
CLI v122 (Release)
Upgrade History: IDS-K9-sig-4.0-2-S30.rpm 14:46:50CST Mon Nov 04 2002
*IDS-K9-sp-4.0-2-S29.rpm 08:02:23 CST Fri Nov 01 2002
```

shutdown

Use the **shutdown** command to disable an interface. Use the no form of this command to restart a disabled interface.

shutdown

no shutdown

Syntax Description

There are no parameters or keywords associated with this command.

Command Modes

Interface Sensing Configuration

Interface Group Configuration

Supported User Roles

Administrator

Usage Guidelines

The **shutdown** command disables all sniffing on the interface.

Using this command on a group interface shuts down all ports assigned to that group. To shut down an individual sensing port without affecting the remaining ports in that group, you must first remove the port from the group.

Example

The following example disables sniffing on sensing int0

```
sensor(config)#interface sensing
sensor(config-if)#shutdown
sensor(config-if)#
```

The following example enables sniffing on sensing int0

```
sensor(config-if)#no shutdown
sensor(config-if)#
```

tls generate-key

Use the **tls generate-key** command to regenerate the self-signed X.509 certificate for the server. If the host is not using a self-signed certificate, an error is returned.

tls generate

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Exec

Supported User Roles

Administrator

Usage Guidelines

This command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

```
sensor(config)#tls generate-key
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor(config)#
```

tls trusted-host

Use the **tls trusted-host** command to add a trusted host to the system. Use the no form of this command to remove a trusted host certificate.

tls trusted-host ip-address *ip-address*

no tls trusted-host ip-address *ip-address*

Syntax Description	
ip-address	IP address host to add or remove.

Command Modes

Global Configuration

Supported User Roles

- Administrator
- Operator

Usage Guidelines

The **tls trusted-host** command retrieves the current fingerprint for the requested host and displays the result. You can accept or reject the fingerprint based on information retrieved directly from the host you are trying to add.

This command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

The following example adds an entry to the trusted host table for IP address 172.21.172.1:

```
sensor(config)#tls trusted-host ip address 172.21.172.1
RSA key MD5 fingerprint is
D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
RSA key SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this
host? [yes]
sensor(config)#
```

telnet-server enable

Use the **telnet-server enable** command to enable the Telnet server. Use the no form of this command to disable Telnet access.

telnet-server enable

no telnet-server enable

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

There is no related command in IOS versions 12.0 and earlier.

Example

The following example enables Telnet access to the device.

```
sensor(config)#telnet-server enable
sensor(config)#
```

terminal

Use the **terminal** command to modify terminal properties for a login session.

terminal[**length** *screen-length*]

Syntax Description	
screen-length	Set the number of lines on the screen. This value will be used to determine when to pause during multiple-screen output. A value of zero results in no pause when the output exceeds the screen length. Default is 24 lines. This value is not saved between login sessions.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **terminal length** command sets the number of lines that will be displayed before the `more` prompt is displayed. This command is allowed for all user roles.

Example

The following example sets the CLI to not pause between screens for multiple-screen displays:

```
sensor#terminal length 0

sensor#

sensor#terminal length 10

sensor#
```

trace

Use the **trace** command to display the route an IP packet takes to a destination.

trace *address[count]*

Syntax Description	
address	Address of system to trace route to.
count	Number of hops to take. Default is 4. Valid values are 1–256.

Command Modes

Exec

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

There is no command interrupt for the **trace** command. The command must run to completion.

Example

```
sensor#trace 10.1.1.1

traceroute to 172.21.172.24 (172.21.172.24), 30 hops max, 40 byte
packets 1 171.69.162.2 (171.69.162.2) 1.25 ms 1.37 ms 1.58 ms 2
172.21.172.24 (172.21.172.24) 0.77 ms 0.66 ms 0.68 ms

sensor#
```

tune-alarm-channel

Use the **tune-alarm-channel** command to enter configuration mode for the virtual alarm channels.

tune-alarm-channel

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Alarm Channel Configuration Mode

Supported User Roles

- Administrator
- Operator
- Viewer

Usage Guidelines

The **tune-alarm-channel** command allows you to configure the event filters and signature definitions 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 the user exits the tune-alarm-channel mode.

This command is IDS specific; there is no related command in IOS versions 12.0 and earlier.

Example

```
sensor(config)#service alarm-channel-configuration virtualAlarm

sensor(config-acc-virtualAlarm)#tune-alarm-channel

sensor(config-acc-tun)#
```

tune-micro-engines

Use the **tune-micro-engines** command to enter the configuration mode for the virtual sensor micro-engines.

tune-micro-engines

Syntax Description

There are no commands or keywords associated with this command.

Command Modes

Virtual Sensor Configuration

Supported User Roles

- Administrator
- Operator
- Viewer (Display Only)

Usage Guidelines

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 are dependent 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 the user exits the tune-micro-engines mode.

There is no related command in IOS versions 12.0 and earlier.

Example

```
sensor(config)#service virtual-sensor-configuration virtualSensor
sensor(config-vsc-virtualSensor)#tune-micro-engines
sensor(config-vsc-tun)#
```

upgrade

Use the **upgrade** command to apply a service pack, signature update or image upgrade.

upgrade *source-url*

Syntax Description	
source-url	The location of the upgrade to retrieve.

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

From the command line, you can type all necessary source and destination URL information and the username. If you type only the command (upgrade) followed by a prefix (ftp: or scp:), you will be prompted for any missing information, including a password where applicable.

The directory specification should be an absolute path to the desired file. The filename is optional. For recurring upgrades, a filename will not be present.

Use the following guidelines when designating the source or destination:

- **ftp:**—Source URL for File Transfer Protocol network server. The syntax for this prefix is ftp:[[//username@]location]/relativeDirectory/filename or ftp:[[//username@]location]//absoluteDirectory/filename.
- **https:**—Source URL for web server. The syntax for this prefix is https:[[//username@]location]/directory]/filename.
- **scp:**—Source URL for the Secure Copy Protocol network server. The syntax for this prefix is scp:[[//username@]location]/relativeDirectory]/filename or scp:[[//username@]location]/absoluteDirectory]/filename.
- **http:**—Source URL for web server. The syntax for this prefix is http:[[//username@]location]/directory]/filename.

There is no related command in IOS versions 12.0 and earlier.

Example

The following example prompts the sensor to immediately check for the specified upgrade. The directory and path are relative to the tester's user account.

```
sensor#upgrade scp://tester@10.1.1.1/upgrade/sp.rpm
Enter password: *****
Re-enter password: *****
```

username

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.

username *name*[**password** *password*][**privilege** *privilege*]

Syntax Description	
name	Specifies the username. A valid username is 1–32 characters long. Acceptable characters are alphanumeric, dash (-), and underscore (_).
password	Specifies the password for the user.
privilege	Sets the privilege level for the user. Allowed levels are Administrator, Operator, or Viewer. The default is Viewer.

Command Modes

Global Configuration

Supported User Roles

Administrator

Usage Guidelines

The **username** command provides username and password authentication for login purposes only. This command cannot be used to remove the user currently 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.

Example

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: *****
```

The following example changes the privilege level of the user ‘tester’ to ‘operator’.

```
sensor(config)#username tester privilege operator
```